# User Manual

# IFS-803SM
# IGS-803SM

## Industrial Grade Managed Ethernet Switches

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, and EN60950-1:2006

***CTC Union Technologies Co., Ltd.***
Far Eastern Vienna Technology Center (Neihu Technology Park)
8F, No. 60, Zhouzi St.
Neihu, Taipei, 114
Taiwan
Phone: +886-2-2659-1021
FAX: +886-2-2799-1355

***IFS/IGS-803SM Series***
Industrial Grade Managed Ethernet Switches

User Manual
Version 1.4 May 2016 (Update)

This manual supports the following models:

| | |
|---|---|
| IFS-803GSM | Fast Ethernet 8TP+3FX Managed Industrial Switch |
| IFS-803GSM-E | Fast Ethernet 8TP+3FX Managed Industrial Switch, Extended Temperature |
| IGS-803SM | Gigabit Ethernet 8TP+3FX Managed Industrial Switch |
| IGS-803SM-E | Gigabit Ethernet 8TP+3FX Managed Industrial Switch, Extended Temperature |
| IFS-803GSM-8PH24 | Fast Ethernet 8TP+3FX Managed Industrial PoE Switch |
| IFS-803GSM-8PHE24 | Fast Ethernet 8TP+3FX Managed Industrial PoE Switch, Extended Temperature |
| IGS-803SM-8PH24 | Gigabit Ethernet 8TP+3FX Managed Industrial PoE Switch |
| IGS-803SM-8PHE24 | Gigabit Ethernet 8TP+3FX Managed Industrial PoE Switch, Extended Temperature |

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.

# CHAPTER 1. INTRODUCTION

## 1.1 Welcome

Welcome and thank you for purchasing this "Industrial Strength" 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 Ethernet switches with the desire of providing a highly stable and reliable product that will give years of trouble free operation. We are so sure of our product design, we offer an unconditional 5 years warrantee.

In this chapter we will introduce all of the various models available in this series, for Fast Ethernet, Gigabit Ethernet, PoE and non-PoE applications. These models can be either wall mounted or DIN rail mounted. Chapter 2 will describe the mounting and installation methods. All the models in this series utilize almost identical management interfaces, whether using serial console and CLI (command line interface) commands, Telnet, SSH, HTTP (Web GUI) or SNMP (Simple Network Management Protocol). Chapter 4 will detail all of the configuration settings by using an easy to point and click Web interface which can be accessed from any available web browser.

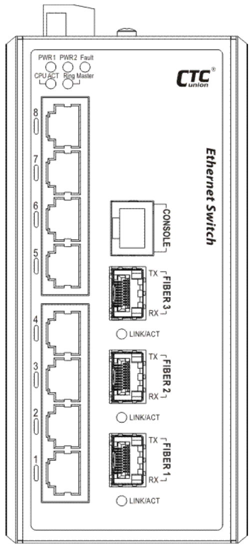
## 1.2 Product Description

**IFS/IGS-803SM** models are managed industrial grade Fast & Gigabit PoE (Power over Ethernet) and non-PoE switches that provide stable and reliable Ethernet transmission. Housed in rugged DIN rail or wall mountable enclosures, these switches are designed for harsh environments, such as industrial networking and intelligent transportation systems (ITS) and are also suitable for many military and utility market applications where environmental conditions exceed commercial product specifications. Standard operating temperature range models (-10°C to 60°C) and wide operating temperature range models (-40°C to 75°C) fulfill the special needs of industrial automation applications.

Throughout the rest of this section, each model in this series will be detailed. After reviewing this section, the naming system for the model names will become clearer. But very basically, this series is divided in both Fast Ethernet and Gigabit Ethernet models. Then they are further divided into PoE capable or non-PoE models. Lastly, there are two temperature ranges for these models, the commercial temperature range (-10°C~60°C) and the extended industrial temperature range (-40°C~75°C).

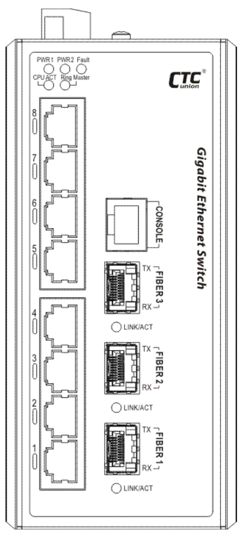
### *1.2.1 IFS-803GSM*

The **IFS-803GSM** is an Industrial Fast Ethernet Switch (IFS) for commercial temperature range of -10°C to +60°C. There are 8 LAN ports with RJ-45 connectors that support 10M/100M Ethernet. There are 3 fiber ports that support 100M/1000M dual rate speed and utilize SFP cages that support any industry standard Fast or Gigabit SFP module. The Ethernet switch is fully manageable; supporting most standard Layer 2 Ethernet configurable settings. The **IFS-803GSM-E** model is identical in every way, except it can support an extended operating temperature range of -40°C to +75°C.



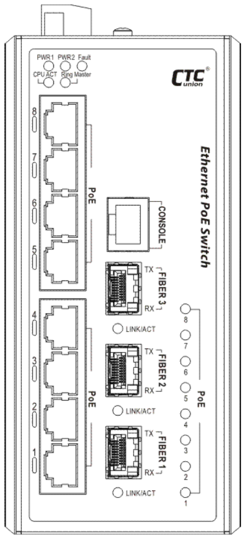

### 1.2.2 IGS-803SM

The **IGS-803SM** is an Industrial Gigabit Ethernet Switch (IGS) for commercial temperature range of -10°C to +60°C. There are 8 LAN ports with RJ-45 connectors that support 10M/100M/1000M Ethernet. There are 3 fiber ports that support 100M/1000M dual rate speed and utilize SFP cages that support any industry standard Fast or Gigabit SFP module. The Ethernet switch is fully manageable; supporting most standard Layer 2 Ethernet configurable settings). The **IGS-803SM-E** model is identical in every way, except it can support an extended operating temperature range of -40°C to +75°C.



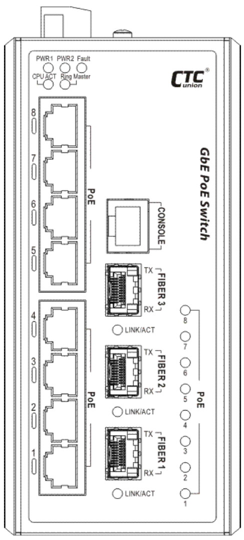

### 1.2.3 IFS-803GSM-8PH24

The **IFS-803GSM-8PH24** is an Industrial Fast Ethernet, Power over Ethernet (PoE), Switch (IFS) for commercial temperature range of -10°C to +60°C. There are 8 LAN ports with RJ-45 connectors that support 10M/100M Ethernet. These LAN ports support PoE for either IEEE802.3af (15.4 watts) or IEEE802.3at (30 watts) with a total power budget of 180watts. This model features a "Power Boost" design which allows it to provide a standard, regulated PoE voltage of 55VDC, but only requires 24VDC running voltage. The lower 24VDC running voltage allows this unit to be deployed in many transportation applications where there is no 48VDC and only 24VDC is available. There are 3 fiber ports that support 100M/1000M dual rate speed and utilize SFP cages that support any industry standard Fast or Gigabit SFP module. The Ethernet switch is fully manageable; supporting most standard Layer 2 Ethernet configurable settings. The **IFS-803GSM-8PHE24** model is identical in every way, except it can support an extended operating temperature range of -40°C to +75°C.




### 1.2.4 IGS-803SM-8PH24

The **IGS-803SM-8PH24** is an Industrial Gigabit Ethernet, Power over Ethernet (PoE), Switch (IGS) for commercial temperature range of -10°C to +60°C. There are 8 LAN ports with RJ-45 connectors that support 10M/100M/1000M Ethernet. These LAN ports support PoE for either IEEE802.3af (15.4 watts) or IEEE802.3at (30 watts) with a total power budget of 180watts. This model features a "Power Boost" design which allows it to provide standard, regulated PoE voltage of 55VDC, but only requires 24VDC running voltage. The lower 24VDC running voltage allows this unit to be deployed in many transportation applications where there is no 48VDC and only 24VDC is available. There are 3 fiber ports that support 100M/1000M dual rate speed and utilize SFP cages that support any industry standard Fast or Gigabit SFP module. The Ethernet switch is fully manageable; supporting most standard Layer 2 Ethernet configurable settings. The **IGS-803SM-8PHE24** model is identical in every way, except it can support an extended operating temperature range of -40°C to +75°C.



## 1.3 Product Features

- Wide temperature model (supports -40°C~75°C)
- 8 x 10/100Base-T(X) RJ-45 with 3 x 100/1000Base-X SFP Fiber (IFS Series)
- 8 x 10/100/1000Base-T(X) RJ-45 with 3 x 100/1000Base-X SFP Fiber (IGS Series)
- 24/48VDC Redundant dual DC inputs
- Normally Closed (NC) user programmable alarm relay contact
- Power booster design for up to 55 VDC for PoE/PoE+ output with only 24VDC input
- Constant and regulated PoE output voltage at 55VDC
- Provides 8-port IEEE802.3af / 802.3at PoE Output (30W per Port)
- Maximum PoE power budget of 180W
- Advanced PoE management that includes PoE PD auto detection, auto reset (cycle power to unresponsive IP camera), PoE configuration for weekly power scheduling
- IP30 rugged metal housing
- UL60950-1, CE, FCC, Rail Traffic EN50121-4 Certified
- Industrial grade EMS (EN61000-6-2) and EMI (EN61000-6-4)
- Cable diagnostic, length measurement, cable OK or broken point distance
- Supports IEEE802.3az EEE (Energy Efficient Ethernet) Management to optimize power consumption
- STP, RSTP, MSTP, ITU-T G.8032 Ethernet Protection Ring(EPR) for cabling redundancy
- QoS, Traffic classification QoS, CoS, Band width control for Ingress and Egress, broadcast storm control, DiffServ
- IEEE802.1q VLAN, MAC based VLAN, IP subnet based VLAN, Protocol based VLAN, VLAN translation, MVR
- Dynamic IEEE 802.3ad LACP Link Aggregation, Static Link Aggregation
- IGMP/MLD snooping V1/V2/V3, IGMP Filtering / Throttling, IGMP query, IGMP proxy reporting, MLD snooping
- Security : Port based and MAC based IEEE802.1X, RADIUS, ACL, TACACS+, HTTP/HTTPS, SSL/SSH v2
- CLI, Web based management, SNMP v1/v2c/v3, Telnet server for management
- Software upgrade via TFTP and HTTP, dual partitioned flash for quick recovery from upgrade failure
- DHCP client/Relay/Snooping/Snooping option 82/Relay option 82
- RMON, MIB II, port mirroring, event syslog, DNS, NTP/SNTP, IEEE802.1ab LLDP
- Supports IPv6 Telnet server /ICMP v6, SNMP, HTTP, SSH/SSL, NTP/SNTP, TFTP, QoS, ACL

## 1.4 Product Specifications

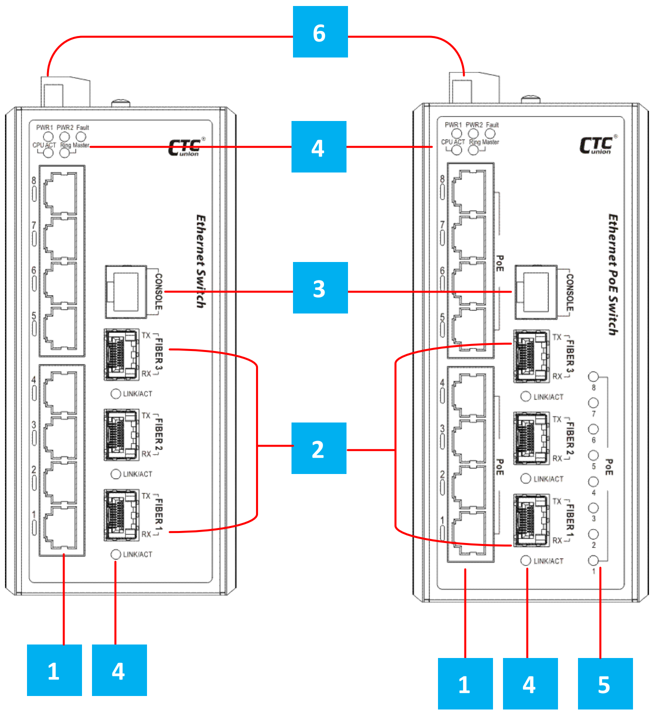
| | | |
|---|---|---|
| **Standards** | IEEE 802.3 | 10Base-T 10Mbit/s Ethernet |
| | IEEE 802.3u | 100Base-TX, 100Base-FX, Fast Ethernet |
| | IEEE 802.3ab | 1000Base-T Gbit/s Ethernet over twisted pair |
| | IEEE 802.3z | 1000Base-X Gbit/s Ethernet over Fiber-Optic |
| | IEEE 802.1d | STP (Spanning Tree Protocol) |
| | IEEE 802.1w | RSTP (Rapid Spanning Tree Protocol ) |
| | IEEE 802.1s | MSTP (Multiple Spanning Tree Protocol ) |
| | ITU-T G.8032 / Y.1344 | EPR (Ethernet Protection Ring ) |
| | IEEE 802.1Q | Virtual LANs (VLAN) |
| | IEEE 802.1X | Port based Network Access Control, Authentication |
| | IEEE 802.3ad | Link aggregation for parallel links with LACP(Link Aggregation Control Protocol) |
| | IEEE 802.3x | Flow control for Full Duplex |
| | IEEE 802.3af | PoE (Power over Ethernet) |
| | IEEE 802.3at | PoE+ (Power over Ethernet enhancements) |
| | IEEE 802.1ad | Stacked VLANs, Q-in-Q |
| | IEEE 802.1p | LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization |
| | IEEE 802.1ab | Link Layer Discovery Protocol (LLDP) |
| | IEEE 802.3az | EEE (Energy Efficient Ethernet) |
| **Switch** | VLAN Groups | up to 4096 |
| | Switching Fabric | 7.6Gbps (IFS series), 22Gbps (IGS series) |
| | 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 |
| **PoE** | PoE standards | IEEE802.3af, IEEE802.3at |
| | PoE Ports | RJ-45 pin assignment, 8 RJ-45 ports support IEEE 802.3af / IEEE 802.3at End-Span |
| | PoE Mode | Alternative A: Positive (VCC+): RJ-45 pin 1, 2. Negative (VCC-): RJ-45 pin 3, 6. Data (1,2,3,6 ) |
| **Connectors** | LAN | 8 x RJ-45 10/100/1000BaseT(X) auto detect speed, auto negotiate duplex, auto MDI/MDI-X function, Full/Half duplex |
| | Fiber | 3 X 100/1000 BaseX dual speed mode SFP slots, supporting DDMI |
| | Console | RS-232 (RJ-45) |
| **Ethernet** | Network Cable | UTP/STP Cat.5e cable or above |
| | EIA/TIA-568 | 100-ohm (100m) |
| | Protocol | CSMA/CD |
| | Reverse polarity | auto detect/correct |
| | Protection | Present |
| | Overload current protection | Present |
| | CPU Watch Dog | Present |
| **Power** | Power Supply | Redundant Dual DC 24/48V (20~57VDC) Input power (Removable Terminal Block ) |

| | | |
|---|---|---|
| **Certifications** | EMC | CE |
| | EMI | FCC Part 15 sub B class A, CE EN55022 Class A |
| | Immunity & Emission for Heavy Industrial Environment | EN61000-6-2, EN61000-6-4 |
| | EMS | EN61000-4-2 (ESD) Level 3, Criteria B<br>EN61000-4-3 (RS) Level3, Criteria A<br>EN61000-4-4 (Burst) Level3, Criteria A<br>EN61000-4-5 (Surge) Level3, Criteria B<br>EN61000-4-6 (CS) Level3, Criteria A<br>EN61000-4-8 (PFMF, Magnetic Field) Field Strength: 300A/m, Criteria A |
| | Safety | UL60950-1 |
| | Railway Traffic | EN50121-4 |
| | Shock | EN60068-2-27 |
| | Freefall | EN60068-2-32 |
| | Vibration | EN60068-2-6 |

# CHAPTER 2. PANELS & INSTALLATION

## 2.1 Views of Panels

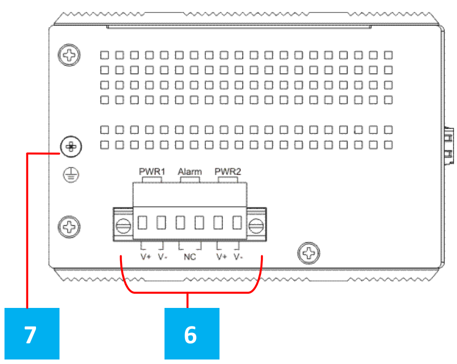
Each physical feature on the panels is indexed numerically and explained briefly in the reference box on the right hand side. Detailed descriptions for each feature are also provided in the following sub-sections.



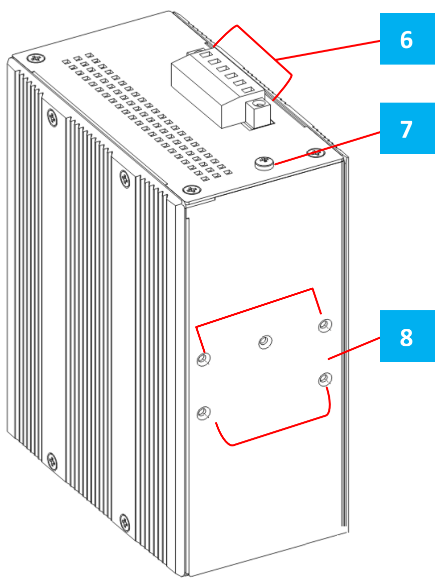

Front Panel

**Index Reference**

| | |
|---|---|
| 1 | RJ-45 LAN ports |
| 2 | SFP-based fiber optical ports |
| 3 | Console port |
| 4 | LED indicators |
| 5 | PoE LED indicators |
| 6 | Terminal block for two power inputs and alarm relay contact |
| 7 | Earth ground screw |
| 8 | Screw holes for din rail and wall-mounting kit |

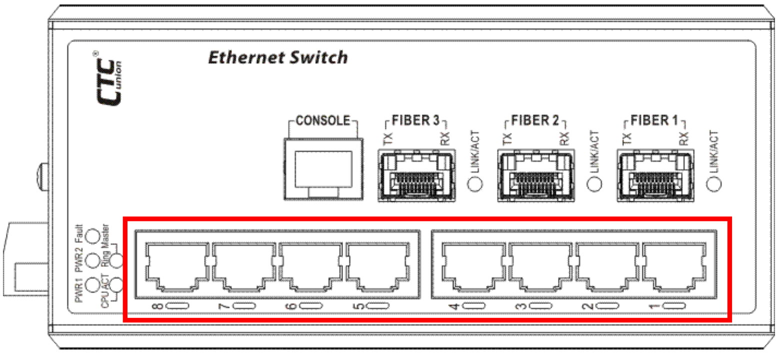



Top Panel




Side & Rear Panel

## 2.2 LAN Connections

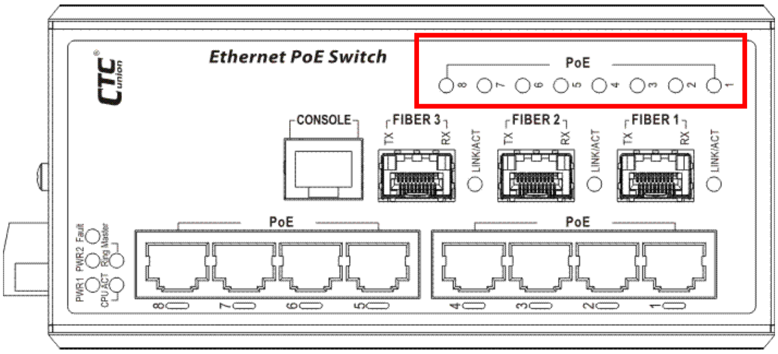



Front of unit

There are 8 shielded RJ-45 that provide LAN connection to the Switch. On the **IFS Series**, these provide Ethernet for 10M/100M connection. On the **IGS Series**, these ports are 10M/100M/1000M. Each of these eight LAN ports has associated LEDs which indicate the active link state and the detected speed of the interface. A green indicates a link and a speed of 100M, while amber color indicates a link and speed of 1000M.

## 2.3 PoE

For **IFS/IGS Series** units with PoE capability, the 8 LAN ports support PoE (Power over Ethernet) per IEEE802.3af (15.4W) or IEEE802.3at (30W) for connection to standard PoE PD (Power Devices) such as IP Cameras, Access Points, IP Phones, Digital Signage, etc. PoE eliminates the need to run separate power to these devices thereby simplifying deployment and reducing expenses. The total power budget for all 8 ports is 180 watts. The LAN ports may also connect to any non-PoE device for normal Ethernet transmission without any damage to the non-PoE device or to the **IFS/IGS** device.

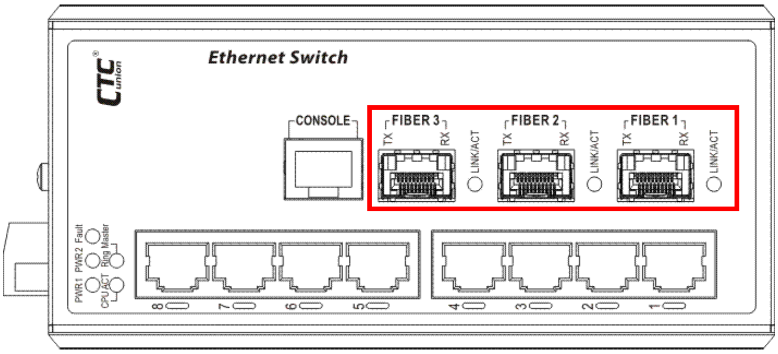



Front of unit

PoE green LEDs indicate the power status of IEEE802.3af/at. When "ON", these LEDs indicate that a PD (Powered Device) has been connected to the LAN port, successfully negotiated PoE and is being supplied power from the **IFS/IGS-803**. In the event of PoE fault (overload, short circuit or failed port) this green LED will flash. When no PoE is being provided, the PoE LED for that port will remain "OFF".

***NOTE:*** *The IFS/IGS-803 with PoE feature requires at least 24VDC input voltage or the PoE circuits will always remain inactive.*

## 2.4 Fiber Connections



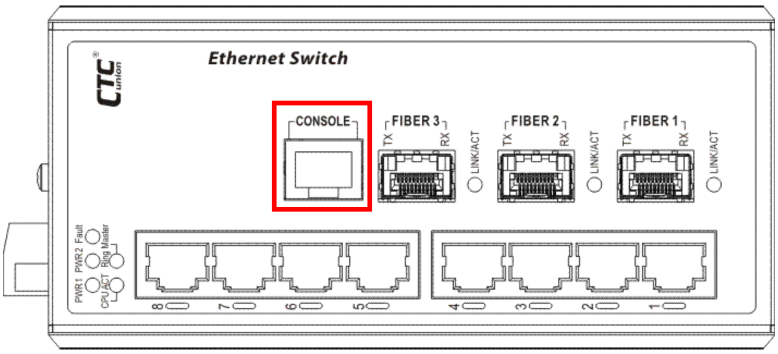

Front of unit

The **IFS/IGS-803** Series utilize SFP modules for fiber transmissions. Each of the fiber ports has an associated status LED to indicate the presence or absence of fiber link and will also flash when there is Ethernet activity on the port. Each of three SFP cages may insert any standard SFP module and be configured for 100M or 1000M operation. By having a third fiber port, these devices can be used in a ring or linear topology while still having a third port for a fiber branch. This makes these units extremely flexible when compared to other brand devices which have only two fiber ports.

Within the management interfaces of the **IFS/IGS-803** Series, the fiber ports are numbered after the eight electrical ports. So, those three ports are seen as ports 9, 10 and 11 by the internal switch and as viewed in management.

## 2.5 Console Port Connection

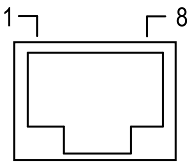
**IFS/IGS-803 Series** has an asynchronous terminal console port for local management via a serial terminal. The terminal provides management via a CLI (Command Line Interface) which will be familiar to many networking engineers. For most users, the CLI can be used to initially configure TCP/IP access so that further configuration can be completed via the GUI (Graphical User Interface) and any web browser.




Front of unit

### 2.5.1 RJ-45 Pin Assignment

This RJ-45 connector provides an RS-232 DCE (data communication equipment) asynchronous serial connection for local management.



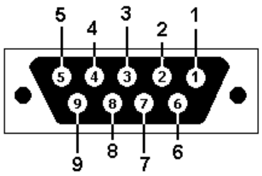

**CONSOLE**

| Pin | Ref. | Definition | Direction |
|---|---|---|---|
| 3 | RxD | Receive Data | Out towards DTE |
| 6 | TxD | Transmit Data | In from DTE |
| 5 | SG | Signal Ground | na |

### 2.5.2 Accessory Cable

This DB9F to RJ-45 cable provides a connection for the RS-232. This cable is used between the **IFS/IGS803** and the serial port of terminal.

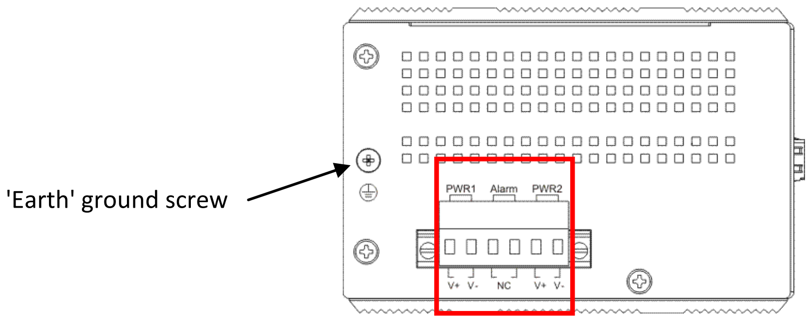
**to PC COM Port**




| Pins | | Ref. | Definition | Direction |
|---|---|---|---|---|
| DB9 | RJ-45 | | | |
| 2 | 3 | RxD | Receive Data | Out IFS/IGS803 towards DTE |
| 3 | 6 | TxD | Transmit Data | In IFS/IGS803 from DTE |
| 5 | 5 | SG | Signal Ground | na |

## 2.6 Power & Alarm

**IFS/IGS803 Series** uses a removable terminal block for connection of DC power and Alarm. This device supports dual input from two different DC power sources so that in the event of a single source failure, the **IFS/IGS803** device will continue to function normally.




Top View

The two power connections are shown in the above graphic. The device has clearly printed on the case the locations of the two power inputs, their DC polarity as well as the alarm connection. The single electrical relay can be wired into an alarm circuit and under normal condition it is connected as Normally Closed (will open upon alarm condition). The alarm conditions include power failure, port link up/down and PoE status (for PoE models only) and are user programmable through Web user interface. See Alarm Configuration in SNMP for more information on configuring alarm relay and triggering fault events. Please note that the alarm relay contact can only support 1A current at 24VDC. Do not apply voltage and current that exceed these specifications.

## 2.7 Earth Ground Connection

A separate 'Earth' grounding terminal is provided on the top mental palate for safety grounding of the **IFS/IGS Series**. It is highly recommended that a stable ground be attached to this device so that any surges on power or via LAN ports can be properly and safely shunted to ground. Follow steps below to install ground wire:

**Step 1.** Prepare one suitable ground screw and one grounding cable.

**Step 2.** Attach the grounding screw to the ring terminal of the grounding cable. Make sure that the grounding cable is long enough to reach the earth.

**Step 3.** Use a screwdriver (or other tools) to fasten the grounding screw on the earth ground hole securely.

## 2.8 LED Indicators

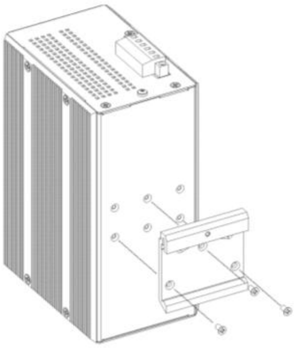
<table>
<tr><th>LED</th><th>Color</th><th>Status</th><th>Meaning</th></tr>
<tr><td rowspan="2">PWR 1</td><td rowspan="2">Green</td><td>On</td><td>Lit if power is connected and active at the PWR1 input terminal connection.</td></tr>
<tr><td>Off</td><td>PWR1 input terminal is not connected.</td></tr>
<tr><td rowspan="2">PWR 2</td><td rowspan="2">Green</td><td>On</td><td>Lit if power is connected and active at the PWR2 input terminal connection.</td></tr>
<tr><td>Off</td><td>PWR2 input terminal is not connected.</td></tr>
<tr><td rowspan="2">Fault</td><td rowspan="2">Amber</td><td>On</td><td>Lit when one or more of the programmable alarm conditions is active.</td></tr>
<tr><td>Off</td><td>No programmable alarm conditions are active.</td></tr>
<tr><td>CPU Act</td><td>Green</td><td>On</td><td>During normal use, this green LED will be lit, indicating a healthy condition of the running CPU.</td></tr>
<tr><td>Ring Master</td><td>Yellow</td><td>On</td><td>Lit when this unit is the 'master' in a fiber ring and all units are configured for u-Ring or ERPS (Ethernet Ring Protection Switching or G.8032).</td></tr>
<tr><td rowspan="4">RJ-45 Link/Act</td><td rowspan="2">Green</td><td>On</td><td>Port link is up and works in 10M/100M.</td></tr>
<tr><td>Blinking</td><td>Traffic is present.</td></tr>
<tr><td rowspan="2">Amber (For IGS-803 only)</td><td>On</td><td>Port link is up and works in 1000M.</td></tr>
<tr><td>Blinking</td><td>Traffic is present.</td></tr>
<tr><td rowspan="4">Fiber Link/Act</td><td rowspan="2">Green</td><td>On</td><td>Port link is up and works in 100M.</td></tr>
<tr><td>Blinking</td><td>Traffic is present.</td></tr>
<tr><td rowspan="2">Amber</td><td>On</td><td>Port link is up and works in 1000M.</td></tr>
<tr><td>Blinking</td><td>Traffic is present.</td></tr>
<tr><td rowspan="3">PoE (For PoE models only)</td><td rowspan="3">Green</td><td>On</td><td>Lit when the respective LAN port has successfully negotiated PoE and is supplying output power to the remote connected PD device.</td></tr>
<tr><td>Off</td><td>The respective LAN port has not successfully negotiated PoE and does not supply output power to the remote connected PD device.</td></tr>
<tr><td>Blinking</td><td>One of the PoE faults (overload, short circuit, port failure at startup) occurs.</td></tr>
</table>

## 2.9 Installation

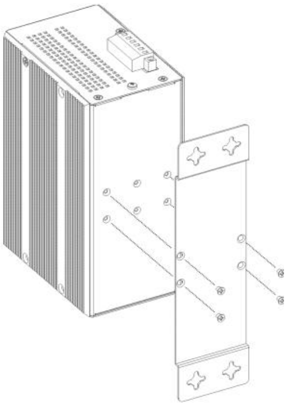
**IFS/IGS Series** is designed for wall mounting or DIN rail mounting. The units come with both wall mount and DIN rail hardware brackets from the factory.

### 2.9.1 Mounting

When installing the DIN rail bracket, be sure to correctly align the orientation pin.



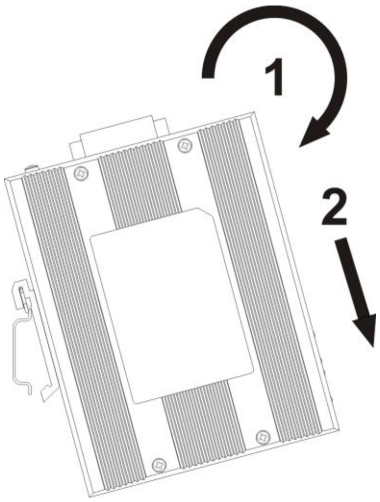
DIN Rail



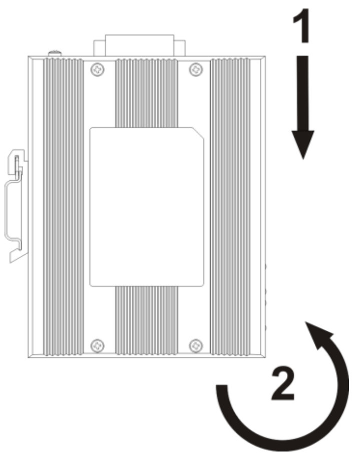
Wall Mount

### 2.9.2 Un-mounting

**IFS/IGS Series** with DIN Rail bracket has a steel spring in the upper rail of the bracket. This spring is compressed for mounting and un-mounting by applying downward force.




Mounting




Un-mounting

# CHAPTER 3. INTRODUCTION TO CLI

## 3.1 General Introduction

The **IFS/IGS** Series of industrial Ethernet switches provide a number of configuration/management methods. The first and very basic is serial console access. This method is also called out-of-band management and is only available when a terminal or administrator PC can be physically connected to the local IFS/IGS Series switch at the CONSOLE port using RJ45 to RS-232 console cable. Accessing the switch via CONSOLE port allows the user to use Command Line Interface (CLI) to manage and configure the device. The out-of-band management is relatively useful when you lose the network connection to the device.

The out-of-band management via console access, using a command line (CLI), is familiar to most network engineers. For engineers that are not comfortable using CLI, this device can also be managed using any standard Web Browser in a more user friendly 'point-and-click' method. Therefore, in most configuration scenarios, the console will only be used to initially configure the IFS/IGS IP address, so that the device may be accessed via the other methods which require working TCP/IP.

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

## 3.2 CONSOLE Operation

Using the provided accessory cable, connect the IFS/IGS "CONSOLE" port (RJ-45) to the PC terminal communications port (DB9). Run any terminal emulation program (HyperTerminal, PuTTY, TeraTerm Pro, etc.) and configure the communication parameters as follows:

Speed: 115,200
Data: 8 bits
Parity: none
Stop bits: 1
Flow Control: None
From a cold start, the following screen will be displayed. At the "Username" prompt, **enter 'admin' with no password**.

```
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.
Platform: VCore-III (MIPS32 24KEc) JAGUAR
RAM: 0x80000000-0x88000000 [0x80021798-0x87fe0000 available]
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
== Executing boot script in 2.000 seconds - enter ^C to abort
RedBoot> fi lo -a -f managed
RedBoot> go
Press ENTER to get started
Username: admin
Password:
```

## 3.3 CLI Modes

The Command Line Interface (CLI) of IFS/IGS series 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 |

## 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:<br>1. If there are more than two options available, a curly bracket can be used to | { { <address> <netmask> } \| { dhcp [ fallback <fallback_address> <fallback_netmask> [ timeout <fallback_timeout> ] ] } } | At least specify one option to complete the command. |

| | | | |
|---|---|---|---|
| | separate them.<br>2. The uter curly bracket means that this is a must parameter. At leaset one value should be specified. | | |
| \| (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
Vlan Address            Method   Status
---- -------------------- -------- ------
   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 1~3 & Port 5’s Config Interface mode.

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

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

### 3.6.3 Save Configurations

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

### 3.6.4 Restart the Device

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

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

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

Press ENTER to get started
```

### 3.6.5 Load Factory Defaults

Load factory default settings

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

Load factory defaults but keep IP settings

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

### 3.6.6 Show System and Software Information

```
#  show version

MEMORY              : Total=85390 KBytes, Free=67087 KBytes, Max=67085 KBytes
MAC Address         : 00-02-ab-00-00-01
Previous Restart    : Cold

System Contact      :
System Name         :
System Location     :
System Time         : 2015-01-01T00:28:35+00:00
System Uptime       : 00:28:39

------------------
SID : 1
------------------
```

```
Product              : IGS-803SM-8PH24 Gigabit Ethernet PoE Switch
Software Version     : "1.100"
Build Date           : 2015-04-17T09:22:35+08:00
```

### 3.6.7 Show SFP Information

```
# show sfp

17
----------
Vendor Name            : CTC UNION
Vendor Part Number     : SFS-7020-WA-DDI
Fiber Type             : Single
Wave Length            : 1310 nm
Wave Length 2          : 1550 nm
Link Length            : 20 km
TX Power               : -6 dBm
RX Power               : -37 dBm
RX Sensitivity         : -23 dBm
Temperature            : 28 degree C

18
----------
Vendor Name            : CTC UNION
Vendor Part Number     : SFS-7020-WB-DDI
Fiber Type             : Single
Wave Length            : 1550 nm
Wave Length 2          : 1310 nm
Link Length            : 20 km
TX Power               : -6 dBm
RX Power               : -37 dBm
RX Sensitivity         : -23 dBm
Temperature            : 25 degree C

19
----------
No SFP Module
#
```

### 3.6.8 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
```

### *3.6.9 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 1/1-5
  exit
  interface GigabitEthernet 1/1-3,5,7
  flowcontrol on
  exit
  show interface * status
  disable
  show clock detail
  show dot1x
  show history
```

### *3.6.10 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?'.)
```

### *3.6.11 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 lldp statistics*

**Syntax:** > clear lldp statistics

**Explanation:** Clear LLDP statistics.

### *3.7.3 > 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.

### 3.7.4 > enable

**Syntax:** > enable [ <new_priv> ]

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

**Explanation:** Enter the Exec mode.

### 3.7.5 > exit

**Syntax:** > exit

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

### 3.7.6 > help

**Syntax:** > help

**Explanation:** Provide help messages.

### 3.7.7 > logout

**Syntax:** > logout

**Explanation:** Logout the Command Line Interface.

### 3.7.8 > 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.

### 3.7.9 > ping ipv6

**Syntax:** > ping ipv6 <v_ipv6_addr> [ repeat <count> ] [ size <size> ] [ interval <seconds> ]

<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.

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

### 3.7.10 > traceroute

**Syntax:** > traceRoute ip <v_ip_addr> [ maxTTL <maxttl> ] [ waittime <waittime> ]

**Parameters:**

<v_ip_addr>: Specify the IP address of the destination host.

[ maxTTL <maxttl> ]: Specify the maximum number of hops that the system will trace.

[ waittime <waittime> ]: Specify how long the system will wait for a reply.

**Explanation:** Trace the the path of a packet to reach the specified IP or host.

### 3.7.11 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 dot1x statistics

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

**Parameter:**

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

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

### 3.8.4 # clear erps

**Syntax:** # clear erps [ <groups> ] statistics

**Parameter:**

[ <groups> ]: Specify the ERPS group that you want to clear.

**Explanation:** Clear (the specified group's) ERPS statistics.

### 3.8.5 # clear ip arp

**Syntax:** # clear ip arp

**Explanation:** Clear ARP cache.

### 3.8.6 # clear ip dhcp detailed statistics

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

**Explanation:** ClearIP  DHCP statistics.

**Parameter:**

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

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

### 3.8.7 # clear ip dhcp server binding <ip>

**Syntax:** # clear ip dhcp server binding <ip>

**Parameter:**

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

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

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

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

**Parameter:**

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

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

### 3.8.9 # clear ip dhcp server statistics

**Syntax:** # clear ip dhcp server statistics

**Explanation:** Clear DHCP server statistics.

### 3.8.10 # clear ip dhcp relay statistics

**Syntax:** # clear ip dhcp relay statistics

**Explanation:** Clear IP DHCP Relay statistics.

### 3.8.11 # clear ip dhcp snooping statistics

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

**Explanation:** Clear IP DHCP Snooping statistics.

### 3.8.12 # clear ip igmp snooping

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

**Explanation:** Clear IP IGMP Snooping statistics.

### 3.8.13 # clear ip statistics

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

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

### 3.8.14# clear ipv6 mld snooping

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

**Explanation:** Clear statistics for IPv6 MLD Snooping.

### 3.8.15# clear ipv6 neighbors

**Syntax:** # clear ipv6 neighbors

**Explanation:** Clear the table for IPv6 neighbors.

### 3.8.16 # 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.

### 3.8.17 # clear lacp statistics

**Syntax:** # clear lacp statistics

**Explanation:** Clear LACP statistics.

### 3.8.18 # clear lldp statistics

**Syntax:** # clear lldp statistics

**Explanation:** Clear LLDP statistics.

### 3.8.19 # clear logging

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

**Explanation:** Clear specific syslog events.

### 3.8.20 # clear mac address-table

**Syntax:** # clear mac address-table

**Explanation:** Clear MAC address table.

### *3.8.21 # clear mep*

**Syntax:** # clear mep <inst> { lm | dm | tst }

**Explanation:** Clear a specific instance MEP information.

### *3.8.22 # clear mvr*

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

**Explanation:** Clear MVR statistics.

### *3.8.23 # 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.

### *3.8.24 # clear statistics*

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

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

### *3.8.25 # config terminal*

**Syntax:** # config terminal

**Explanation:** Enter the Global Config mode.

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

### *3.8.26 # 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.
```

### *3.8.27 # 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.
```

### *3.8.28 # 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.
```

### 3.8.29 # disable & # enable

**Explanation:** Return to user mode or enter exec mode.

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

### 3.8.30 # dot1x

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

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

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

**Explanation:** To initialize dot1x function in an interface immediately.

### 3.8.31 # erps

**Syntax:** # erps <group> command {clear | force | manual} {port0 | port1}

**Explanation:** Configure ERPS instance.

**Parameters:**

<group: 1-64>: Specify a group number between 1~64.

{clear | force | manual}: Specify an action.

{port0 | port1}: Specify port0 (east) or port1 (west) that applies to this command.

### 3.8.32 # firmware swap

**Syntax:** # firmware swap

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

### 3.8.33 # firmware upgrade

**Syntax:** # firmware upgrade <TFTPServer_path_file : word>

<TFTPServer_path_file : word>: Specify the TFTP server IP address and firmware filename.

**Explanation:** Upgrade the firmware image.

### 3.8.34 # 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.

### 3.8.35 # more

**Syntax:** # more <path>

<path>: Specify the filename.

**Explanation:** Display file in Flash or in TFTP server.

### 3.8.36 # 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 or IPv6 address for ping test.

### 3.8.37 # ping ipv6

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

< v_ipv6_addr >: Specify the IPv4 address or 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.

### *3.8.38 # ptp*

**Syntax:** # ptp <clockinst> local-clock { update }

**Explanation:** Update PTP local clock status.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

{ update }: Update the current PTP status.

### *3.8.39 # reload cold*

**Syntax:** # reload cold

**Explanation:** Perform a cold reload on the system.

### *3.8.40 # reload defaults*

**Syntax:** # reload defaults [keep-ip]

**Explanation:** Restore the device to factory default settings.

**Parameters:**

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

### *3.8.41 # 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.

### *3.8.42 # terminal editing*

**Syntax:** # terminal editing

**Explanation:** Enable command line editing.

**Show: >** show terminal
**#** show terminal

**Negation:** # no terminal editing

### *3.8.43 # terminal exec-timeout*

**Syntax:** # terminal exec-timeout <0-1440> [<0-3600>]

**Parameters:**

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

[<0-3600>]: Specify the timeout value in seconds.

**Explanation:** Set up terminal timeout value.

**Show: >** show terminal
**#** show terminal

**Negation:** # no terminal exec-timeout

### *3.8.44 # 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

### *3.8.45 # 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

### *3.8.46 # 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

### *3.8.47 # traceroute ip*

**Syntax:** # traceRoute ip <v_ip_addr> [ maxTTL <maxttl> ] [ waittime <waittime> ]

**Parameters:**

<v_ip_addr>: Specify the IP address of the destination host.

[ maxTTL <maxttl> ]: Specify the maximum number of hops that the system will trace.

[ waittime <waittime> ]: Specify how long the system will wait for a reply.

**Explanation:** Trace the path of a packet to reach the specified IP or host.

### *3.8.48 # 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.

### *3.8.49 # show interface ( <port_type> [ <v_port_type_list> ] ) veriphy*

**Syntax:** # show interface ( <port_type> [ <v_port_type_list> ] ) veriphy

**Explanation:** Issuing this command will run the VeriPHY™ Cable Diagnostics for 10/100 and 1G copper ports. This will take approximately 5 seconds per port. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table.

Note that VeriPHY is only accurate for cables of length 7 - 140 meters.
10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

**Parameters:**

( <port_type> [ <v_port_type_list> ] ): Specify the port type and port number that apply to this Veriphy diagnostics test.

### *3.8.50 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 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

## 3.9.2 (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:** (config)# access-list ace <AceId : 1-256> [ action {deny | filter | permit}] [ dmac-type {any| broadcast | multicast | unicast } ] [frame-type {any| arp|etype|ipv4|ipv4-icmp|ipv4-tcp|ipv4-udp|ipv6|ipv6-icmp|ipv6-tcp|ipv6-udp} ] [ingress {any | interface <PORT_TYPE> }] [logging] [mirror] [next { <AceId : 1-256>|last}] [policy <PolicyId : 0-255>] [rate-limiter {<RateLimiterId : 1-16>|disable}] [redirect {disable| interface <PORT_TYPE>}] [shutdown] [tag {any|tagged|untagged}] [tag-priority {0-1| 0-3| 2-3| 4-5| 4-7| 6-7| <TagPriority : 0-7>|any}] [vid { <Vid : 1-4095>|any}]

**Explanation:** Configure an access control list.

**Parameters:**

<AceId : 1-256>: 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 : 0-255>]: Specify the policy ID.

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

[redirect {disable| interface <PORT_TYPE>}]: Redirect frames to a specific port 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 ace update*

**Syntax:** (config)# access-list ace update <AceId : 1-256> [ action {deny | filter | permit}] [ dmac-type {any| broadcast | multicast | unicast } ] [frame-type {any| arp|etype|ipv4|ipv4-icmp|ipv4-tcp|ipv4-udp|ipv6|ipv6-icmp|ipv6-tcp|ipv6-udp} ] [ingress {any | interface <PORT_TYPE> }] [logging] [mirror] [next { <AceId : 1-256>|last}] [policy <PolicyId : 0-255>] [rate-limiter {<RateLimiterId : 1-16>|disable}] [redirect {disable| interface <PORT_TYPE>}] [shutdown] [tag {any|tagged|untagged}] [tag-priority {0-1| 0-3| 2-3| 4-5| 4-7| 6-7| <TagPriority : 0-7>|any}] [vid { <Vid : 1-4095>|any}]

**Explanation:** Update an access control list.

**Parameters:**

<AceId : 1-256>: 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 : 0-255>]: Specify the policy ID.

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

[redirect {disable| interface <PORT_TYPE>}]: Redirect frames to a specific port 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>

### *3.9.3.3 (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>]

### *3.9.3.4 (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> ] ) ] ]

### *3.9.3.5 (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

### *3.9.3.6 (config-if)# access-list mirror*

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

**Explanation:** Enable a specific port's frames to be mirrored to a destination port.

**Show:** # show access-list [ interface [ ( <port_type> [ <v_port_type_list> ] ) ] ]

**Negation:** (config-if)# no access-list mirror

### *3.9.3.7 (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

### *3.9.3.8 (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

#### 3.9.3.9 (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

#### 3.9.3.10 (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

#### 3.9.3.11 (config-if)# access-list { redirect | port-copy }

**Syntax:** (config-if)# access-list { redirect | port-copy } interface { <port_type> <port_type_id> | ( <port_type> [ <port_type_list> ] ) }

**Parameters:**

{ redirect | port-copy }: Redirect or copy this port's frames to the specified port.

interface { <port_type> <port_type_id> | ( <port_type> [ <port_type_list> ] ) }: Specify the redirect or copy port type and port list.

**Explanation:** Redirect or copy this port's frames to the specified port.

**Negation:** (config-if)# no access-list { redirect | port-copy }

### 3.9.4 (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 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
```

### 3.9.8 (config)# dot1x

#### 3.9.8.1 (config)# dot1x system-auth-control

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

**Explanation:** To enable 802.1x service.

**Parameters:** None.

**Example:** Enable 802.1x service.

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

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

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

#### 3.9.8.2 (config)# dot1x re-authentication

**Syntax:** (config)# dot1x re-authentication

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

**Example:** Enable re-authentication function.

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

**Negation:** (config)# no dot1x re-authentication

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

### *3.9.8.3 (config)# dot1x authentication timer re-authenticate*

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

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

**Parameters:**

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

**Example:** Set re-authentication timer to 100.

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

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

### *3.9.8.4 (config)# dot1x timeout tx-period*

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

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

**Parameters:**

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

**Example:** Set EAPOL timeout to 30 seconds.

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

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

### 3.9.8.5 (config)#dot1x authentication timer inactivity

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

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

**Parameters:**

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

**Example:** Set the aging time to 300 seconds.

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

**Negation:** (config)# no dot1x authentication timer inactivity

### 3.9.8.6 (config)# dot1x timeout quiet-period

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

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

**Parameters:**

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

**Example:** Set hold time to 30 seconds.

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

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

### 3.9.8.7 (config)# dot1x feature

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

**Explanation:** Enable the specified feature.

**Parameters:**

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

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

[radius-qos]: Enable RADIUS assigned QoS.

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

**Example:** Enable guest VLAN service.

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

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

### *3.9.8.8 (config)# dot1x guest-vlan*

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

**Explanation:** Configure a guest VLAN ID.

**Parameters:**

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

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

### *3.9.8.9 (config)# dot1x guest-vlan supplicant*

**Syntax:** (config)# dot1x guest-vlan supplicant

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

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

### *3.9.8.10 (config)# dot1x max-requth-req*

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

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

**Parameters:**

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

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

### 3.9.8.11 (config-if)# dot1x port-control

**Syntax:** (config-if)# dot1x port-control { force-authorized | force-unauthorized | auto | single | multi | mac-based }

**Parameters:**

{ force-authorized | force-unauthorized | auto | single | multi | mac-based }: Specify one of the authentication modes on the selected interfaces. This setting works only when NAS is globally enabled. The following modes are available:

**force-authorized:** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

**force unauthorized:** In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

**auto (Port-Based 802.1X):** This mode requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.

**single (802.1X):** In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the “Port Security” module is used to secure a supplicant's MAC address once successfully authenticated.

**multi (802.1X):** In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the “Port Security” module.

**mac-based:** Unlike port-based 802.1X, MAC-based authentication do not transmit or receive EAPOL frames. In MAC-based authentication, the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

**Example:** Set Gigabit Ethernt port 1-10’s admin state to “auto”

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x port-control auto
```

**Negation:** (config-if)# no dot1x port-control

### 3.9.8.12 (config-if)# dot1x guest-vlan

**Syntax:** (config-if)# dot1x guest-vlan

**Explanation:** Enable the guest VLAN on the selected interfaces.

**Parameters:** None.

**Example:** Enable guest VLAN on port 1-10.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x guest-vlan
```

**Negation:** (config-if)# no dot1x guest-vlan

### 3.9.8.13 (config-if)# dot1x radius-qos

**Syntax:** (config-if)# dot1x radius-qos

**Explanation:** Enable RADIUS Assigned QoS on the selected interfaces.

**Parameters:** None.

**Example:** Enable RADIUS Assigned QoS on port 1-10.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x radius-qos
```

**Negation:** (config-if)# no dot1x radius-qos

### 3.9.8.14 (config-if)# dot1x radius-vlan

**Syntax:** (config-if)# dot1x radius-vlan

**Explanation:** Enable RADIUS Assigned VLAN on the selected interfaces.

**Parameters:** None.

**Example:** Enable RADIUS Assigned VLAN on port 1-10.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x radius-vlan
```

**Negation:** (config-if)# no dot1x radius-vlan

#### 3.9.8.15 (config-if)# dot1x re-authenticate

**Syntax:** (config-if)# dot1x re-authenticate

**Explanation:** Schedules reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. This command only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

**Show:** > show dot1x statistics { eapol | radius | all } [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show dot1x statistics { eapol | radius | all } [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### 3.9.9 (config-if)# duplex

**Syntax:** (config-if)# duplex { half | full | auto [ half | full ] }

**Explanation:** Configure port's duplex mode.

**Parameters:**

{ half | full | auto [ half | full ] }: Specify the duplex mode for this specific interface.

**Example:** Set port 1's duplex mode to auto.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# duplex auto
```

**Negation:** (config-if)# no duplex

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

### 3.9.10 (config)# enable

#### 3.9.10.1 (config)# enable password

**Syntax:** (config)# enable password <password>

**Explanation:** Configure enable password.

**Parameters:**

password <password>: Specify the enable mode password.

### 3.9.10.2 (config)# enable password level

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

**Explanation:** Configure enable password and privilege level.

**Parameters:**

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

<password>: Specify the enable mode password.

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

### 3.9.10.3 (config)# enable secret

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

**Parameters:**

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

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

<password>: Specify the enable mode password.

**Explanation:** Configure enable secret password and privilege level.

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

## 3.9.11 (config)# erps

### 3.9.11.1 (config)# erps <group> guard <guard_time_ms>

**Syntax:** (config)# erps <group> guard <guard_time_ms>

**Explanation:** Configure the specified group's guard time.

**Parameters:**

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

<guard_time_ms: 10-2000>: Specify the guard time. The allowed range is 10 to 2000 ms.

**Negation:** (config)# no erps <group> guard

**Negation: #** show erps [ <groups> ] [ detail | statistics ]

### 3.9.11.2 (config)# erps <group> holdoff <holdoff_time_ms>

**Syntax:** (config)# erps <group> holdoff <holdoff_time_ms>

**Parameters:**

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

<holdoff_time_ms: 0-10000>: Specify the holdoff time. The allowed range is 0 to 10000 ms.

**Explanation:** Configure the specified group's holdoff time.

**Negation:** (config)# no erps <group> holdoff

**Negation: #** show erps [ <groups> ] [ detail | statistics ]

### 3.9.11.3 (config)# erps <group> major port0 interface port1 interface <port_type> <port1> [ interconnect ]

**Syntax:** (config)# erps <group> major port0 interface <port_type> <port0> port1 interface <port_type> <port1>
[ interconnect ]

**Explanation:** Create an ERPS instance.

**Parameters:**

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

<port_type> <port0>: Specify Port 0's port type and port number. Port 0 is also known as E port (East port) which is used by some of the other vendors.

<port_type> <port1>: Specify Port 1's port type and port number. Port 1 is also known as W port (West port) which is used by some of the other vendors. When this port is interconnected with the other sub-ring, "0" is used in this field to indicate that no west port is associated with this instance.

[ interconnect ]: Specify this parameter if this is an interconnected node for this instance.

**Show: #** show erps [ <groups> ] [ detail | statistics ]

### 3.9.11.4 (config)# erps <group> mep port0 sf <p0_sf> aps <p0_aps> port1 sf <p1_sf> aps <p1_aps>

**Syntax:** (config)# erps <group> mep port0 sf <p0_sf> aps <p0_aps> port1 sf <p1_sf> aps <p1_aps>

**Explanation:** Configure the specified group's MEP & APS settings.

**Parameters:**

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

<p0_sf>: This is also known as East Signal Fail APS MEP. Assign the East Signal Fail reporting MEP in this field.

<p0_aps>: Specify the East APS PDU handling MEP.

<p1_sf>: This is also known as West Signal Fail APS MEP. When interconnected with the other sub-ring, “0” is used in this field to indicate that no west SF MEP is associated with this instance.  Assign the West Signal Fail reporting MEP in this field.

<p1_aps>:  Specify the West APS PDU handling MEP. When interconnected with the other sub-ring, “0” is used in this field to indicate that no west APS MEP is associated with this instance.

**Negation:** (config)# no erps <group> mep

**Show: #** show erps [ <groups> ] [ detail | statistics ]

### *3.9.11.5 (config)# erps <group> revertive <wtr_time_minutes>*

**Syntax:** (config)# erps <group> revertive <wtr_time_minutes>

**Explanation:** Configure the Wait-to-Restore timer in revertive mode.

**Parameters:**

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

<wtr_time_minutes>: Specify Wait-to-Restore timer in minutes. The allowed range is from 1 to 12 minutes.

**Negation:** (config)# no erps <group> revertive

**Show: #** show erps [ <groups> ] [ detail | statistics ]

### *3.9.11.6 (config)# erps <group> rpl { owner | neighbor } { port0 | port1 }*

**Syntax:** (config)# erps <group> rpl { owner | neighbor } { port0 | port1 }

**Explanation:** Specify the Ethernet ring port on the local node as the RPL (Ring Protection Link) owner or neighbor.

**Parameters:**

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

{ owner | neighbor }: Specify the ring port is a owner or neighbor. RPL (Ring Protection Link) is responsible for blocking traffic over the RPL so that no loops are formed in the Ethernet traffic.

{ port0 | port1 }: Specify the port applies to this rule.

**Negation:** (config)# no erps <group> rpl

**Show: #** show erps [ <groups> ] [ detail | statistics ]

### *3.9.11.7 (config)# erps <group> sub port0 interface <port_type> <port0> { { port1 interface <port_type> <port1> } | { interconnect <major_ring_id> [ virtual-channel ] } }*

**Syntax:** (config)# erps <group> sub port0 interface <port_type> <port0> { { port1 interface <port_type> <port1> } | { interconnect <major_ring_id> [ virtual-channel ] } }

**Explanation:** Create a profile and configure the Sub ERPS interface port 0, port 1.

**Parameters:**

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

<port_type> <port0>: Specify sub port's port type and port number.

{ { port1 interface <port_type> <port1> } | { interconnect <major_ring_id> [ virtual-channel ] } }: Specify Port 1's port type and port numbr or specify major ring's group ID.

**Negation:** (config)# no erps <group>

**Show: #** show erps [ <groups> ] [ detail | statistics ]

### *3.9.11.8 (config)# erps <group> topology-change propagate*

**Syntax:** (config)# erps <group> topology-change propagate

**Parameters:**

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

**Explanation:** Allow topology change notification propagation.

**Negation:** (config)# no erps <group> topology-change propagate

**Show: #** show erps [ <groups> ] [ detail | statistics ]

### *3.9.11.9 (config)# erps <group> version { 1 | 2 }*

**Syntax:** (config)# erps <group> version { 1 | 2 }

**Explanation:** Configure ERPS version for a specific profile.

**Parameters:**

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

{ 1 | 2 }: Specify ERPS version 1 or 2.

**Negation:** (config)# no erps <group> version

**Show: #** show erps [ <groups> ] [ detail | statistics ]

#### 3.9.11.10 (config)# erps <group> vlan { none | [ add | remove ] <vlans> }

**Syntax:** (config)# erps <group> vlan { none | [ add | remove ] <vlans> }

**Explanation:** Configure VLANs for a specific ERPS profile.

**Parameters:**

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

{ none | [ add | remove ] <vlans> } : Specify an option.

**none:** Do not include any VLANs.

**[ add | remove ] <vlans>:** Add or remove a specific VLAN.

**Negation:** (config)# no erps <group> vlan

**Show: #** show erps [ <groups> ] [ detail | statistics ]

### 3.9.12 (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

### 3.9.13 (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

## 3.9.14 (config)# green-ethernet

### 3.9.14.1 (config)# green-ethernet led interval

**Syntax:** (config)# green-ethernet led interval <v_0_to_24> intensity <v_0_to_100>

**Explanation:** Configure the LED time interval and LED light intensity to reduce power consumption.

**Parameters:**

led interval <v_0_to_24>: Specify LED time interval. The first value is the starting time. The second one is the ending time. The allowed value is from 0 to 24.

intensity <v_0_to_100>: LED intensity. The value is from 0 to 100.

**Example:** LED intensity reduces to 80% during 9:00 and 18:00.

```
# config t
(config)# green-ethernet led interval 9-18 intensity 80
```

**Negation:** (config)# no green-ethernet led interval <0~24>

### 3.9.14.2 (config)# green-ethernet led on-event

**Syntax:** (config)# green-ethernet led on-event { [ link-change <v_0_to_65535> ] [ error ]}

**Explanation:** The switch will bring LED intensity to 100% for the specified period in the event of any error (such as link down).

**Parameters:**

[ link-change <v_0_to_65535> ]: Specify how long LED intensity 100% lasts when errors occur. The allowed value is from 0 to 65535.

[error]: Bring LED intensity to 100% in the event of errors.

**Example:** Bring LED intensity to 100% for 10 minutes when errors occur.

```
# config t
(config)# green-ethernet led on-event link-change 600 error
```

**Negation:** (config)# no green-ethernet led on-event [ link-change ] [ error ]

### 3.9.14.3 (config)# green-ethernet eee optimize-for-power

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

**Explanation:** Enables the EEE function for this switch.

**Parameters:** None

**Example:** Enable EEE function for optimized power.

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

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

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

### *3.9.14.4 (config-if)# green-ethernet eee*

**Syntax:** (config-if)# green-ethernet eee

**Explanation:** Enable EEE (Energy-Efficient Ethernet) on the selected interface.

**Negation:** (config-if)# no green-ethernet eee

**Show:** # show green-ethernet eee [ interface ( <port_type> [ <port_list> ] ) ]

### *3.9.14.5 (config-if)# green-ethernet urgent-queues*

**Syntax:** (config-if)# green-ethernet eee urgent-queues [ <urgent_queue_range_list> ]

**Explanation:** It is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

**Parameters:**

[ <urgent_queue_range_list> ]: Specify urgent queue range. The allowed range is from 1 to 8.

**Negation:** (config-if)# no green-ethernet eee urgent-queues [ <urgent_queue_range_list> ]

### *3.9.14.6 (config-if)# green-ethernet energy-detect*

**Syntax:** (config-if)# green-ethernet energy-detect

**Explanation:** Enable power saving function for this specific interface when there is no link partner.

**Negation:** (config-if)# no green-ethernet energy-detect

**Show:** # show green-ethernet energy-detect [ interface ( <port_type> [ <port_list> ] ) ]

### 3.9.14.7 (config-if)# green-ethernet short-reach

**Syntax:** (config-if)# green-ethernet short-reach

**Explanation:** Enable power saving for ports which is connect to link partner with short cable.

**Negation:** (config-if)# no green-ethernet short-reach

**Show:** # show green-ethernet short-reach [ interface ( <port_type> [ <port_list> ] ) ]

## 3.9.15 (config)# gvrp

### 3.9.15.1 (config)# gvrp

**Syntax:** (config)# gvrp

**Explanation:** Globally enable GVRP function.

**Parameters:** None.

**Example:** Globally enable GVRP function.

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

**Negation:** (config)# no gvrp

### 3.9.15.2 (config)# gvrp max-vlans

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

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

**Parameters:**

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

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

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

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

### 3.9.15.3 (config)# gvrp time

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

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

**Parameters:**

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

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

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

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

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

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

### 3.9.15.4 (config-if)# gvrp

**Syntax:** (config-if)# gvrp

**Explanation:** Enable GVRP function on the specified interfaces.

**Parameters:** None.

**Example:** Enable GVRP function on port 1~5.

```
# config t
(config)# interface GigabitEthernet 1/1-5
(config-if)# gvrp
(config-if)#
```

**Negation:** (config-if)# no gvrp

## 3.9.16 (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

### 3.9.17 (config)# interface

#### 3.9.17.1(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> ] ) }

#### 3.9.17.2 (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)#
```

### 3.9.18 (config)# ip

#### 3.9.18.1 (config)# ip arp inspection

**Syntax:** (config)# ip arp inspection

**Explanation:** Enable ARP inspection function.

**Negation:** (config)# no ip arp inspection

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

**Clear:** # clear ip arp

#### 3.9.18.2 (config)# ip arp inspection entry interface

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

**Explanation:** Create ARP static entry.

**Parameters:**

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

<vlan_var>: Specify a configured VLAN ID.

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

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

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

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

**Clear:** # clear ip arp

### 3.9.18.3 (config)# ip arp inspection translate

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

**Explanation:** Translate the dynamic entry to static one.

**Parameters:**

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

<vlan_var>: Specify a configured VLAN ID.

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

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

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

### 3.9.18.4 (config)# ip arp inspection vlan

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

**Explanation:** Specify ARP inspection is enabled on which VLAN.

**Parameters:**

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

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

**Show:** < show ip arp
# show ip arp

**Clear:** # clear ip arp

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

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

**Explanation:** Enable log function.

**Parameters:**

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

**Deny:** Log denied entries.

**Permit:** Log permitted entries.

**All:** Log all entries.

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

**Show:** < show ip arp
# show ip arp

**Clear:** # clear ip arp

### 3.9.18.6 (config)# ip dhcp relay

**Syntax:** (config)# ip dhcp relay

**Explanation:** Enable DHCP relay function.

**Example:** Enable DHCP relay function.

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

**Negation:** (config)#  no ip dhcp relay

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

**Clear:** # clear ip dhcp relay statistics

### 3.9.18.7 (config)# ip dhcp relay information option

**Syntax:** (config)# ip dhcp relay information option

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

**Example:** Enable DHCP Relay option 82 function

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

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

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

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

**Explanation:** Specify DHCP Relay information policy action.

**Parameters:**

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

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

**keep:** Keep the client's DHCP information.

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

**Example:** Keep the client's DHCP information.

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

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

### 3.9.18.9 (config)# ip dhcp snooping

**Syntax:** (config)# ip dhcp snooping

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

**Example:** Enable DHCP snooping function.

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

**Negation:** (config)#  no ip dhcp snooping

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

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

### 3.9.18.10 (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

### 3.9.18.11 (config)# ip helper-address

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

**Explanation:** Configure DHCP Relay server IPv4 address.

**Parameters:**

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

**Negation:** (config)# no ip helper-address

### 3.9.18.12 (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

### 3.9.18.13 (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

### 3.9.18.14 (config)# ip igmp host-proxy

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

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

**Parameters:**

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

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

**Show:** # show ip igmp snooping detail

### 3.9.18.15 (config)# ip igmp snooping

**Syntax:** (config)# ip igmp snooping

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

**Negation:** (config)# no ip igmp snooping

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

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

### 3.9.18.16 (config)# ip igmp snooping vlan

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

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

**Parameters:**

<v_vlan_list>: Specify valid IGMP VLANs.

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

**Show:** # show ip igmp snooping

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

### 3.9.18.17 (config)# ip igmp ssm-range

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

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

**Parameters:**

<v_ipv4_mcast>: Specify valid IPv4 multicast address.

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

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

### 3.9.18.18 (config)# ip igmp unknown-flooding

**Syntax:** (config)# ip igmp unknown-flooding

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

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

### 3.9.18.19 (config)# ip name-server

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

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

**Parameters:**

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

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

**Negation:** (config)# no ip name-server

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

### 3.9.18.20 (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

### 3.9.18.21 (config)# ip routing

**Syntax:** (config)# ip routing

**Explanation:** Enable IPv4 and IPv6 routing.

**Example:** Enable IPv4 and IPv6 routing.

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

**Negation:** (config)# no ip routing

**Show:** > show ip route
> show ipv6 route [interface vlan <vlan_list>]
# show ip route
# show ipv6 route [interface vlan<vlan_list>]

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

### 3.9.18.22 (config)# ip source binding interface

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

**Explanation:** Create a static entry.

**Parameters:**

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

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

<ipv4_var>: Specify a valid IPv4 address.

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

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

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

### *3.9.18.23 (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.*

### *3.9.18.24 (config)# ip verify source*

**Syntax:** (config)# ip verify source

**Explanation:** Enable IP source guard function.

**Negation:** (config)# no ip verify source

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

### *3.9.18.25 (config)# ip verify source translate*

**Syntax:** (config)# ip verify source translate

**Explanation:** Translate Dynamic entries to Static ones.

### 3.9.18.26 (config-if)# ip arp inspection check-vlan

**Syntax:** (config-if)# ip arp inspection check-vlan

**Explanation:** Enable check vlan function.

**Negation:** (config-if)# no ip arp inspection check-vlan

### 3.9.18.27 (config-if)# ip arp inspection logging

**Syntax:** (config-if)# ip arp inspection logging { deny | permit | all }

**Explanation:** Enable log function on a specific interface.

**Parameters:**

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

**Deny:** Log denied entries.

**Permit:** Log permitted entries.

**All:** Log all entries.

**Negation:** (config-if)# no ip arp inspection logging

### 3.9.18.28 (config-if)# ip arp inspection trust

**Syntax:** (config-if)# ip arp inspection trust

**Explanation:** Enable trust state on the selected interfaces.

**Negation:** (config-if)# no ip arp inspection trust

### 3.9.18.29 (config-if)# ip dhcp snooping trust

**Syntax:** (config-if)# ip dhcp snooping trust

**Explanation:** Set this interface to DHCP Snooping trusted port.

**Negation:** (config-if)# no ip dhcp snooping trust

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

### 3.9.18.30 (config-if)# ip igmp snooping filter

**Syntax:** (config-if)# ip igmp snooping filter <profile_name>

**Explanation:** Use this command to filter specific multicast traffic on a per port basis.

**Parameters:**

<profile_name>: Specify the configured multicast groups that are denied on a port. When a certain multicast group is selected on a port, IGMP join reports received on a port are dropped.

**Negation:** (config-if)# no ip igmp snooping filter

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

### 3.9.18.31 (config-if)# ip igmp snooping immediate-leave

**Syntax:** (config-if)# ip igmp snooping immediate-leave

**Explanation:** Enable fast leave function on a specific port. When a leave packet is received, the switch immediately removes it from a multicast service without sending an IGMP group-specific (GS) query to that interface.

**Negation:** (config-if)# no ip igmp snooping immediate-leave

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

### 3.9.18.32 (config-if)# ip igmp snooping max-groups

**Syntax:** (config-if)# ip igmp snooping max-groups <throttling>

**Explanation:** Specify the maximum number of multicast groups that a port can join at the same time.

**Parameters:**

<throttling>: This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new IGMP join reports will be dropped. By default, unlimited is selected. The allowed range can be specified is 1 to 10.

**Negation:** (config-if)# no ip igmp snooping max-groups

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

### *3.9.18.33 (config-if)# ip igmp snooping mrouter*

**Syntax:** (config-if)# ip igmp snooping mrouter

**Explanation:** Set this interface to Router port. If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

**Negation:** (config-if)# no ip igmp snooping mrouter

**Show:** > show ip igmp snooping mrouter [ detail ]
# show ip igmp snooping mrouter [ detail ]

### *3.9.18.34 (config-if)# ip verify source*

**Syntax:** (config-if)# ip verify source

**Explanation:** Enable IP Source Guard on this interface

**Negation:** (config-if)# no ip verify source

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

### *3.9.18.35 (config-if)# ip verify source limit*

**Syntax:** (config-if)# ip verify source limit <0-2>

**Explanation:** Specify the maximum number of dynamic clients that can be learned on a port. The available options are 0, 1, 2. If the port mode is enabled and the maximum number of dynamic clients is equal 0, the switch will only forward IP packets that are matched in static entries for a given port.

**Parameters:**

<0-2>: Specify the maximum number of dynamic clients that can be learned on a port.

**Negation:** (config-if)# no ip verify source limit

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

### *3.9.18.36 (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

### 3.9.18.37 (config-if-vlan)# ip igmp snooping

**Syntax:** (config-if-vlan)# ip igmp snooping

**Explanation:** Eanble IGMP Snooping on this specific VLAN.

**Negation:** (config-if-vlan)# no ip igmp snooping

**Show:** > show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
# show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]

### 3.9.18.38 (config-if-vlan)# ip igmp snooping compatibility

**Syntax:** (config-if-vlan)# ip igmp snooping compatibility { auto | v1 | v2 | v3 }

**Explanation:** Configure IGMP Snooping version used for this specific VLAN.

**Parameters:**

{ auto | v1 | v2 | v3 }: Specify one of the IGMP Snooping options.

**auto:** Compatible with Version 1, Version 2, and Version 3.

**v1:** Compatible with IGMP version 1.

**v2:** Compatible with IGMP version 2.

**v3:** Compatible with IGMP version 3.

**Negation:** (config-if-vlan)# no ip igmp snooping compatibility

### 3.9.18.39 (config-if-vlan)# ip igmp snooping last-member-query-interval

**Syntax:** (config-if-vlan)# ip igmp snooping last-member-query-interval <ipmc_lmqi>

**Explanation:** LMQI stands for Last Member Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The allowed range is 0~31744 tenths of a second.

**Parameters:**

<ipmc_lmqi: 0-31744>: Specify LMQI (Last Member Query Interval) value.

**Negation:** (config-if-vlan)# no ip igmp snooping last-member-query-interval

### *3.9.18.40 (config-if-vlan)# ip igmp snooping priority*

**Syntax:** (config-if-vlan)# ip igmp snooping priority <cos_priority>

**Explanation:** Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0 -7.

**Parameters:**

<cos_priority: 0-7>: Specify COS for this specific VLAN. The valid range is 0 to 7.

**Negation:** (config-if-vlan)# no ip igmp snooping priority

### *3.9.18.41 (config-if-vlan)# ip igmp snooping querier address*

**Syntax:** (config-if-vlan)# ip igmp snooping querier address <v_ipv4_ucast>

**Explanation:** Specify IGMP Snooping querier IP address.

**Parameters:**

<v_ipv4_ucast>: Specify IGMP Snooping querier unicast IP address.

**Negation:** (config-if-vlan)# no ip igmp snooping querier address

### *3.9.18.42 (config-if-vlan)# ip igmp snooping querier election*

**Syntax:** (config-if-vlan)# ip igmp snooping querier election

**Explanation:** Enable IGMP Snooping querier election function.

**Negation:** (config-if-vlan)# no ip igmp snooping querier election

### *3.9.18.43 (config-if-vlan)# ip igmp snooping query-interval*

**Syntax:** (config-if-vlan)# ip igmp snooping query-interval <ipmc_qi>

**Explanation:** Specify IPMC Query interval value.

**Parameters:**

<ipmc_qi: 1-31744>: Specify IPMC Query interval value. The valid value is 1~31744.

**Negation:** (config-if-vlan)# no ip igmp snooping query-interval

### 3.9.18.44 (config-if-vlan)# ip igmp snooping query-max-response-time

**Syntax:** (config-if-vlan)# ip igmp snooping query-max-response-time <ipmc_qri>

**Explanation:** Specify IPMC Query Response time value.

**Parameters:**

<ipmc_qri>: Specify IPMC Query Response time value. The valid value is 1~31744.

**Negation:** (config-if-vlan)# no ip igmp snooping query-max-response-time

### 3.9.18.45 (config-if-vlan)# ip igmp snooping robustness-variable

**Syntax:** (config-if-vlan)# ip igmp snooping robustness-variable <ipmc_rv>

**Explanation:** The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

**Parameters:**

<ipmc_rv: 1-255>: Specify IPMC Robustness Variable value. The valid value is 1~255.

**Negation:** (config-if-vlan)# no ip igmp snooping robustness-variable

### 3.9.18.46 (config-if-vlan)# ip igmp snooping unsolicited-report-interval

**Syntax:** (config-if-vlan)# ip igmp snooping unsolicited-report-interval <ipmc_uri>

**Explanation:** The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. The allowed range for URI is 0 -31744 seconds.

**Parameters:**

<ipmc_uri: 0-31744>: Specify Unsolicited Report Interval value. The valid value is 0~31744.

**Negation:** (config-if-vlan)# no ip igmp snooping unsolicited-report-interval

### 3.9.18.47 (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 } ]

### 3.9.18.48 (config-if-vlan)# ipv6 mld snooping

**Syntax:** (config-if-vlan)# ipv6 mld snooping

**Explanation:** Eanble MLD (Multicast Listener Discovery) Snooping on this specific VLAN.

**Negation:** (config-if-vlan)# no ipv6 mld snooping

**Show:** > show ipv6 statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
# show ipv6 statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]

### 3.9.18.49 (config-if-vlan)# ipv6 mld snooping compatibility

**Syntax:** (config-if-vlan)# ipv6 mld snooping compatibility { auto | v1 | v2 }

**Explanation:** Configure MLD Snooping version used for this specific VLAN.

**Parameters:**

{ auto | v1 | v2 | v3 }: Specify one of the MLD Snooping options.

**auto:** Compatible with Version 1, Version 2.

**v1:** Compatible with MLD version 1.

**v2:** Compatible with MLD version 2.

**Negation:** (config-if-vlan)# no ipv6 mld snooping compatibility

### 3.9.18.50 (config-if-vlan)# ipv6 mld snooping last-member-query-interval

**Syntax:** (config-if-vlan)# ipv6 mld snooping last-member-query-interval <ipmc_lmqi>

**Explanation:** LMQI stands for Last Member Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The allowed range is 0~31744 tenths of a second.

**Parameters:**

<ipmc_lmqi: 0-31744>: Specify LMQI (Last Member Query Interval) value.

**Negation:** (config-if-vlan)# no ipv6 mld snooping last-member-query-interval

#### 3.9.18.51 (config-if-vlan)# ipv6 mld snooping priority <cos_priority>

**Syntax:** (config-if-vlan)# ipv6 mld snooping priority <cos_priority>

**Explanation:** Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0 -7.

**Parameters:**

<cos_priority: 0-7>: Specify COS for this specific VLAN. The valid range is 0 to 7.

**Negation:** (config-if-vlan)# no ipv6 mld snooping priority

#### 3.9.18.52 (config-if-vlan)# ipv6 mld snooping querier election

**Syntax:** (config-if-vlan)# ipv6 mld snooping querier election

**Explanation:** Enable MLD Snooping querier election function.

**Negation:** (config-if-vlan)# no ipv6 mld snooping querier election

#### 3.9.18.53 (config-if-vlan)# ipv6 mld snooping query-interval <ipmc_qi>

**Syntax:** (config-if-vlan)# ipv6 mld snooping query-interval <ipmc_qi>

**Explanation:** Specify MLD Query interval value.

**Parameters:**

<ipmc_qi: 1-31744>: Specify IPMC Query interval value. The valid value is 1~31744.

**Negation:** (config-if-vlan)# no ipv6 mld snooping query-interval

#### 3.9.18.54 (config-if-vlan)# ipv6 mld snooping query-max-response-time <ipmc_qri>

**Syntax:** (config-if-vlan)# ipv6 mld snooping query-max-response-time <ipmc_qri>

**Explanation:** Specify MLD Query Response time value.

**Parameters:**

<ipmc_qri>: Specify MLD Query Response time value. The valid value is 1~31744.

**Negation:** (config-if-vlan)# no ipv6 mld snooping query-max-response-time

#### 3.9.18.55 (config-if-vlan)# ipv6 mld snooping robustness-variable <ipmc_rv>

**Syntax:** (config-if-vlan)# ipv6 mld snooping robustness-variable <ipmc_rv>

**Explanation:** The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

**Parameters:**

<ipmc_rv: 1-255>: Specify IPMC Robustness Variable value. The valid value is 1~255.

**Negation:** (config-if-vlan)# no ipv6 mld snooping robustness-variable

#### 3.9.18.56 (config-if-vlan)# ipv6 mld snooping unsolicited-report-interval <ipmc_uri>

**Syntax:** (config-if-vlan)# ipv6 mld snooping unsolicited-report-interval <ipmc_uri>

**Explanation:** The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. The allowed range for URI is 0 -31744 seconds.

**Parameters:**

<ipmc_uri: 0-31744>: Specify Unsolicited Report Interval value. The valid value is 0~31744.

**Negation:** (config-if-vlan)# no ipv6 mld snooping unsolicited-report-interval

### 3.9.19 (config)# ipmc

#### 3.9.19.1 (config)# ipmc profile

**Syntax:** (config)# ipmc profile

**Explanation:** Enable IPMC (IP multicast) profile globally.

**Negation:** (config)# no ipmc profile

**Show: #** show ipmc profile

#### 3.9.19.2 (config)# ipmc profile <profile_name>

**Syntax:** (config)# ipmc profile <profile_name>

**Parameters:**

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

**Explanation:** Set up an IPMC profile.

**Example:** Create an IPMC profile named “goldpass”.

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

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

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

### 3.9.19.3 (config)# ipmc range

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

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

**Parameters:**

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

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

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

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

### 3.9.19.4 (config-ipmc-profile)# default range

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

**Parameters:**

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

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

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

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

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

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

### 3.9.19.5 (config-ipmc-profile)# description

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

**Parameters:**

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

**Explanation:** Specify descriptive information for the designated profile.

**Example:** Provide descriptive information for IPMC profile goldpass.

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

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

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

### 3.9.19.6 (config-ipmc-profile)# range

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

**Parameters:**

<entry_name>: Specify an entry name.

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

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

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

[ log ]: Log when matching

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

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

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

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

## 3.9.20 (config)# ipv6 mld host-proxy

### 3.9.20.1 (config)# ipv6 mld host-proxy

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

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

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

**Example:** Enable IPv6 MLD Proxy.

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

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

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

### 3.9.20.2 (config)# ipv6 mld host-proxy leave-proxy

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

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

**Example:** Enable IPv6 MLD leave proxy.

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

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

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

### *3.9.20.3 (config)# ipv6 mld snooping*

**Syntax:** (config)# ipv6 mld snooping

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

**Example:** Enable IPv6 MLD snooping.

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

**Negation:** (config)# no ipv6 mld snooping

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

### *3.9.20.4 (config)# ipv6 mld snooping vlan*

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

**Parameters:**

<v_vlan_list>: Specify VLAN ID for MLD.

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

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

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

### *3.9.20.5 (config)# ipv6 mld ssm-range*

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

**Parameters:**

<v_ipv6_mcast>: Specify valid IPv6 mluticast address.

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

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

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

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

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

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

### *3.9.20.6 (config)# ipv6 mld unknown-flooding*

**Syntax:** (config)# ipv6 mld unknown-flooding

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

**Example:** To flood unregistered IPv6 multicast traffic

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

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

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

### *3.9.20.7 (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> ]

### 3.9.20.8 (config-if)# ipv6 mld snooping filter

**Syntax:** (config-if)# ipv6 mld snooping filter <profile_name>

**Explanation:** Use this command to filter specific multicast traffic on a per port basis.

**Parameters:**

<profile_name>: Specify the configured multicast groups that are denied on a port. When a certain multicast group is selected on a port, IGMP join reports received on a port are dropped.

**Negation:** (config-if)# no ipv6 mld snooping filter

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

### 3.9.20.9 (config-if)# ipv6 mld snooping immediate-leave

**Syntax:** (config-if)# ipv6 igmp snooping immediate-leave

**Explanation:** Enable fast leave function on a specific port. When a leave packet is received, the switch immediately removes it from a multicast service without sending an IGMP group-specific (GS) query to that interface.

**Negation:** (config-if)# no ipv6 mld snooping immediate-leave

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

### 3.9.20.10 (config-if)# ipv6 mld snooping max-groups

**Syntax:** (config-if)# ip igmp snooping max-groups <throttling>

**Explanation:** Specify the maximum number of multicast groups that a port can join at the same time.

**Parameters:**

<throttling>: This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new IGMP join reports will be dropped. By default, unlimited is selected. The allowed range can be specified is 1 to 10.

**Negation:** (config-if)# no ipv6 mld snooping max-groups

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

#### *3. 9.20.11 (config-if)# ipv6 mld snooping mrouter*

**Syntax:** (config-if)# ipv6 mld snooping mrouter

**Explanation:** Set this interface to Router port. If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

**Negation:** (config-if)# no ipv6 mld snooping mrouter

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

### *3.9.21 (config-if)# l2cp*

**Syntax:** (config-if)# l2cp { [ peer [ <l2cp_peer_list> ] ] [ forward [ <l2cp_forward_list> ] ] }

**Parameters:**

[ peer [ <l2cp_peer_list> ] ] : Redirect to CPU to allow peering/tunneling/discard depending on ECE and protocol configuration. Specify 0-15 for BPDU addresses, 16 for select All bridge address, 17-32 for GARP addresses.

[ forward [ <l2cp_forward_list> ] ]: Allow peering/forwarding/tunneling/discarding depending on ECE and protocol configuration. Specify 0-15 for BPDU addresses, 16 for select All bridge address, 17-32 for GARP addresses.

**Explanation:** Configure the L2CP frame handling mode for the corresponding destination MAC address (DMAC). The MAC DA range for Bridge block of protocol is 01-80-C2-00-00-00 through 01-80-C2-00-00-0F (0-15) and for GARP block of protocol is 01-80-C2-00-00-20 through 01-80-C2-00-00-2F (17-32).

**Example:** Enable L2CP on interface 1 and set 01-80-C2-00-00-00 to 01-80-C2-00-00-05 to Forward mode.

```
# config t
(config)# interface FastEthernet 1/1
(config-if)#l2cp forward 0-5
(config-if)#
```

### *3.9.22(config)# lacp*

#### *3.9.22.1 (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.

```
# 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 }

### *3.9.22.2 (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

### *3.9.22.3 (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 }

### *3.9.22.4 (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 }

### 3.9.22.5 (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 }

### 3.9.22.6 (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 }

## 3.9.23 (config)# line

### 3.9.23.1 (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 ]

### 3.9.23.2 (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)#
```

### 3.9.23.3 (config-line)# editing

**Syntax:** (config-line)# editing

**Explanation:** Enable command line editing.

**Negation:** (config-line)# no editing

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

# show line [ alive ]

### 3.9.23.4 (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
#
```

### 3.9.23.5 (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 ]

### 3.9.23.6 (config-line)# exec-timeout

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

**Parameters:**

<min>: Specify timeout in minutes. The allowed range is 0 to 1440.

[<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 ]

### 3.9.23.7 (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)#
```

### 3.9.23.8 (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?'.)
```

### 3.9.23.9 (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 ]

### 3.9.23.10 (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 ]

### 3.9.23.11 (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 ]

### 3.9.23.12 (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 ]

### 3.9.23.13 (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 ]

### 3.9.23.14 (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 ]

## 3.9.24 (config)# lldp

### 3.9.24.1 (config)# lldp holdtime

**Syntax:** (config)# lldp holdtime <val>

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

**Parameters:**

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

**Example:** Set the holdtime to 5.

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

**Negation:** (config)# no lldp holdtime

### 3.9.24.2 (config)# lldp reinit

**Syntax:** (config)# lldp reinit <val>

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

**Parameters:**

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

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

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

**Negation:** (config)# no lldp reinit

### 3.9.24.3 (config)# lldp timer

**Syntax:** (config)# lldp timer <val>

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

**Parameters:**

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

**Example:** Set the LLDP timer value to 35.

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

**Negation:** (config)# no lldp timer

### 3.9.24.4 (config)# lldp transmission-delay

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

**Parameters:**

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

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

**Example:** Set the LLDP transmission delay value to 2.

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

**Negation:** (config)# no lldp transmission-delay

### 3.9.24.5 (config)# lldp med datum

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

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

**Parameters:**

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

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

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

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

**Example:** Set the map datum to wgs84.

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

**Negation:** (config)# no lldp med datum

### 3.9.24.6 (config)# lldp med fast

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

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

**Parameters:**

<v_1_to_10>: Specify a valid value between 1 and 10.

**Example:** Set the value to 5.

```
# config t
(config)# lldp med fast 5
```

**Negation:** (config)# no lldp med fast

### 3.9.24.7 (config)# lldp med location-tlv altitude

**Syntax:** (config)# lldp med location-tlv altitude { meters | floors } <v_word11>

**Explanation:** Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). “meters” means meters of Altitude defined by the vertical datum specified; while, “floors” means altitude in a form more relevant in buildings which have different floor-to-floor dimensions.

**Parameters:**

{ meters | floors }: Specify one of the options.

<v_word11>: Specify a value for the specified option.

**Example:** Set the altitude value to “floors 10”.

```
# config t
(config)# lldp med location-tlv altitude floors 10
```

**Negation:** (config)# no lldp med location-tlv altitude

### *3.9.24.8 (config)# lldp med location-tlv civic-addr*

**Syntax:** (config)# lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code } <v_string250>

**Explanation:** Configure civic address information.

**Parameters:**

{ country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code }: Specify one of the options.

**country:** The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

**state:** National subdivisions (state, canton, region, province, prefecture).

**county:** County, parish, gun (Japan), district.

**city:** City, township, shi (Japan) - Example: Copenhagen.

**district:** City division, borough, city district, ward, chou (Japan).

**block:** Neighbourhood, block.

**street:** Street - Example: Poppelvej.

**leading-street-direction:** Example: N.

**trailings-street-suffix:** Example: SW.

**street-suffix:** Ave, Platz.

**house-no:** Specify house number.

**house-no-suffix:** Example: A, 1/2.

**landmark:** Landmark or vanity address - Example: Columbia University.

**additional-info:** Example: South Wing.

**Name:** Example: Flemming Jahn.

**zip-code:** Postal/zip code - Example: 2791.

**building:** Building (structure). Example: Low Library.

**apartment:** Unit (Apartment, suite). Example: Apt 42.

**floor:** Example: 4.

**room-number:** Room number - Example: 450F.

**place-type:** Example: Office.

**postal-community-name:** Example: Leonia.

**p-o-box:** Example: 12345.

**additional code:** Example: 1320300003.

**Example:** Set the country code to "UK".

```
# config t
(config)# lldp med location-tlv civic-addr country UK
```

**Negation:** (config)# no lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code }

### *3.9.24.9 (config)# lldp med location-tlv elin-addr*

**Syntax:** (config)# lldp med location-tlv elin-addr <v_word25>

**Explanation:** Configure a value for Emergency Location Information.

**Parameters:**

<v_word25>: A value for Emergency Location Information (ELIN).

**Example:** Set the emergency location information to "911".

```
# config t
(config)# lldp med location-tlv elin-addr 911
```

**Negation:** (config)# no lldp med location-tlv elin-addr

### *3.9.24.10 (config)# lldp med location-tlv latitude*

**Syntax:** (config)# lldp med location-tlv latitude { north | south } <v_word8>

**Explanation:** Configure a value for latitude. Latitude value should be between 0 and 90.

**Parameters:**

{ north | south }: Specify one of the options, either north or south.

<v_word8>: Specify latitude value for the selected option.

**Example:** Set the north latitude to 5.

```
# config t
(config)# lldp med location-tlv latitude north 5
```

**Negation:** (config)# no lldp med location-tlv latitude

### *3.9.24.11 (config)# lldp med location-tlv longitude*

**Syntax:** (config)# lldp med location-tlv longitude { west | east } <v_word9>

**Explanation:** Configure a value for longitude. Longitude value should be between 0 and 180.

**Parameters:**

{ west | east }: Specify one of the options, either west or east.

<v_word9>: Specify longitude value for the selected option.

**Example:** Set the west longitude to 90.

```
# config t
(config)# lldp med location-tlv longitude west 90
```

**Negation:** (config)# no lldp med location-tlv longitude

### *3.9.24.12 (config)# lldp med media-vlan-policy*

**Syntax:** (config)# lldp med media-vlan-policy <policy_index> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { tagged <v_vlan_id> | untagged } [ l2-priority <v_0_to_7> ] [ dscp <v_0_to_63> ]

**Explanation:** Configure a LLDP MED policy ID for a service.

**Parameters:**

<policy_index>: Specify a policy ID. The valid range is from 0 to 31.

{ voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling }: Specify one of the services for this policy ID.

{ tagged <v_vlan_id> | untagged }: Specify whether this service is tagged or untagged. When "tagged" is specified, a VLAN ID should be provided.

[ l2-priority <v_0_to_7> ]: Specify a value for L2 priority. The valid value is from 0 to 7.

[ dscp <v_0_to_63> ]: Specify a value for DSCP. The valid value is from 0 to 63.

**Example:** Create a policy ID 1 for tagged Voice VLAN.

```
# config t
(config)# lldp med media-vlan-policy 1 voice tagged 100 l2-priority 7 DSCP 63
```

**Negation:** (config)# no lldp med media-vlan-policy <policies_list>

**Show:** > show lldp med media-vlan-policy [ <v_0_to_31> ]
# show lldp med media-vlan-policy [ <v_0_to_31> ]

### 3.9.24.13 (config-if)# lldp cdp-aware

**Syntax:** (config-if)# lldp cdp-aware

**Explanation:** Configures if the interface shall be CDP aware (CDP discovery information is added to the LLDP neighbor table).

**Example:** Set interface 1 to CDP aware.

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

**Negation:** (config-if)# no lldp cdp-aware

**Show: >** show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### 3.9.24.14 (config-if)# lldp med media-vlan policy-list

**Syntax:** (config-if)# lldp med media-vlan policy-list <v_range_list>

**Explanation:** To apply MED Media-VLAN policy of LLDP on this interface.

**Parameters:**

<v_range_list>: Assign a policy to this interface.

**Negation:** (config-if)# no lldp med media-vlan policy-list <v_range_list>

**Show:** > show lldp med media-vlan-policy [ <v_0_to_31> ]
# show lldp med media-vlan-policy [ <v_0_to_31> ]

### 3.9.24.15 (config-if)# lldp med transmit-tlv

**Syntax:** (config-if)# lldp med transmit-tlv [ capabilities ] [ location ] [ network-policy ]

**Explanation:** To configure LLDP-MED TLV Type for specific interface.

**Parameters:**

[ capabilities ]: Enable transmission of the optional capabilities TLV.

[ location ]: Enable transmission of the optional location TLV.

[ network-policy ]: Enable transmission of the optional network policy TLV.

**Negation:** (config-if)# no lldp med transmit-tlv [ capabilities ] [ location ] [ network-policy ]

**Show:** > show lldp med media-vlan-policy [ <v_0_to_31> ]
# show lldp med media-vlan-policy [ <v_0_to_31> ]

### 3.9.24.16 (config-if)# lldp receive

**Syntax:** (config-if)# lldp receive

**Explanation:** The switch will analyze LLDP information received from neighbours.

**Negation:** (config-if)# no lldp receive

**Show:** > show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### 3.9.24.17 (config-if)# lldp tlv-select

**Syntax:** (config-if)# lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }

**Explanation:** To configure LLDP-MED TLV attributes for specific interface.

**Parameters:**

{ management-address | port-description | system-capabilities | system-description | system-name }: Specify a LLDP TLV attribute. LLDP uses several attributes to discover neighbour devices. These attributes contains type, length, and value descriptions and are referred to TLVs. Details such as port description, system name, system description, system capabilities, management address can be sent from this device.

**Negation:** (config-if)# no lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }

**Show:** > show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### 3.9.24.18 (config-if)# lldp transmit

**Syntax:** (config-if)# lldp transmit

**Explanation:** To configure LLDP Tx only mode for specific interface

**Negation:** (config-if)# no lldp transmit

**Show:** # show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### 3.9.25 (config)# logging

#### 3.9.25.1 (config)# logging on

**Syntax:** (config)# logging on

**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.

**Example:** Enable log server operation.

```
# config t
(config)# logging on
```

**Negation:** (config)# no logging on

**Show:** # show logging

Clear: # clear logging [ info ] [ warning ] [ error ] [ switch <switch_list> ]

#### 3.9.25.2 (config)# logging host

**Syntax:** (config)# logging host { <v_ipv4_ucast> | <v_word45> }

**Parameters:**

{ <hostname> | <ipv4_ucast> }: Specify one of the options. The hostname is the domain name of the log server; while the latter is 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]

#### 3.9.25.3 (config)# logging level

**Syntax:** (config)# logging level { info | warning | error }

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

**Parameters:**

{ info | warning | error }: Specify one of the log message options.

**Info:** Send information, warnings and errors.

**Warning:** Send warnings and errors.

**Error:** Send errors only.

**Example:** Send error messages to log server.

```
# config t
(config)# logging level error
```

**Show:** # show logging
# show logging <logging_id: 1-4294967295>
# show logging [info] [warning] [error]

## 3.9.26 (config)# loop-protect

### 3.9.26.1 (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> ] ) ]

### 3.9.26.2 (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> ] ) ]

### 3.9.26.3 (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> ] ) ]

### 3.9.26.4 (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> ] ) ]

### 3.9.26.5 (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> ] ) ]

### 3.9.26.6 (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> ] ) ]

## 3.9.27 (config)# mac

### 3.9.27.1 (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

### 3.9.27.2 (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

### *3.9.27.3 (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

## *3.9.28 (config-if)# media-type*

**Syntax:** (config-if)# media-type { rj45 | sfp | dual }

**Explanation:** Configure the media type supported for this specific interface.

**Parameters:**

{ rj45 | sfp | dual }: The options are RJ-45, SFP, or dual (both RJ-45 & SFP are supported.).

**Negation:** (config-if)# no media-type

### 3.9.29 (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

### 3.9.30 (config)# mep

#### 3.9.30.1 (config)# mep <inst>

**Syntax:** (config)# mep <inst> [ mip ] { up | down } domain { port | evc | vlan } [ vid <vid> ] flow <flow> level <level> interface <port_type> <port>

**Explanation:** Create a MEP instance.

**Parameters:**

<inst>: Specify an instance ID number.

[ mip ]: Mip (Maintenance Entity Intermediate Point) mode.

{ up | down }: Specify the traffic direction either Ingress or Egress for monitoring on a residence port.

domain { port | evc | vlan }: Specify a domain option.

**Port:** This is a MEP in the Port Domain. 'Flow Instance' is a Port. (CURRENTLY, Port is available for use.)

**Evc:** This is a MEP in the EVC Domain. 'Flow Instance' is a EVC. The EVC must be created.

**VLAN:** This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. The VLAN must be created.

[ vid <vid> ]: A C-tag or S-tag (depending on VLAN port type) is added with this VID. Entering “0” means no tag will be added.

flow <flow>: The MEP related to this flow.

level <level>: The MGP level of this MEP.

interface <port_type> <port>: Specify a port number that you want to moinitor.

**Negation:** (config)# no mep <inst>

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

### *3.9.30.2 (config)# mep <inst> ais*

**Syntax:** (config)# mep <inst> ais [ fr1s | fr1m ] [ protect ]

**Explanation:** To configure AIS of a MEP instance.

**Parameters:**

<inst>: Specify an instance ID number.

ais [ fr1s | fr1m ]: Ais stands for Alarm Indication Signal. “fr1s” means that frame rate is 1 f/s. “fr1m” means that frame rate is 1 f/min.

[ protect ]: The AIS can be used for protection. At the point of state change three AIS PDUs are transmitted as fast as possible.

**Negation:** (config)# no mep <inst> ais

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

### *3.9.30.3 (config)# mep <inst> aps*

**Syntax:** (config)# mep <inst> aps <prio> [ multi | uni ] { laps | { raps [ octet <octet> ] } }

**Explanation:** Configure APS of a MEP instance.

**Parameters:**

<inst>: Specify an instance ID number.

aps <prio>: The priority to be inserted as PCP bits in TAG (if any).

[ multi | uni ]: Specify an option.

**multi:** OAM PDU is transmitted with multicast MAC. Must be “multi” in case of RAPS (Ring Automatic Protection Switching Protocol).

**uni:** OAM PDU is transmitted with unicast MAC. The MAC is taken from peer MEP MAC database. This option is only possible in case of LAPS (Linear Automatic Protection Switching Protocol).

{ laps | { raps [ octet <octet> ] } }: Specify an option.

**laps:** APS PDU is transmitted as L-APS (this is for ELPS).

**raps:** APS PDU is transmitted as R-APS (this is for ERPS).

**octet:** This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

**Negation:** (config)# no mep <inst> aps

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

### *3.9.30.4 (config)# mep <inst> cc*

**Syntax:** (config)# mep <inst> cc <prio> [ fr300s | fr100s | fr10s | fr1s | fr6m | fr1m | fr6h ]

**Explanation:** Configure Continuity Check of a MEP instance.

**Parameters:**

<inst>: Specify an instance ID number.

cc: Continuity Check

<prio: 0-7>: The priority to be inserted as PCP bits in TAG (if any).

[ fr300s | fr100s | fr10s | fr1s | fr6m | fr1m | fr6h ]: The frame rate is 300 f/s, 100 f/s, 10 f/s, 1 f/s, 6 f/min, 1 f/min, 6 f/hour.

**Negation:** (config)# no mep <inst> cc

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

### *3.9.30.5 (config)# mep <inst> client domain*

**Syntax:** (config)# mep <inst> client domain { evc | vlan }

**Explanation:** Configure client domain of a MEP instance.

**Parameters:**

<inst>: Specify an instance ID number.

cc: Continuity Check

{ evc | vlan }: The client layer domain. Options available are EVC and VLAN domain.

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

### *3.9.30.6 (config)# mep <inst> client flow*

**Syntax:** (config)# mep <inst> client flow <cflow> level <level> [ ais-prio [ <aisprio> | ais-highest ] ] [ lck-prio [ <lckprio> | lck-highest ] ]

**Explanation:** Configure the priority to be used when transmitting AIS in each client flow.

**Parameters:**

<inst>: Specify an instance ID number.

client flow <cflow: unit>: The client layer flow number.

level <level: 0-7>: The MEG level value.

[ ais-prio [ <aisprio:0-7> | ais-highest ] ]:  Configure AIS injection priority. Specify either 0-7 or the highest possible number.

[ lck-prio [ <lckprio: 0-7> | lck-highest ] ]: Configure LCK injection priority. Specify either 0-7 or the highest possible number.

**Negation:** (config)# no mep <inst> client-flow { <cflow> | all }

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

### *3.9.30.7 (config)# mep <inst> dm*

**Syntax:** (config)# mep <inst> dm <prio> [ multi | { uni mep-id <mepid> } ] [ single | dual ] [ rdtrp | flow ] interval <interval> last-n <lastn>

**Explanation:** To configure Delay Measurement of a MEP.

**Parameters:**

<inst>: Specify an instance ID number.

dm <prio: 0-7>: Configure Delay Measurement (DM) priority value. Priority in case of tagged OAM. In the EVC domain this is the COS-ID.

[ multi | { uni mep-id <mepid> } ]: Specify multicast or unicast MEP ID.

[ single | dual ]: One-Way or Two-Way Delay Measurement implemented on 1DM or DMM/DMR, respectively.

[ rdtrp | flow ]:  Specify one value.

**rdtrp:** The frame delay calculated by the transmitting and receiving timestamps of initiators. Frame Delay = RxTimeb-TxTimeStampf.

**Flow:** The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay = (RxTimeb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf).

interval <interval>: Interval between PDU transmission in 10ms. Min value is 10.

last-n <lastn>: The last N dalays used for average last N calculation. Min value is 10.

**Negation:** (config)# no mep <inst> dm

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

**Clear:** # clear mep <inst> { lm | dm |tst }

### *3.9.30.8 (config)# mep <inst> dm ns*

**Syntax:** (config)# mep <inst> dm ns

**Explanation:** Configure Delay Measurement (nanosecond) of a MEP.

**Parameters:**

<inst>: Specify an instance ID number.

**Negation:** (config)# no mep <inst> dm ns

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

**Clear:** # clear mep <inst> { lm | dm |tst }

### *3.9.30.9 (config)# mep <inst> dm overflow-reset*

**Syntax:** (config)# mep <inst> dm overflow-reset

**Explanation:** Reset all Delay Measurement results on total delay counter overflow.

**Parameters:**

<inst>: Specify an instance ID number.

**Negation:** (config)# no mep <inst> dm overflow-reset

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

**Clear:** # clear mep <inst> { lm | dm |tst }

### *3.9.30.10 (config)# mep <inst> dm proprietary*

**Syntax:** (config)# mep <inst> dm proprietary

**Explanation:** Use proprietary Delay Measurement.

**Parameters:**

<inst>: Specify an instance ID number.

**Negation:** (config)# no mep <inst> dm proprietary

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

**Clear:** # clear mep <inst> { lm | dm |tst }

### *3.9.30.11 (config)# mep <inst> dm syncronized*

**Syntax:** (config)# mep <inst> dm syncronized

**Explanation:** Configure time sync of Delay Measurement.

**Parameters:**

<inst>: Specify an instance ID number.

**Negation:** (config)# no mep <inst> dm syncronized

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

**Clear:** # clear mep <inst> { lm | dm |tst }

### 3.9.30.12 (config)# mep <inst> lb

**Syntax:** (config)# mep <inst> lb <prio> [ dei ] [ multi | { uni { { mep-id <mepid> } | { mac <mac> } } } ] count <count> size <size> interval <interval>

**Explanation:** Configure loopback of a MEP.

**Parameters:**

<inst>: Specify an instance ID number.

lb <prio: 0-7>: Configure loopback priority. The priority to be inserted as PCP bits in TAG (if any).

[ dei ]: The DEI to be inserted as PCP bits in TAG (if any).

[ multi | { uni { { mep-id <mepid> } | { mac <mac> } } } ]: Specify LBM PDU to be transmitted as unicast or multicast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop Back is possible.

count <count>: The number of LBM PDU to be sent.

size <size>: The number of bytes in the LBM PDU Data Pattern TLV.

interval <interval>: The number of bytes in the LBM PDU Data Pattern TLV.

**Negation:** (config)# no mep <inst> lb

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

### 3.9.30.13 (config)# mep <inst> lck

**Syntax:** (config)# mep <inst> lck [ fr1s | fr1m ]

**Explanation:** Configure Locked Frame Rate of a MEP.

**Parameters:**

<inst>: Specify an instance ID number.

[ fr1s | fr1m ]: Frame rate is 1 f/s or 1 f/min.

**Negation:** (config)# no mep <inst> lck

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

### *3.9.30.14 (config)# mep <inst> level*

**Syntax:** (config)# mep <inst> level <level>

**Explanation:** Configure MEG level of a MEP.

**Parameters:**

<inst>: Specify an instance ID number.

<level:0-7>: The MEG level value.

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

### *3.9.30.15 (config)# mep <inst> lm*

**Syntax:** (config)# mep <inst> lm <prio> [ multi | uni ] [ single | dual ] [ fr10s | fr1s | fr6m | fr1m | fr6h ] [ flr <flr> ]

**Explanation:** Configure Locked Frame Rate of a MEP.

**Parameters:**

<inst>: Specify an instance ID number.

lm <prio: 0-7>: Configure loss measurement priority in case of tagged OAM. In the EVC domain this is the COS-ID.

[ multi | uni ]: multi OAM PDU is transmitted with multicast MAC. uni OAM PDU is transmitted with unicast MAC. The MAC is taken from peer MEP MAC database. In case of LM there is only one peer MEP.

[ single | dual ]: Dual ended LM is based on CCM PDU. Single ended LM is based on LMM/LMR PDU.

[ fr10s | fr1s | fr6m | fr1m | fr6h ]: Specify a frame rate.

fr10s: Frame rate is 10 f/s.

fr1s: Frame rate is 1 f/s.

fr6m: Frame rate is 6 f/min.

fr1m: Frame rate is 1 f/min.

fr6h: Frame rate is 6 f/hour.

[ flr <flr: unit> ]: The Frame Loss Ratio interval value.

**Negation:** (config)# no mep <inst> lm

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

**Clear:** # clear mep <inst> { lm | dm |tst }

### 3.9.30.16 (config)# mep <inst> lt

**Syntax:** (config)# mep <inst> lt <prio> { { mep-id <mepid> } | { mac <mac> } } ttl <ttl>

**Explanation:** Configure link trace of a MEP.

**Parameters:**

<inst>: Specify an instance ID number.

lt <prio: 0-7>: Configure link trace priority in case of tagged OAM. In the EVC domain this is the COS-ID.

{ { mep-id <mepid> } | { mac <mac> } }: Specify Peer MEP-ID for Link Trace target unicast MAC or Link Trace target unicast MAC address.

ttl <ttl> Time to live value.

**Negation:** (config)# no mep <inst> lt

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

### 3.9.30.17 (config)# mep <inst> meg-id

**Syntax:** (config)# mep <inst> meg-id <megid> { itu | itu-cc | { ieee [ name <name> ] } }

**Explanation:** To configure MEG-ID format.

**Parameters:**

<inst>: Specify an instance ID number.

meg-id <megid>: Specify a MEG ID string. This is either the ITU MEG-ID or the IEEE Short MA, depending on the selected MEG-ID format. The ITU max. is 13 characters. The ITU-CC max. is 15 characters. The IEEE max. is 16 characters..

{ itu | itu-cc | { ieee [ name <name> ] } }: Specify a MEG-ID format.

**itu:**The MEG-ID has ITU format (ICC - UMC). The meg-id max. is 13 characters.

**itu-cc:**The MEG-ID has ITU Country Code format (CC - ICC - UMC). The meg-id max. is 15 characters.

**ieee:** The MEG-ID (Short MA Name) has IEEE Character String format. The meg-id max. is 16 characters.

**name <name>:** This is only relevant for IEEE.

### 3.9.30.18 (config)# mep <inst> peer-mep-id

**Syntax:** (config)# mep <inst> peer-mep-id <mepid> [ mac <mac> ]

**Explanation:** Configure peer MEP-ID of a MEP.

**Parameters:**

<inst>: Specify an instance ID number.

peer-mep-id <mepid>: Configure the peer MEP-ID value.

[ mac <mac> ]: The peer MAC address.

**Negation:** (config)# no mep <inst> peer-mep-id { <mepid> | all }

### *3.9.30.19 (config)# mep <inst> performance-monitoring*

**Syntax:** (config)# mep <inst> performance-monitoring

**Explanation:** Enable perofmrance monitoring of MEP.

**Parameters:**

<inst>: Specify an instance ID number.

**Negation:** (config)# no mep <inst> performance-monitoring

### *3.9.30.20 (config)# mep <inst> tst*

**Syntax:** (config)# mep <inst> tst <prio> [ dei ] mep-id <mepid> [ sequence ] [ all-zero | all-one | one-zero ] rate <rate> size <size>

**Explanation:** Enable test signal of MEP.

**Parameters:**

<inst>: Specify an instance ID number.

tst <prio: 0-7>: Configure the test signal priority in case of tagged OAM. In the EVC domain this is the COS-ID.

[ dei ]: Drop Eligible Indicator in case of tagged OAM.

mep-id <mepid>: Configure Peer MEP-ID value for unicast TST. The MAC is taken from peer MEP MAC database.

[ sequence ]: Enable sequence number in TST PDU.

[ all-zero | all-one | one-zero ]: Specify an option.

**all-zero:** Test pattern is set to all zero.

**all-one:** Test pattern is set to all one.

**one-zero:** Test pattern is set to 10101010.

rate <rate>: Transmission rate value.

size <size>: Frame size value.

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

**Clear:** # clear mep <inst> { lm | dm |tst }

### 3.9.30.21 (config)# mep <inst> tst rx

**Syntax:** (config)# mep <inst> tst rx

**Explanation:** Enable test signal RX transmission of MEP.

**Parameters:**

<inst>: Specify an instance ID number.

**Negation:** (config)# no mep <inst> tst rx

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

**Clear:** # clear mep <inst> { lm | dm |tst }

### 3.9.30.22 (config)# mep <inst> tst rx

**Syntax:** (config)# mep <inst> tst tx

**Explanation:** Enable test signal TX transmission of MEP.

**Parameters:**

<inst>: Specify an instance ID number.

**Negation:** (config)# no mep <inst> tst tx

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

**Clear:** # clear mep <inst> { lm | dm |tst }

### 3.9.30.23 (config)# mep <inst> vid

**Syntax:** (config)# mep <inst> vid <vid>

**Explanation:** To configure VID of MEP.

**Parameters:**

<inst>: Specify an instance ID number.

<vid>: The MEP VID value.

**Negation:** (config)# no mep <inst> vid

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

#### 3.9.30.24 (config)# mep <inst> voe

**Syntax:** (config)# mep <inst> voe

**Explanation:** MEP is VOE based.

**Parameters:**

<inst>: Specify an instance ID number.

**Negation:** (config)# no mep <inst> voe

**Show:** # show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]

### 3.9.31 (config)# monitor

#### 3.9.31.1 (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 10.

```
# config t
(config)# monitor destination interface gigabitethernet 1/10
```

**Negation:** (config)# no monitor destination

#### 3.9.31.2 (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 one of the options. * 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> ] } }

### *3.9.32 (config)# mvr*

#### *3.9.32.1 (config)# mvr*

**Syntax:** (config)# mvr

**Explanation:** Enable MVR function.

**Example:** Enable MVR function.

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

**Negation**: (config)# no mvr

**Show:** > show mvr
# show mvr

#### *3.9.32.2 (config)# mvr name <mvr_name> channel*

**Syntax:** (config)# mvr name <mvr_name> channel <profile_name>

**Explanation:** Configure MVR name and channel.

**Parameters:**

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

<profile_name>: Specify a channel name for this MVR entry. The allowed characters are 16.

**Example:** Set up a MVR entry “video1” and its corresponding channel profile name “1”.

```
# config t
(config)# mvr name video1 channel 1
```

**Negation**: (config)# no mvr name <mvr_name> channel

**Show:** > show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

#### *3.9.32.3 (config)# mvr name <mvr_name> frame priority*

**Syntax:** (config)# mvr name <mvr_name> frame priority <cos_priority>

**Explanation:** Configure the priority for transmitting IGMP/MLD control frames for the specified MVR entry.

**Parameters:**

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

<cos_priority>: Specify a Cos priority for this MVR entry. The allowed range is from 0 to 7.

**Example:** Set up a MVR entry "video1" and its corresponding priority value "0".

```
# config t
(config)# mvr name video1 frame priority 0
```

**Negation**: (config)# no mvr name <mvr_name> frame priority

**Show:** > show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### *3.9.32.4 (config)# mvr name <mvr_name> frame tagged*

**Syntax:** (config)# mvr name <mvr_name> frame tagged

**Explanation:** Tagged IGMP/MLD frames will be sent.

**Parameters:**

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

**Example:** Set "video1" MVR entry to send tagged IGMP/MLD frames.

```
# config t
(config)# mvr name video1 frame tagged
```

**Negation**: (config)# no mvr name <mvr_name> frame tagged

**Show:** > show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### *3.9.32.5 (config)# mvr name <mvr_name> igmp-address*

**Syntax:** (config)# mvr name <mvr_name> igmp-address <v_ipv4_ucast>

**Explanation:** Configure IGMP IPv4 address for the specified MVR entry.

**Parameters:**

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

<v_ipv4_ucast>: Specify the IPv4 unicast address as source address used in IP header for IGMP control frames.

**Example:** Set up a MVR entry “video1” and its corresponding IGMP address “10.1.1.100”.

```
# config t
(config)# mvr name video1 igmp-address 10.1.1.100
```

**Negation**: (config)# no mvr vlan <mvr_name> igmp-address

**Show:** > show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### 3.9.32.6 (config)# mvr name <mvr_name> last-member-query-interval

**Syntax:** (config)# mvr name <mvr_name> last-member-query-interval <ipmc_lmqi>

**Explanation:** Configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership.

**Parameters:**

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

<ipmc_lmqi>: Specify the LMQI (Last Member Query Interval) value. By default, LMQI is set to 5 tenths of a second (0.5 second). The allowed range is from 0 to 31744 tenths of a second.

**Example:** Set LMQI value to 600 tenths of a second.

```
# config t
(config)# mvr name video1 last-member-query-interval 600
```

**Negation**: (config)# no mvr vlan <mvr_name> last-member-query-interval

**Show:** > show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### 3.9.32.7 (config)# mvr name <mvr_name> mode

**Syntax:** (config)# mvr name <mvr_name> mode { dynamic | compatible }

**Explanation:** Configure MVR mode.

**Parameters:**

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

{ dynamic | compatible }: Specify one of the options.

**Dynamic:** MVR allows dynamic MVR membership reports on source ports. (This is the default mode.)

**Compatible:** MVR membership reports are forbidden on source ports.

**Example:** Set MVR mode to dynamic.

```
# config t
(config)# mvr name video1 mode dynamic
```

**Negation**: (config)# no mvr name <mvr_name> mode

**Show:** > show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### *3.9.32.8 (config)# mvr vlan <v_vlan_list>*

**Syntax:** (config)# mvr vlan <v_vlan_list> [ name <mvr_name> ]

**Explanation:** Configure a MVR VLAN and its corresponding MVR name.

**Parameters:**

<v_vlan_list>: Specify multicast VLAN ID.

[ name <mvr_name> ]: Specify a name for this MVR entry. This argument is optional.

**Example:** Set up MVR VLAN 201 and its corresponding name.

```
# config t
(config)# mvr vlan 201 video1
```

**Negation**: (config)# no mvr vlan <v_vlan_list>

**Show:** > show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### *3.9.32.9 (config)# mvr vlan <v_vlan_list> channel*

**Syntax:** (config)# mvr vlan <v_vlan_list> channel <profile_name>

**Explanation:** Configure MVR name and channel.

**Parameters:**

<v_vlan_list>: Specify  MVR VLAN ID for this entry.

<profile_name>: Specify a channel name for this MVR entry. The allowed characters are 16.

**Example:** Set up Set up MVR VLAN 201 and its corresponding channel.

```
# config t
(config)# mvr vlan 201 channel 1
```

**Negation**: (config)# no mvr vlan <v_vlan_list> channel

**Show:** > show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### *3.9.32.10 (config)# mvr vlan <v_vlan_list> frame priority*

**Syntax:** (config)# mvr vlan <v_vlan_list> frame priority <cos_priority>

**Explanation:** Configure the priority for transmitting IGMP/MLD control frames for the specified MVR VLAN ID.

**Parameters:**

<v_vlan_list>: Specify MVR VLAN ID for this entry.

<cos_priority>: Specify a Cos priority for this MVR entry. The allowed range is from 0 to 7.

**Example:** Set up a MVR VLAN 201 and its corresponding priority value “0”.

```
# config t
(config)# mvr vlan 201 frame priority 0
```

**Negation**: (config)# no mvr vlan <v_vlan_list> frame priority

**Show:** > show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### *3.9.32.11 (config)# mvr vlan <v_vlan_list> frame tagged*

**Syntax:** (config)# mvr vlan <v_vlan_list> frame tagged

**Explanation:** Tagged IGMP/MLD frames will be sent.

**Parameters:**

<v_vlan_list>: Specify MVR VLAN ID for this entry.

**Example:** Set MVR VLAN 201 to send tagged IGMP/MLD frames.

```
# config t
(config)# mvr vlan 201 frame tagged
```

**Negation**: (config)# no mvr vlan <v_vlan_list> frame tagged

**Show:** > show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

#### *3.9.32.12 (config)# mvr vlan <v_vlan_list> igmp-address*

**Syntax:** (config)# mvr vlan <v_vlan_list> igmp-address <v_ipv4_ucast>

**Explanation:** Configure IGMP IPv4 address for the specified MVR entry.

**Parameters:**

<v_vlan_list>: Specify  MVR VLAN ID for this entry.

<v_ipv4_ucast>: Specify the IPv4 unicast address as source address used in IP header for IGMP control frames.

**Example:** Set up a MVR VLAN 201 and its corresponding IGMP address “10.1.1.100”.

```
# config t
(config)# mvr vlan 201 igmp-address 10.1.1.100
```

**Negation**: (config)# no mvr vlan <v_vlan_list> igmp-address

**Show:** > show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

#### *3.9.32.13 (config)# mvr vlan <v_vlan_list>  last-member-query-interval*

**Syntax:** (config)# mvr vlan <v_vlan_list> last-member-query-interval <ipmc_lmqi>

**Explanation:** Configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership.

**Parameters:**

<v_vlan_list>: Specify  MVR VLAN ID for this entry.

<ipmc_lmqi>: Specify the LMQI (Last Member Query Interval) value. By default, LMQI is set to 5 tenths of a second (0.5 second). The allowed range is from 0 to 31744 tenths of a second.

**Example:** Set LMQI value to 600 tenths of a second.

```
# config t
(config)# mvr vlan 201 last-member-query-interval 600
```

**Negation**: (config)# no mvr vlan <v_vlan_list> last-member-query-interval

**Show:** > show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### 3.9.32.14 (config)# mvr vlan <v_vlan_list> mode

**Syntax:** (config)# mvr vlan <v_vlan_list> mode { dynamic | compatible }

**Explanation:** Configure MVR mode.

**Parameters:**

<v_vlan_list>: Specify MVR VLAN ID for this entry.

{ dynamic | compatible }: Specify one of the options.

Dynamic: MVR allows dynamic MVR membership reports on source ports. (This is the default mode.)

Compatible: MVR membership reports are forbidden on source ports.

**Example:** Set MVR mode to dynamic.

```
# config t
(config)# mvr vlan 201 mode dynamic
```

**Negation**: (config)# no mvr vlan <v_vlan_list> mode

**Show:** > show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show mvr [ vlan <v_vlan_list> | name <mvr_name> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]

### 3.9.32.15 (config-if)# mvr immediate-leave

**Syntax:** (config-if)# mvr immediate-leave

**Explanation:** Enable immediate leave function. When enabled, the device immediately removes a port from a multicast stream as soon as it receives leave message for that group. This option only applies to an interface configured as MVR receivers.

**Example:** Enable immediate leave function on port 1.

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

**Negation**: (config-if)# no mvr immediate leave

#### *3.9.32.16 (config-if)# mvr name*

**Syntax:** (config-if)# mvr name <mvr_name> type { source | receiver }

**Explanation:** Configure port role of specific MVR profile for specific interface.

**Parameters:**

<mvr_name>: Specify a MVR name. The maximum length of the MVR name string is 16. Both alphabets and numbers are allowed for use.

{ source | receiver }: Specify MVR port role.

**source:** MVR source port.

**receiver:** MVR receiver port.

**Negation**: (config-if)# no mvr name <mvr_name> type

#### *3.9.32.17 (config-if)# mvr vlan*

**Syntax:** (config-if)# mvr vlan <v_vlan_list> type { source | receiver }

**Explanation:** Configure port role of a specific MVR VLAN ID for this specific interface.

**Parameters:**

<v_vlan_list>: MVR Multicast VLAN list

{ source | receiver }: Specify MVR port role.

**source:** MVR source port.

**receiver:** MVR receiver port.

**Negation**: (config-if)# no mvr immediate leave

### *3.9.33 (config)# ntp*

#### *3.9.33.1 (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

### 3.9.33.2 (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

## 3.9.34 (config)# poe (For PoE Models Only)

### 3.9.34.1 (config)# poe management mode

**Syntax:** (config)# poe management mode { class-consumption | class-reserved-power | allocation-consumption | allocation-reserved-power | lldp-consumption | lldp-resserved-power }

**Explanation:** Power over Ethernet (PoE) commands are used to set the maximum PoE power provided to a port, the maximum power budget for the switch (power available to all RJ-45 ports), the port PoE operating mode, power allocation priority, and the maximum power allocated to each port. If the power demand from devices connected to the switch exceeds the power budget, the switch uses port power priority settings to limit the supplied power.

**Parameters:**

consumption & reserved power mode: "consumption" & "reserved-power" mode decide how ports are shut down.

**consumption:** When this mode is used, ports are shut down in the event of the following situations.

1. When the actual power consumption for all ports exceeds the amount of power supply can deliver.

2. When the actual power consumption for a given port exceeds the reserved power for that port.

Ports are shut down according to their port priority. If two ports have the same priority, the port with the higher port number is shut down.

**reserved-power:** When this mode is selected, ports are shut down when total reserved power exceeds the amount of power that the power supply can deliver. In this mode, if the PD (Powered Device) keeps requesting more power than available from the power supply, then the port power is not turned on.

class, allocation & lldp: These modes are used to set up how attached PD may reserve power:

**class:** Each port automatically determines how much power to reserve according to the class which the connected PD belongs. Four different port classes are used; these are 4, 7, 15.4 and 30 Watts.

**allocation:** The amount of power reserved for each is specified in "Maximum Power [W]" field.

**lldp:** This mode is similar to Class mode except that each port determines the amount power it reserves by exchanging PoE information using LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the Class mode.

***NOTE:*** *If ports use more power than the power reserved for them, they will be shut down.*

**Negation:** (config)# no poe management mode

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

### *3.9.34.2 (config)# poe supply*

**Syntax:** (config)# poe supply <v_1_to_180>

**Explanation:** Configure the maximum power supply that the device can deliver.

**Parameters:**

<v_1_to_180>: Specify maximum power supply that the device can deliver.

**Negation:** (config)# no poe supply

### 3.9.34.3 (config-if)# poe check

**Syntax:** (config-if)# poe check

**Explanation:** Enable PoE failure check function. This switch can monitor PD working status by pinging its IP address. If the switch does not receive a response from PD within the specified response time, the PD status is regarded as failed. Once the PD fails, the switch (PSE) can take an appropriate action selected in “No Response Action” field.

**Negation:** (config-if)# no poe check

### 3.9.34.4 (config-if)# poe check { interval [ <v_10_to_300> ] }

**Syntax:** (config-if)# poe check { interval [ <v_10_to_300> ] }

**Explanation:** Specify the interval between each ping checking.

**Parameters:**

{ interval [ <v_10_to_300> ] }: Specify PoE Check interval between each ping checking. Valid range is 10 to 300 seconds.

### 3.9.34.5 (config-if)# poe check ip-address

**Syntax:** (config-if)# poe check ip-address <word_var>

**Explanation:** Specify the PD’s IP address for ping purposes. Both IPv4 and IPv6 IP addresses are supported.

**Parameters:**

<word_var: 1-45>: Specify IPv4 or IPv6 IP address.

**Negation:** (config-if)# no poe check ip-address

### 3.9.34.6 (config-if)# poe check { no-response-action [ no-action | reboot | power-off ] }

**Syntax:** (config-if)# poe check { no-response-action [ no-action | reboot | power-off ] }

**Explanation:** If PDs fails to respond ping requests sent by the switch (PSE), then the switch (PSE) can take an appropriate action specified in this command.

**Parameters:**

{ no-response-action [ no-action | reboot | power-off ] }: Specify a “no-response-action” option.

**no-action:** The switch (PSE) will not take any actions on the PD.

**reboot:** The switch (PSE) reboots the PD after the PD failure check.

**power-off:** The switch (PSE) turns off the PD after the PD failure check.

### *3.9.34.7 (config-if)# poe check { reboot-time [ <v_60_to_120> ] }*

**Syntax:** (config-if)# poe check { reboot-time [ <v_60_to_120> ] }

**Explanation:** Specify the reboot time in seconds.

**Parameters:**

{ reboot-time [ <v_60_to_120> ] }: Specify the reboot time. Valid range is 60 to 120 seconds.

### *3.9.34.8 (config-if)# poe check { timeout [ <v_1_to_10> ] }*

**Syntax:** (config-if)# poe check { timeout [ <v_1_to_10> ] }

**Explanation:** Specify the total cycles of IP checking.

**Parameters:**

{ timeout [ <v_1_to_10> ] }: Specify the total cycles of IP checking.

### *3.9.34.9 (config-if)# poe mode { standard | plus }*

**Syntax:** (config-if)# poe mode { standard | plus }

**Explanation:** Configure PoE operating mode.

**Parameters:**

{ standard | plus }: Specify one of the options.

**standard:** Enable IEEE 802.3af (Class 4 PDs limited to 15.4W).

**plus:** Enable IEEE 802.3at (Class 4 PDs limited to 30W).

**Negation:** (config-if)# no poe mode

### *3.9.34.10 (config-if)# poe power limit { <v_word9> }*

**Syntax:** (config-if)# poe power limit { <v_word9> }

**Explanation:** Configure maximum power for this specific interface.

**Parameters:**

{ <v_word9> }: Specify maximum power for this specific interface (0~15.4W for PoE standard mode, 0~30W for PoE plus mode.)

**Negation:** (config-if)# no poe power limit

### 3.9.34.11 (config-if)# poe priority { low | high | critical }

**Syntax:** (config-if)# poe priority { low | high | critical }

**Explanation:** When ports or attached PDs requested more power than the power supply can provide, ports are shut down based on their priority level. The switch will start from shutting down ports that have the low priority and the highest port number.

**Parameters:**

{ low | high | critical }: Specify port priority for this specific interface.

**Negation:** (config-if)# no poe priority

### 3.9.34.12 (config-if)# poe schedule

**Syntax:** (config-if)# poe schedule

**Explanation:** Enable PoE port scheduling function on this specific interface.

**Negation:** (config-if)# no poe schedule

### 3.9.34.13 (config-if)# poe schedule monday

**Syntax:** (config-if)# poe schedule monday

**Explanation:** Enable PoE Monday scheduling function on this specific interface.

**Negation:** (config-if)# no poe schedule monday

### 3.9.34.14 (config-if)# poe schedule monday { start-time <v_start_time> }

**Syntax:** (config-if)# poe schedule monday { start-time <v_start_time> }

**Explanation:** Configure the start time for PoE Monday scheduling function on this specific interface.

**Parameters:**

{ start-time <v_start_time> }: Specify the start time. Valid range is 0 to 23. The default value is 0.

**Negation:** (config-if)# no poe schedule monday

### 3.9.34.15 (config-if)# poe schedule monday { end-time <v_end_time> }

**Syntax:** (config-if)# poe schedule monday { end-time <v_end_time> }

**Explanation:** Configure the end time for PoE Monday scheduling function on this specific interface.

**Parameters:**

{ end-time <v_end_time> }: Specify the end time. Valid range is 0 to 23. The default value is 23.

**Negation:** (config-if)# no poe schedule monday

### 3.9.34.16 (config-if)# poe schedule tuesday

**Syntax:** (config-if)# poe schedule tuesday

**Explanation:** Enable PoE Tuesday scheduling function on this specific interface.

**Negation:** (config-if)# no poe schedule tuesday

### 3.9.34.17 (config-if)# poe schedule tuesday { start-time <v_start_time> }

**Syntax:** (config-if)# poe schedule tuesday { start-time <v_start_time> }

**Explanation:** Configure the start time for PoE Tuesday scheduling function on this specific interface.

**Parameters:**

{ start-time <v_start_time> }: Specify the start time. Valid range is 0 to 23. The default value is 0.

**Negation:** (config-if)# no poe schedule tuesday

### 3.9.34.18 (config-if)# poe schedule tuesday { end-time <v_end_time> }

**Syntax:** (config-if)# poe schedule tuesday { end-time <v_end_time> }

**Explanation:** Configure the end time for PoE Tuesday scheduling function on this specific interface.

**Parameters:**

{ end-time <v_end_time> }: Specify the end time. Valid range is 0 to 23. The default value is 23.

**Negation:** (config-if)# no poe schedule tuesday

#### *3.9.34.19 (config-if)# poe schedule wednesday*

**Syntax:** (config-if)# poe schedule wednesday

**Explanation:** Enable PoE Wednesday scheduling function on this specific interface.

**Negation:** (config-if)# no poe schedule wednesday

#### *3.9.34.20 (config-if)# poe schedule wednesday{ start-time <v_start_time> }*

**Syntax:** (config-if)# poe schedule wednesday { start-time <v_start_time> }

**Explanation:** Configure the start time for PoE Wednesday scheduling function on this specific interface.

**Parameters:**

{ start-time <v_start_time> }: Specify the start time. Valid range is 0 to 23. The default value is 0.

**Negation:** (config-if)# no poe schedule wednesday

#### *3.9.34.21 (config-if)# poe schedule wednesday { end-time <v_end_time> }*

**Syntax:** (config-if)# poe schedule wednesday { end-time <v_end_time> }

**Explanation:** Configure the end time for PoE Wednesday scheduling function on this specific interface.

**Parameters:**

{ end-time <v_end_time> }: Specify the end time. Valid range is 0 to 23. The default value is 23.

**Negation:** (config-if)# no poe schedule wednesday

#### *3.9.34.22 (config-if)# poe schedule thursday*

**Syntax:** (config-if)# poe schedule thursday

**Explanation:** Enable PoE Thursday scheduling function on this specific interface.

**Negation:** (config-if)# no poe schedule thursday

#### *3.9.34.23 (config-if)# poe schedule thursday { start-time <v_start_time> }*

**Syntax:** (config-if)# poe schedule thursday { start-time <v_start_time> }

**Explanation:** Configure the start time for PoE Thursday scheduling function on this specific interface.

**Parameters:**

{ start-time <v_start_time> }: Specify the start time. Valid range is 0 to 23. The default value is 0.

**Negation:** (config-if)# no poe schedule thursday

### *3.9.34.24 (config-if)# poe schedule thursday { end-time <v_end_time> }*

**Syntax:** (config-if)# poe schedule thursday { end-time <v_end_time> }

**Explanation:** Configure the end time for PoE Thursday scheduling function on this specific interface.

**Parameters:**

{ end-time <v_end_time> }: Specify the end time. Valid range is 0 to 23. The default value is 23.

**Negation:** (config-if)# no poe schedule thursday

### *3.9.34.25 (config-if)# poe schedule friday*

**Syntax:** (config-if)# poe schedule friday

**Explanation:** Enable PoE Friday scheduling function on this specific interface.

**Negation:** (config-if)# no poe schedule friday

### *3.9.34.26 (config-if)# poe schedule friday { start-time <v_start_time> }*

**Syntax:** (config-if)# poe schedule friday { start-time <v_start_time> }

**Explanation:** Configure the start time for PoE Friday scheduling function on this specific interface.

**Parameters:**

{ start-time <v_start_time> }: Specify the start time. Valid range is 0 to 23. The default value is 0.

**Negation:** (config-if)# no poe schedule friday

### *3.9.34.27 (config-if)# poe schedule friday { end-time <v_end_time> }*

**Syntax:** (config-if)# poe schedule friday { end-time <v_end_time> }

**Explanation:** Configure the end time for PoE Friday scheduling function on this specific interface.

**Parameters:**

{ end-time <v_end_time> }: Specify the end time. Valid range is 0 to 23. The default value is 23.

**Negation:** (config-if)# no poe schedule friday

### *3.9.34.28 (config-if)# poe schedule saturday*

**Syntax:** (config-if)# poe schedule saturday

**Explanation:** Enable PoE Saturday scheduling function on this specific interface.

**Negation:** (config-if)# no poe schedule saturday

### *3.9.34.29 (config-if)# poe schedule saturday { start-time <v_start_time> }*

**Syntax:** (config-if)# poe schedule saturday { start-time <v_start_time> }

**Explanation:** Configure the start time for PoE Saturday scheduling function on this specific interface.

**Parameters:**

{ start-time <v_start_time> }: Specify the start time. Valid range is 0 to 23. The default value is 0.

**Negation:** (config-if)# no poe schedule saturday

### *3.9.34.30 (config-if)# poe schedule saturday { end-time <v_end_time> }*

**Syntax:** (config-if)# poe schedule saturday { end-time <v_end_time> }

**Explanation:** Configure the end time for PoE Saturday scheduling function on this specific interface.

**Parameters:**

{ end-time <v_end_time> }: Specify the end time. Valid range is 0 to 23. The default value is 23.

**Negation:** (config-if)# no poe schedule saturday

### *3.9.34.31 (config-if)# poe schedule sunday*

**Syntax:** (config-if)# poe schedule sunday

**Explanation:** Enable PoE Sunday scheduling function on this specific interface.

**Negation:** (config-if)# no poe schedule sunday

### *3.9.34.32 (config-if)# poe schedule sunday { start-time <v_start_time> }*

**Syntax:** (config-if)# poe schedule sunday { start-time <v_start_time> }

**Explanation:** Configure the start time for PoE Sunday scheduling function on this specific interface.

**Parameters:**

{ start-time <v_start_time> }: Specify the start time. Valid range is 0 to 23. The default value is 0.

**Negation:** (config-if)# no poe schedule sunday

#### 3.9.34.33 (config-if)# poe schedule sunday { end-time <v_end_time> }

**Syntax:** (config-if)# poe schedule sunday { end-time <v_end_time> }

**Explanation:** Configure the end time for PoE Sunday scheduling function on this specific interface.

**Parameters:**

{ end-time <v_end_time> }: Specify the end time. Valid range is 0 to 23. The default value is 23.

**Negation:** (config-if)# no poe schedule sunday

### 3.9.35 (config)# port-security

#### 3.9.35.1 (config)# port-security

**Syntax:** (config)# port-security

**Explanation:** Enable port security function globally.

**Example:** Enable port security function globally.

```
# config t
(config)# port-security
```

**Negation:** (config)# no port-security

**Show: >** show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]

#### 3.9.35.2 (config)# port-security aging

**Syntax:** (config)# port-security aging

**Explanation:** Enable port security aging function. If enabled, secured MAC addresses are subject to aging as discussed in "Aging time" command. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

**Example:** Enable port security aging function.

```
# config t
(config)# port-security aging
```

**Negation:** (config)# no port-security aging

**Show:** > show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]

#### *3.9.35.3 (config)# port-security aging time*

**Syntax:** (config)# port-security aging time <v_10_to_10000000>

**Explanation:** Configure a desired aging time value. If "Aging" is enabled, secured MAC addresses are subject to aging as discussed this command. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

**Parameters:**

<v_10_to_10000000>: Specify the aging time value. The allowed range is between 10 and 10,000,000 seconds.

**Example:** Set the aging time value to 1800 seconds.

```
# config t
(config)# port-security aging time 1800
```

**Negation:** (config)# no port-security aging time

**Show:** > show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]

#### *3.9.35.4 (config)# port-security link-detection*

**Syntax:** (config)# port-security link-detection

**Explanation:** Enable link detection function globally.

**Example:** Enable link detection function globally.

```
# config t
(config)# port-security link-detection
(config)#
```

**Negation:** (config)# no port-security link-detection

**Show:** # show running-config

#### *3.9.35.5 (config-if)# port-security*

**Syntax:** (configt-if)# port-security

**Explanation:** Enable the port security function on the selected ports.

**Example:** Enable Gigabit Ethernet port 1-10's port security function.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# port-security
```

**Negation:** (configt-if)# no port-security

**Show:** > show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### *3.9.35.6 (config-if)# port-security link-detection*

**Syntax:** (configt-if)# port-security link-detection

**Explanation:** Enable link-detection function on the selected ports.

**Example:** Enable Gigabit Ethernet port 5's link detection function.

```
# config t
(config)# interface gigabitethernet 1/5
(config-if)# port-security link-detection
(config-if)#
```

**Negation:** (configt-if)# no port-security link-detection

**Show:** > show running-config
# show running-config

### *3.9.35.7 (config-if)# port-security link-detection action*

**Syntax:** (configt-if)# port-security link-detection action { trap | shutdown | trap-shutdown }

**Explanation:** Specify a link detection action. When the specified link detection condition occurs, the specified action will be triggered.

**Parameters:**

{ trap | shutdown | trap-shutdown }: Specify one of the actions taken when the link detection condition occurs.

**trap:** If the selected link condition occurs on a port, a SNMP trap will be sent.

**shutdown:** If the selected link condition occurs on a port, the corresponding port will be shutdown. When the port is shutdown, there are four ways to open or activate the shutdown port.

(1) Reboot the switch.
(2) Disable and re-enable on the shutdown port.
(3) Select other link conditions or action modes.
(4) Click the "Reopen" button on the shutdown port to open the port.

**trap-shutdown:** If the selected link condition occurs on a port, a SNMP trap will be sent and the corresponding port will be shutdown. When the port is shutdown, there are four ways to open the port.

(1) Reboot the switch.
(2) Disable and re-enable on the shutdown port.
(3) Select other link conditions or action modes.
(4) Click the "Reopen" button on the shutdown port to open the port.

**Example:** Send a SNMP trap when the specified link detection condition occurs.

```
# config t
(config)# interface gigabitethernet 1/5
(config-if)# port-security link-detection action trap
(config-if)#
```

**Negation:** (configt-if)# no port-security link-detection action { trap | shutdown | trap-shutdown }

### 3.9.35.8 (config-if)# port-security link-detection condition

**Syntax:** (configt-if)# port-security link-detection condition { link-down | link-up | link-down-and-up }

**Explanation:** Specify a link detection condition. When the specified link detection condition occurs, the specified action will be triggered.

**Parameters:**

{ link-down | link-up | link-down-and-up }: Specify one of the conditions that apply to the specified action.

l**ink-down:** If the link is changed from up to down, the device will trigger the selected action.

l**ink-up:** If the link is changed from down to up, the device will trigger the selected action.

**link-down-and-up:** If the link is changed from up to down and then up again, the device will trigger the selected action.

**Example:** When link down occurs on Port 5, shutdown the port.

```
# config t
(config)# interface gigabitethernet 1/5
(config-if)# port-security link-detection action shutdown
(config-if)# port-security link-detection condition link-down
(config-if)#
```

**Negation:** (configt-if)# no port-security link-detection condition { link-down | link-up | link-down-and-up }

### 3.9.35.9 (config-if)# port-security maximum

**Syntax:** (configt-if)# port-security maximum [ <v_1_to_1024> ]

**Explanation:** The maximum number of MAC addresses that can be secured on this port. The number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

**Parameters:**

[ <v_1_to_1024> ]: Specify a value between 1 and 1024.

**Example:** Limit Gigabit Ethernet port 1-10's MAC addresses can be learnt to 5.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# port-security maximum 5
```

**Negation:** (configt-if)# no port-security maximum

**Show:** > show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### *3.9.35.10 (config-if)# port-security violation*

**Syntax:** (configt-if)# port-security violation { protect | trap | trap-shutdown | shutdown }

**Explanation:** If the limit is exceeded, the specified action will take effect.

**Parameters:**

{ protect | trap | trap-shutdown | shutdown }: Specify one of the actions taken when the limit is exceeded.

**protect:** Do not allow more than the specified limit of MAC addresses to access on a port. No action is further taken.

**trap:** If Limit + 1 MAC addresses are seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit is exceeded.

**trap-shutdown:** If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

**shutdown:** If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new addresses will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:
* Boot the switch
* Disable and re-enable Limit Control on the port or the switch
* Click the "Reopen" button

**Example:** Send a SNMP trap when the limit is exceeded.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# port-security violation trap
```

**Negation:** (configt-if)# no port-security violation

**Show:** > show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]

### 3.9.36 (config)# privilege

**Syntax:** (config)# privilege { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile } level <privilege> <cmd>

**Explanation:** This command is used to change the privilege level of commands available in Configuration mode.

**Parameters:**

{ exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile }: Specify the group command that you want to configure.

level <privilege>: Specify the privilege level. The allowed range is 0 to 15.

<cmd>: Initial valid words and literals of the command to modify, in 128 characters.

**Example:** The following example sets the privilege level to 15 for any Exec mode (user or privileged) command 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 | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile } level <0-15> <cmd>

**Show:** > show privilege
# show privilege

### 3.9.37 (config)# ptp

#### 3.9.37.1 (config)# ptp <clockinst> domain

**Syntax:** (config)# ptp <clockinst> domain <domain>

**Explanation:** Configure the clock domain for PTP.

**Parameters:**
<clockinst: 0-3>: Specify the instance number.

<domain: 0-127>: Specify clock domain for PTP.

**Negation:** (config)# no ptp <clockinst> domain

**Show:** # show ptp <clockinst> local-clock

### 3.9.37.2 (config)# ptp <clockinst> filter

**Syntax:** (config)# ptp <clockinst> filter [ delay <delay> ] [ period <period> ] [ dist <dist> ]

**Explanation:** Configure the clock filter for PTP.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

[ delay <delay: 0-6> ]: Set delay parameter.

[ period <period: 1-10000> ]: Specify measurement period in number of sync events. The valid value is from 1 to 10000.

**Negation:** (config)# no ptp <clockinst> filter

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }
# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

### 3.9.37.3 (config)# ptp <clockinst> mode

**Syntax:** (config)# ptp <clockinst> mode { boundary | e2etransparent | p2ptransparent | master | slave } [ onestep | twostep ] [ ethernet | ip4multi | ip4unicast ] [ oneway | twoway ] [ id <v_clock_id> ] [ vid <vid> [ <prio> ] [ tag ] ]

**Explanation:** Configure details of a PTP clock instance.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

{ boundary | e2etransparent | p2ptransparent | master | slave }: Indicate the mode of the clock instance. There are five device modes, these are: boundary, End-to-end transparent clock, Peer-to-peer transparent clock, master only clock, slave only clock.

[ onestep | twostep ]: Onestep or twostep mode.

[ ethernet | ip4multi | ip4unicast ]: Specify transport protocol used by the PTP protocol engine. There are three options available, these are: Etherent PTP over Ethernet Multicast, PTP over IPv4 Multicast, PTP over IPv4 Unicast.

NOTE: IPv4 unicast protocol only works in Master Only and Slave Only clocks

[ oneway | twoway ]: Specify one-way or two-way measurement is used.

[ id <v_clock_id> ]: Specify clock ID.

[ vid <vid> [ <prio> ] [ tag ] ]: Specify VLAN ID and Priority code point (PCP) values used for PTP frames. Enable VLAN tagging for PTP frames if needed.

**Negation:** (config)# no ptp <clockinst> mode { boundary | e2etransparent | p2ptransparent | master | slave }

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

### 3.9.37.4 (config)# ptp <clockinst> priority1

**Syntax:** (config)# ptp <clockinst> priority1 <priority1>

**Explanation:** Configure the PTP priority 1.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

<priority1: 0-255>: Specify Clock priority 1 for PTP BMC algorithm (0 is highest priority).

**Negation:** (config)# no ptp <clockinst> priority1

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }
# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

### 3.9.37.5 (config)# ptp <clockinst> priority2

**Syntax:** (config)# ptp <clockinst> priority2 <priority2>

**Explanation:** Configure the PTP priority 2.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

<priority2: 0-255>: Specify Clock priority 2 for PTP BMC algorithm (0 is highest priority).

**Negation:** (config)# no ptp <clockinst> priority2

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }
# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

### 3.9.37.6 (config)# ptp <clockinst> time-property

**Syntax:** (config)# ptp <clockinst> time-property [ utc-offset <utc_offset> ] [ valid ] [ leap-59 | leap-61 ] [ time-traceable ] [ freq-traceable ] [ ptptimescale ] [ time-source <time_source> ]

**Explanation:** This command defines members needed to interpret the time provided in PTP messages. The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, i.e. the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

[ utc-offset <utc_offset> ]: Specify UTC Offset value. Valid range is -32768 to 32767.

[ valid ]: Specify “valid” to denote UTC Valid is True.

[ leap-59 | leap-61 ]: Specify one of the option.

[ time-traceable ]: Specify this to denote time-traceable “True”.

[ freq-traceable ]: Specify this to denote freq-traceable “True”.

[ ptptimescale ]: Specify this to denote ptptimescale “True”.

[ time-source <time_source> ]: Specify time source value. Valid range is 0 to 255.

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }
# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

### 3.9.37.7 (config)# ptp <clockinst> uni

**Syntax:** (config)# ptp <clockinst> uni <idx> [ duration <duration> ] <ip>

**Explanation:** When operating in IPv4 Unicast mode, the slave is configured up to 5 master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then request Sync messages from the selected master.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

<idx: 0-4>: Specify index number in the Slave table.

[ duration <duration: 10-1000> ]: Specify the number of seconds for which the Announce/Sync messages are requested.

<ip>: Specify IPv4 address of requested master clock.

**Negation:** (config)# no ptp <clockinst> uni <idx>

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }
# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

#### *3.9.37.8 (config-if)# ptp <clockinst>*

**Syntax:** (config-if)# ptp <clockinst>

**Explanation:** Apply the PTP clock instance rule to this specific interface.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

**Negation:** (config-if)# no ptp <clockinst>

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }
# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

#### *3.9.37.9 (config-if)# ptp <clockinst> announce*

**Syntax:** (config-if)# ptp <clockinst> announce { [ interval <interval> ] [ timeout <timeout> ] }*1

**Explanation:** Configure the settings for announce timing messages.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

{ [ interval <interval> ] [ timeout <timeout> ] }*1: Specify the time for sending announce messages. The range is 0 to 4 seconds. For timeout value, specify the time for announcing timeout messages. The range is 2 to 10 seconds.

**Negation:** (config-if)# no ptp <clockinst> announce { interval | timeout }

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }
# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

#### *3.9.37.10 (config-if)# ptp <clockinst> delay-asymmetry*

**Syntax:** (config-if)# ptp <clockinst> delay-asymmetry <delay_asymmetry>

**Explanation:** If the transmission delay for a link in not symmetric, the asymmetry can be configured using this command.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

<delay_asymmetry>: Specify delay asymmetry value in ns. The valid range is -100000-100000.

**Negation:** (config-if)# no ptp <clockinst> delay-asymmetry

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }
# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

### *3.9.37.11 (config-if)# ptp <clockinst> delay-mechanism { e2e | p2p }*

**Syntax:** (config-if)# ptp <clockinst> delay-mechanism { e2e | p2p }

**Explanation:** Configure member delay Mechanism for this specific interface.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

{ e2e | p2p }: Configure delay mechanism used for the port. This can be defined per port in an Ordinary/Boundary clock. In a transparent clock, all ports use the same delay mechanism, determined by the clock type.

**e2e:** End to end delay measurement

**p2p:** Peer to peer delay measurement.

**Negation:** (config-if)# no ptp <clockinst> delay-asymmetry

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }
# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

### *3.9.37.12 (config-if)# ptp <clockinst> delay-req interval <interval>*

**Syntax:** (config-if)# ptp <clockinst> delay-req interval <interval>

**Explanation:** Configure the time recommended to the member devices to send delay request messages when the port is in the master state.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

<interval>: Specify delay requestion message interval. The valid range -7 to 5.

**Negation:** (config-if)# no ptp <clockinst> delay-req interval

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }
# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

### 3.9.37.13 (config-if)# ptp <clockinst> egress-latency <egress_latency>

**Syntax:** (config-if)# ptp <clockinst> egress-latency <egress_latency>

**Explanation:** Configure Egress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

<egress_latency>: Specify egress latency. The range is -100000 to 100000.

**Negation:** (config-if)# no ptp <clockinst> egress-latency

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }
# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

### 3.9.37.14 (config-if)# ptp <clockinst> ingress-latency <ingress_latency>

**Syntax:** (config-if)# ptp <clockinst> ingress-latency <ingress_latency>

**Explanation:** Configure ingress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

<ingress_latency>: Specify ingress latency. The range is -100000 to 100000.

**Negation:** (config-if)# no ptp <clockinst> ingress-latency

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }
# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

### 3.9.37.15 (config-if)# ptp <clockinst> sync-interval <interval>

**Syntax:** (config-if)# ptp <clockinst> sync-interval <interval>

**Explanation:** Configure the interval for issuing sync messages in master.

**Parameters:**

<clockinst: 0-3>: Specify the instance number.

<interval>: Specify the interval for issuing sync messages. The range is -7 to 4.

**Negation:** (config-if)# no ptp <clockinst> sync-interval

**Show:** > show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }
# show ptp <clockinst> { default | current | parent | time-property | filter | uni | slave | { { port-state | port-ds } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } }

## *3.9.38 (config-if)# pvlan*

### *3.9.38.1 (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>

### *3.9.38.2 (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>] ) ]

## *3.9.39 (config)# qos*

### *3.9.39.1 (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> ] } ]

### *3.9.39.2 (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> ] } ]

### *3.9.39.3 (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> ] } ]

### 3.9.39.4 (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> ] } ]

### 3.9.39.5 (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> ] } ]

### *3.9.39.6 (config)# qos qce refresh*

**Syntax:** (config)# qos qce refresh

**Explanation:** To refresh QCE.

**Example:** Refresh QCE.

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

### *3.9.39.7 (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> ] } ]

### *3.9.39.8 (config)# qos storm*

**Syntax:** (config)# qos storm { unicast | multicast | broadcast } { { <rate> [ kfps ] } | { 1024 kfps } }

**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

### *3.9.39.9 (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> ] } ]

### *3.9.39.10 (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> ] } ]

### *3.9.39.11 (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> ] } ]

### *3.9.39.12 (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> ] } ]

### *3.9.39.13 (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> ] } ]

### *3.9.39.14 (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> ] } ]

### *3.9.39.15 (config-if)# qos map cos-tag cos*

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

**Explanation:** Configure (QoS class, DP level) to (PCP, DEI) Mapping of QoS for specific interface.

**Parameters:**

cos <cos: 0-7>: Specify a QoS class value.

dpl <dpl:0-1>: Specify a DPL value (0 or 1).

pcp <pcp: 0-7>: Specify a PCP (Priority Code Point) value.

dei <dei: 0-1>: Specify a DEI value (0 or 1).

**Negation**: (config-if)# no qos map cos-tag cos <cos> dpl <dpl>

**Show:** # show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]

### 3.9.39.16 (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> ] } ]

### 3.9.39.17 (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> ] } ]

### 3.9.39.18 (config-if)# qos policer

**Syntax:** (config-if)# qos policer <rate> [ fps ] [ 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.

[ fps ]: Rate is fps. 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> ] } ]

### *3.9.39.19 (config-if)# qos queue-policer queue*

**Syntax:** (config-if)# qos queue-policer queue <queue> <rate>

**Explanation:** Configure Ingress Queue Policers Rate of QoS for specific interface.

**Parameters:**

<queue: 0-7>: Specify a queue or a range.

<rate: 100-3300000>: 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> ] } ]

### *3.9.39.20 (config-if)# qos queue-shaper queue*

**Syntax:** (config-if)# qos queue-shaper queue <queue> <rate> [ excess ]

**Explanation:** Configure Egress Queue Policers Rate of QoS for specific interface.

**Parameters:**

<queue: 0-7>: Specify a queue or a range.

<rate: 100-3300000>: Specify Policer rate in kbps.

[ excess ]: Allow all excess bandwidth.

**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> ] } ]

### *3.9.39.21 (config-if)# qos shaper*

**Syntax:** (config-if)# qos shaper <rate>

**Explanation:** Configure Egress Queue Policers Rate of QoS for specific interface.

**Parameters:**

<rate: 100-3300000>: Specify Policer rate in kbps.

**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> ] } ]

### *3.9.39.22 (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> ] } ]

### *3.9.39.23 (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> ] } ]

### *3.9.39.24 (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> ] } ]

### 3.9.39.25 (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> ] } ]

## 3.9.40 (config)# radius-server

### 3.9.40.1 (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.

```
# config t
(config)# radius-server attribute 32 cabinet5aSW
```

**Negation:** (config)# no radius-server attribute 32

**Show:** # show radius-server [statistics]

### 3.9.40.2 (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]

### 3.9.40.3 (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]

### 3.9.40.4 (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]

### 3.9.40.5 (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]

### 3.9.40.6 (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

### 3.9.40.7 (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]

### 3.9.40.8 (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]

### *3.9.41 (config)# ring*

#### *3.9.41.1 (config)# ring <instance> chain*

**Syntax:** (config)# ring <instance> chain [ master ] east interface <port_type> <east_port> [ edge ] west interface <port_type> <west_port> [ edge ]

**Parameters:**

<instance: 0-5>: Specify the ring instance number.

chain: This is a chain ring.

[ master ]: Set this ring to master ring.

east interface <port_type> <east_port> [ edge ]: Specify the east port type (Fast Ethernet or Gigabit Ethernet) and port number. If this port is the edge port, add “edge” after the port number.

west interface <port_type> <west_port> [ edge ]: Specify the west port type (Fast Ethernet or Gigabit Ethernet) and port number. If this port is the edge port, add “edge” after the port number.

**Explanation:** Create a chain ring instance.

**Example:** Create a chain instance 1.

```
# config t
(config)# ring 1 chain east interface GigabitEthernet 1/1 west interface
GigabitEthernet 1/2
```

**Negation:** (config)# no ring <instance>

**Show:** # show ring [ <instances> ]

#### *3.9.41.2 (config)# ring <instance> ring*

**Syntax:** (config)# ring <instance> ring [ master ] east interface <port_type> <east_port>  west interface <port_type> <west_port>

**Parameters:**

<instance: 0-5>: Specify the ring instance number.

ring: This is a closed ring type.

[ master ]: Set this ring to master ring.

east interface <port_type> <east_port>: Specify the east port type (Fast Ethernet or Gigabit Ethernet) and port number.

west interface <port_type> <west_port>: Specify the west port type (Fast Ethernet or Gigabit Ethernet) and port number.

**Explanation:** Create a closed ring instance.

**Example:** Create a ring instance 2.

```
# config t
(config)# ring 2 ring east interface GigabitEthernet 1/3 west interface
GigabitEthernet 1/4
```

**Negation:** (config)# no ring <instance>

**Show:** # show ring [ <instances> ]

#### 3.9.41.3 (config)# ring <instance> sub

**Syntax:** (config)# ring <instance> sub [ master ] east interface <port_type> <east_port>

**Parameters:**

<instance: 0-5>: Specify the ring instance number.

sub: This is a sub-ring type.

[ master ]: Set this ring to master ring.

east interface <port_type> <east_port>: Specify the east port type (Fast Ethernet or Gigabit Ethernet) and port number.

**Explanation:** Create a sub ring instance.

**Example:** Create a ring instance 3.

```
# config t
(config)# ring 3 ring east interface GigabitEthernet 1/1
```

**Negation:** (config)# no ring <instance>

**Show:** # show ring [ <instances> ]

### 3.9.42 (config)# rmon

#### 3.9.42.1 (config)# rmon alarm

**Syntax:** (config)# rmon alarm <id> <oid_str> <interval> { absolute | delta } rising-threshold <rising_threshold> [ <rising_event_id> ] falling-threshold <falling_threshold> [ <falling_event_id> ] { [ rising | falling | both ] }

**Syntax:** (config)# rmon alarm <id> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors } <ifIndex> <interval> { absolute | delta } rising-threshold <rising_threshold> [ <rising_event_id> ] falling-threshold <falling_threshold> [ <falling_event_id> ] { [ rising | falling | both ] }

**Explanation:** Configure RMON alarm settings. RMON Alarm configuration defines specific criteria that will generate response events. It can be set to test data over any specified time interval and can monitor absolute or changing values. Alarms can also be set to respond to rising or falling thresholds.

**Parameters:**

<id>: Indicates the index of the entry. The range is from 1 to 65535.

<oid_str>: The object number of the MIB variable to be sampled. Only variables of the type ifEntry.n.n may be sampled. Possible variables are ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifOutDiscards, ifErrors, ifInUnknownProtos, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, ifOutDiscards, ifOutErrors.

<interval>: The polling interval for sampling and comparing the rising and falling threshold. The range is from 1to 2^31 (2147483647) seconds.

{ absolute | delta }: Test for absolute or relative change in the specified variable.

**Absolute:** The variable is compared to the thresholds at the end of the sampling period.

**Delta:** The last sample is subtracted from the current value and the difference is compared to the thresholds.

rising-threshold <rising_threshold>: If the current value is greater than the rising threshold and the last sample value is less than this threshold, then an alarm will be triggered. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. The threshold range is -2147483647 to 2147483647.

[ <rising_event_id> ]: Indicates the rising index of an event. The range is 1 - 65535.

falling-threshold <falling_threshold>: If the current value is less than the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold. (Range: -2147483647 to 2147483647)

[ <falling_event_id> ]: Indicates the falling index of an event. The range is 0 - 65535.

{ [ rising | falling | both ] }: Specify a method that is used to sample the selected variable and calculate the value to be compared against the thresholds.

**rising:** Trigger alarm when the first value is larger than the rising threshold.

**falling:** Trigger alarm when the first value is less than the falling threshold.

**both:** Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold.

**Negation:** (config)# no rmon alarm <id>

**Show:** # show rmon alarm [ <id_list> ]
# show rmon history [ <id_list> ]
# show rmon statistics [ <id_list> ]

### *3.9.42.2(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> ]

### 3.9.42.3 (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> ]

### 3.9.42.4 (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> ]

### *3.9.43 (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

### *3.9.44 (config)# smtp*

#### *3.9.44.1 (config)# smtp*

**Syntax:** (config)# smtp

**Explanation:** Enable NTP client mode operation.

**Negation:** (config)# no smtp

**Show:** # show smtp status

#### *3.9.44.2 (config)# smtp auth*

**Syntax:** (config)# smtp auth

**Explanation:** Enable Server authentication.

**Negation:** (config)# no smtp auth

**Show:** # show smtp status

#### *3.9.44.3 (config)# smtp event*

**Syntax:** (config)# smtp event [ system [ warmstart ] [ coldstart ] ] [ power [ power1 ] [ power2 ] ] [ interface [ linkup ] [ linkdown ] [ poe ] ]

**Explanation:** Specify what events will result in alert email messages being generated and sent.

**Parameters:**

[ system [ warmstart ] [ coldstart ] ]: Enable Warm Start and Cold Start mail event.

[ power [ power1 ] [ power2 ] ]: Enable Power 1  and Power 2 status mail event.

[ interface [ linkup ] [ linkdown ] [ poe ] ]: Enable interface link up, linkdown, and PoE mail event.

**Negation:** (config)# no smtp event

**Show:** # show smtp status

### 3.9.44.4 (config)# smtp port

**Syntax:** (config)# smtp port [ <port_number> ]

**Explanation:** Set the SMTP port number. The default SMTP port is 25.

**Parameters:**

[ <port_number> ]: Specify SMTP port number.

**Show:** # show smtp status

### 3.9.44.5 (config)# smtp recipient

**Syntax:** (config)# smtp recipient <recipient_var> ip-address <word_var>

**Explanation:** Configure recipients' Email addresses. Up to four recipient's E-mail addresses may be entered. When alert events are triggered, email messages will be sent to the indicated email addresses.

**Parameters:**

recipient <recipient_var:1-4>: Specify the recipient number.

ip-address <word_var>: Specify the recipient's Email address.

**Negation:** (config)# no smtp recipient

**Show:** # show smtp status

### 3.9.44.6 (config)# smtp server ip-address

**Syntax:** (config)# smtp server ip-address <word_var>

**Explanation:** Configure SMTP server IP address.

**Parameters:**

ip-address <word_var>: Specify SMTP server IP address.

**Negation:** (config)# no smtp server

**Show:** # show smtp status

#### *3.9.44.7 (config)# smtp username <username> password encrypted*

**Syntax:** (config)# smtp username <username> password encrypted <encry_password>

**Explanation:** Configure username and encrypted password for SMTP server authentication.

**Parameters:**

username <username>: Specify the valid authentication username for SMTP server.

password encrypted <encry_password>: Enter the authentication password for username of SMTP server.

**Show:** # show smtp status

#### *3.9.44.8 (config)# smtp username <username> password none*

**Syntax:** (config)# smtp username <username> password none

**Explanation:** Configure username for SMTP server authentication.

**Parameters:**

username <username>: Specify the valid authentication username for SMTP server.

**Show:** # show smtp status

#### *3.9.44.9 (config)# smtp username <username> password unencrypted*

**Syntax:** (config)# smtp username <username> password unencrypted <password>

**Explanation:** Configure username and unencrypted password for SMTP server authentication.

**Parameters:**

username <username>: Specify the valid authentication username for SMTP server.

password unencrypted <encry_password>: Enter the authentication password for username of SMTP server.

**Show:** # show smtp status

### *3.9.45 (config)# snmp-server*

#### *3.9.45.1 (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

### 3.9.45.2 (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 } ]

### 3.9.45.3 (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

### *3.9.45.4 (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

### *3.9.45.5 (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

### 3.9.45.6 (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

### 3.9.45.7 (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 ]

### 3.9.45.8 (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

### 3.9.45.9 (config)# snmp-server security-to-group

**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> ]

### 3.9.45.10 (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

### 3.9.45.11 (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> ]

### *3.9.45.12 (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

### 3.9.45.13 (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> ]

### 3.9.45.14 (config-if)# snmp-server host <conf_name> alarm

**Syntax:** (config-if)# snmp-server host <conf_name> alarm [ linkdown ]

**Explanation:** Configure SNMP linkdown alarm for the selected interface.

**Parameters:**

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

alarm [ linkdown ]: Enable linkdown alarm.

**Show:** # show snmp alarm [ <conf_name> ] [ power ] [ interface ]

### 3.9.45.15 (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

### 3.9.45.16 (config-snmps-host)# alarm

**Syntax:** (config-snmps-host)# alarm [ power [ power1 ] [ power2 ] ]

**Explanation:** Configure power alarms for this host.

**Parameters:**

[ power [ power1 ] [ power2 ] ]: Initiate power alarms when Power 1 or Power 2 fails.

### 3.9.45.17 (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

### 3.9.45.18 (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

### *3.9.45.19 (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

### *3.9.45.20 (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

### *3.9.45.21 (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

### *3.9.45.22 (config-snmps-host)# traps*

**Syntax:** (config-snmps-host)# traps [ aaa authentication ] [ system [ coldstart ] [ warmstart ] ] [ switch [ stp ] [ rmon ] ]

**Explanation:** Configure SNMP trap events.

**Parameters:**

[ aaa authentication ]: Authentication, Authorization and Accounting. A trap will be issued at any 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 that 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 aaa authentication
```

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

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

## *3.9.46 (config)# spanning-tree*

### *3.9.46.1 (config)# spanning-tree aggregation*

**Syntax:** (config)# spanning-tree aggregation

**Explanation:** Enable aggregation mode of Spanning Tree.

```
# config t
(config)# spanning-tree aggregation
(config-stp-aggr)#
```

**Show:** # show spanning-tree

### *3.9.46.2 (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

### *3.9.46.3 (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

### 3.9.46.4 (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

### 3.9.46.5 (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

### 3.9.46.6 (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

### 3.9.46.7 (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

### *3.9.46.8 (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

### *3.9.46.9 (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

### *3.9.46.10 (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

### *3.9.46.11 (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

### *3.9.46.12 (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

### *3.9.46.13 (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

### *3.9.46.14 (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

### *3.9.46.15 (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

### 3.9.46.16 (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

### 3.9.46.17 (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

### 3.9.46.18 (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

### 3.9.46.19 (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

### 3.9.46.20 (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

### 3.9.46.21 (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

### 3.9.46.22 (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

### 3.9.46.23 (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

### 3.9.46.24 (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

### 3.9.46.25 (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

### 3.9.46.26 (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

### *3.9.46.27 (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

### *3.9.46.28 (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

#### 3.9.46.29 (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

#### 3.9.46.30 (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

### 3.9.47 (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

### 3.9.48 (config)# switchport

#### 3.9.48.1 (config)# switchport vlan mapping

**Syntax:** (config)# switchport vlan mapping <group ID> <vlan_list> <translation_vlan>

**Explanation:** VLAN Translation is especially useful for users who want to translate the original VLAN ID to a new VLAN ID so as to exchange data across different VLANs and improve VLAN scaling. VLAN translation replaces an incoming C-VLAN tag with an S-VLAN tag instead of adding an additional tag. When configuring VLAN Translation, both ends of the link normally must be able to replace tags appropriately. In other words, both ends must be configured to translate the C-VLAN tag to S-VLAN tag and S-VLAN tag to C-VLAN tag appropriately in a network. Note that only access ports support VLAN translation. It is not recommended to configure VLAN Translation on trunk ports.

**Parameters:**

<group ID: 1-28>: Indicate the Group ID that applies to this translation rule.

<vlan_list>: Indicate the VLAN ID that will be mapped to a new VID.

<translation_vlan>: Indicate the new VID to which VID of ingress frames will be changed.

**Example:** Map the group ID 5 with VLAN ID 100 to be translated to 201.

```
# config t
(config)# switchport vlan mapping 5 100 201
```

**Negation:** (config)# no switchport vlan mapping <group> <v_vlan_id_from>

### 3.9.48.2 (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

### 3.9.48.3 (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> } ]

### *3.9.48.4 (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

### *3.9.48.5 (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

### *3.9.48.6 (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

### *3.9.48.7 (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

### *3.9.48.8 (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

### *3.9.48.9 (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.

<table>
<tr><th>Action / Port Type</th><th>Ingress Action</th><th>Egress Action</th></tr>
<tr><td rowspan="2">Unaware</td><td>When a tagged frame is received on a port,<br>1. If the tagged frame with TPID=0x8100, it becomes a double-tag frame and is forwarded.<br>2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.</td><td rowspan="2">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.</td></tr>
<tr><td>When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.</td></tr>
<tr><td rowspan="2">C-port</td><td>When a tagged frame is received on a port,<br>1. If a tagged frame with TIPID=0x8100, it is forwarded.<br>2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.</td><td rowspan="2">The TPID of frame transmitted by C-port will be set to 0x8100.</td></tr>
<tr><td>When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.</td></tr>
<tr><td rowspan="2">S-port</td><td>When a tagged frame is received on a port,<br>1. If a tagged frame with TPID=0x88A8, it is forwarded.<br>2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.</td><td rowspan="2">The TPID of frame transmitted by S-port will be set to 0x88A8</td></tr>
<tr><td>When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.</td></tr>
<tr><td rowspan="2">S-custom port</td><td>When a tagged frame is received on a port,<br>1. If a tagged frame with TPID=0x88A8, it is forwarded.<br>2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.</td><td rowspan="2">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.</td></tr>
<tr><td>When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.</td></tr>
</table>

**Negation:** (config-if)# no switchport hybrid port-type

**Show:** # show vlan status

### *3.9.48.10 (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

### 3.9.48.11 (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

### 3.9.48.12 (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

### 3.9.48.13 (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

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

**Syntax:** (config-if)# switchport vlan ip-subnet id <vce_id> <ipv4> vlan <vid>

**Explanation:** IP Subnet-based VLAN configuration is to map untagged ingress frames to a specific VLAN if the source address is found in the IP subnet-to-VLAN mapping table. When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

**Parameters:**

<vce_id: 1-128>: Specify index of the entry. Valid range is 1~128.

<ipv4>: Specify IP address and subnet mask. The format is xx.xx.xx.xx/mm.mm.mm.mm.

<vid>: Indicate the VLAN ID.

**Negation:** (config-if)# no switchport vlan ip-subnet id <vce_id_list>

**Show:** # show vlan ip-subnet [ id <subnet_id> ]

### 3.9.48.15 (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> ]

### 3.9.48.16 (config-if)# switchport vlan mapping

**Syntax:** (config-if)# switchport vlan mapping <group>

**Explanation:** Configure group VLAN mapping table for this specific interface.

**Parameters:**

<group: 1-20>: Indicate the Group ID that applies to this rule.

**Negation:** (config-if)# no switchport vlan mapping

### 3.9.48.17 (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> ]

## 3.9.49 (config)# tacacs-server

### 3.9.49.1 (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

### 3.9.49.2 (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

### *3.9.49.3 (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

### *3.9.49.4 (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

### 3.9.50 (config)# upnp

#### 3.9.50.1 (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

#### 3.9.50.2 (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

#### 3.9.50.3 (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

## 3.9.51 (config)# username

### 3.9.51.1 (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

### 3.9.51.2 (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

### *3.9.51.3 (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

## 3.9.52 (config)# vlan

### 3.9.52.1 (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> }

### 3.9.52.2 (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> }

### 3.9.52.3 (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> ]

### *3.9.53 (config)# web privilege group*

**Syntax:** (config)# web privilege group <group_name> level { [ cro <cro> ] [ crw <crw> ] [ sro <sro> ] [ srw <srw> ] }*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:

cro (configuration read-only): The privilege level is 1 to 15.

crw (configuration/execute read-write): The privilege level is 1 to 15.

sro (status/statistics read-only): The privilege level is 1 to 15.

srw (status/statistics read-write): The privilege level is 1 to 15.

User Privilege should be the same or greater than the authorization Privilege level to have access to that group.

**Example:** Assign Aggregation group to crw (configuration/excute read-write) level 15.

```
# config t
(config)# web privilege group aggregation level crw 15
(config)# exit
# show web privilege group level
Group Name                        Privilege Level
                                  CRO CRW SRO SRW
-------------------------------- --- --- --- ---
Aggregation                         5  15   5  10
DHCP                                5  10   5  10
Dhcp_Client                         5  10   5  10
Diagnostics                         5  10   5  10
EEE                                 5  10   5  10
ERPS                                5  10   5  10
Green_Ethernet                      5  10   5  10
IP2                                 5  10   5  10
IPMC_Snooping                       5  10   5  10
LACP                                5  10   5  10
LLDP                                5  10   5  10
Loop_Protect                        5  10   5  10
MAC_Table                           5  10   5  10
Maintenance                        15  15  15  15
Mirroring                           5  10   5  10
MVR                                 5  10   5  10
NTP                                 5  10   5  10
POE                                 5  10   5  10
Ports                               5  10   1  10
-- more --, next page: Space, continue: g, quit: ^C
```

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

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

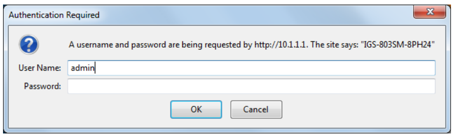
# CHAPTER 4. WEB OPERATION & CONFIGURATION

## 4.1 Home Page

Web-based management provides easy-to-use and straightforward graphic interface for users to configure the device quickly. The web-based management of this device supports various web browsers such as Internet Explorer (Version 9.0 or above is recommended), Firefox or Google Chrome. To access the web management interface for the first time or after returning the device back to factory defaults, enter the default IP address of the **IFS/IGS** in the browser's location bar. See below for explanations.

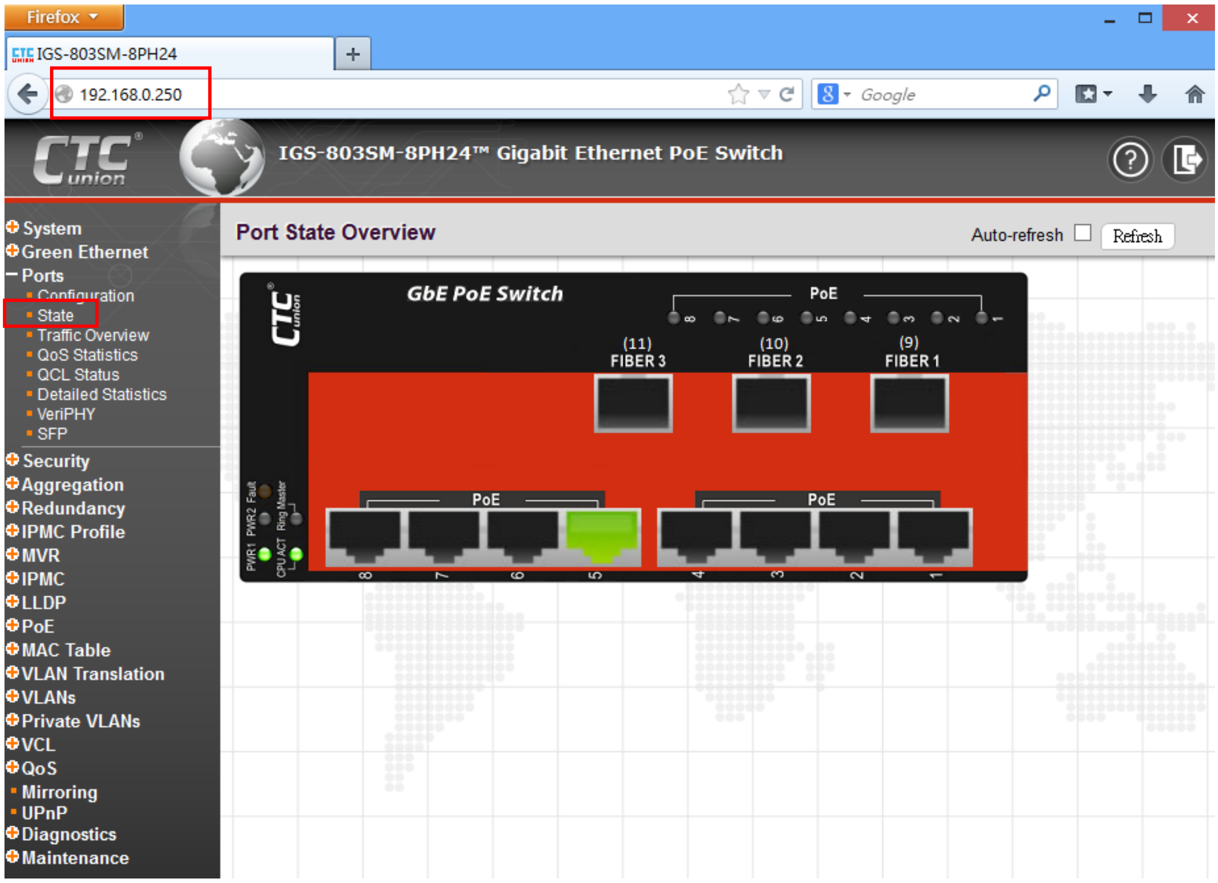
### *4.1.1 Login*

To enter the web based management for the first time or after returning the device back to factory defaults, input the default IP address "**10.1.1.1**" in your web browser. Then, a standard login prompt will appear depending on the type of browser used. The example below is with Firefox browser.




Enter the **IFS/IGS** factory default username "**admin**" with "**no password**". After successfully entering the web based management, the Port State page will appear.

***NOTE:*** *Both IFS/IGS devices have the same software functions despite of the difference in the number of ports. In this user manual, we use IGS-803SM-8PH24 Gigabit Ethernet Switch to demonstrate software functions. Therefore, if you purchase IFS devices, the Port State page and other pages involved with port configurations will be slightly different from the demonstrative screenshots provided in this manual.*




Web Home Page

### *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" port 1 LAN indicates a LAN connection with a speed of 100M. The "Amber" colored port 2 LAN and Fiber port 1 (9) indicates a connection speed of 1000M.

The status display can be reached by using the left side menu, and return to **Ports>State**.

### *4.1.3 Refresh*

To update the screen, click the "Refresh" button. For automatic updating of the screen, the "Auto-refresh" tick box may be ticked. The screen will be auto refreshed every 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.

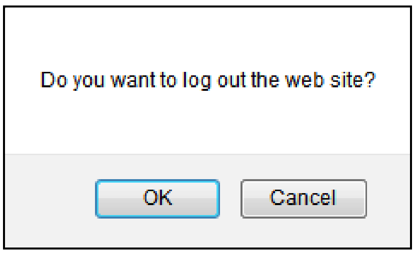
### *4.1.4 Help System*

The **IFS/IGS803 Series** has an online "help" system to aid the engineer when setting the parameters of the device. Each functional setting page is accompanied by a specific "help" for that functional page. The user can display this help "pop up" at any time by clicking the "help" icon.

### *4.1.5 Logout*

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

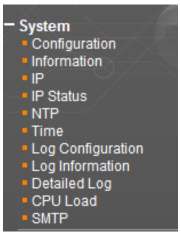
After clicking the logout icon, a confirmation screen will be displayed. Click "OK" to finish logging out or click "Cancel" to return to the web configuration GUI.




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.

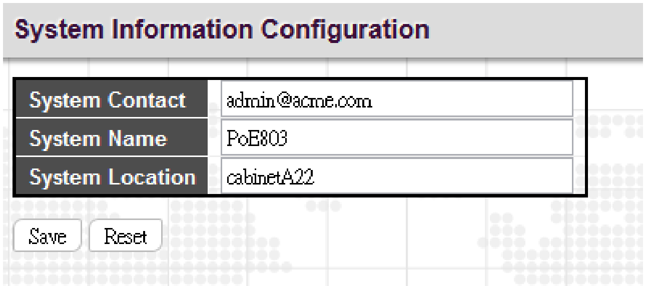
## 4.2 System

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.



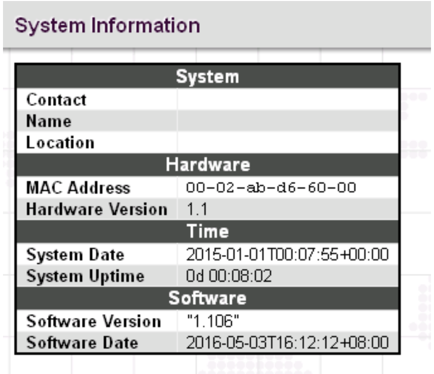

**System Contact:** Indicate the descriptive contact information. This could be a person’s name, email address or other descriptions. The allowed string length is 0~255 and the allowed content is the ASCII characters from 32~126.

**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.

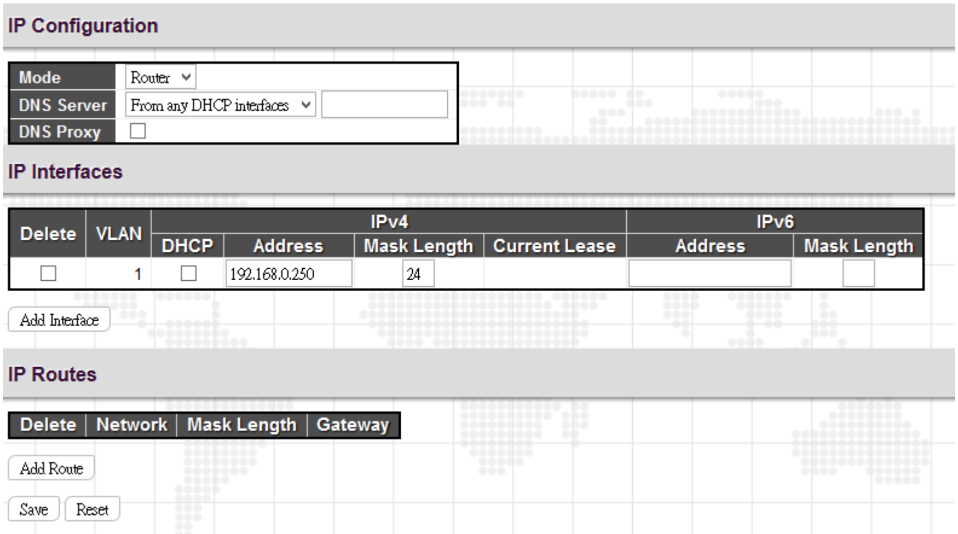
### 4.2.2 System Information

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.

**DNS Server:** This setting controls the DNS name resolution done by the switch. The following modes are supported:

**From any DHCP interfaces:** The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.

**No DNS server:** No DNS server will be used.

**Configured:** Explicitly provide the IP address of the DNS Server in dotted decimal notation.

**From this DHCP interface:** Specify from which DHCP-enabled interface a provided DNS server should be preferred.

**DNS Proxy:** When DNS proxy is enabled, the system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.

***IP Interface***

Click "Add Interface" to add a new IP interface. A maximum of 8 interfaces is supported.

**VLAN:** This is the VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.

**DHCP:** 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.

**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.

**IPv4 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.

**IPv6 Mask:** 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.

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

**Gateway:** This is the IP address of the gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.

### 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 **IFS/IGS-803** 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.

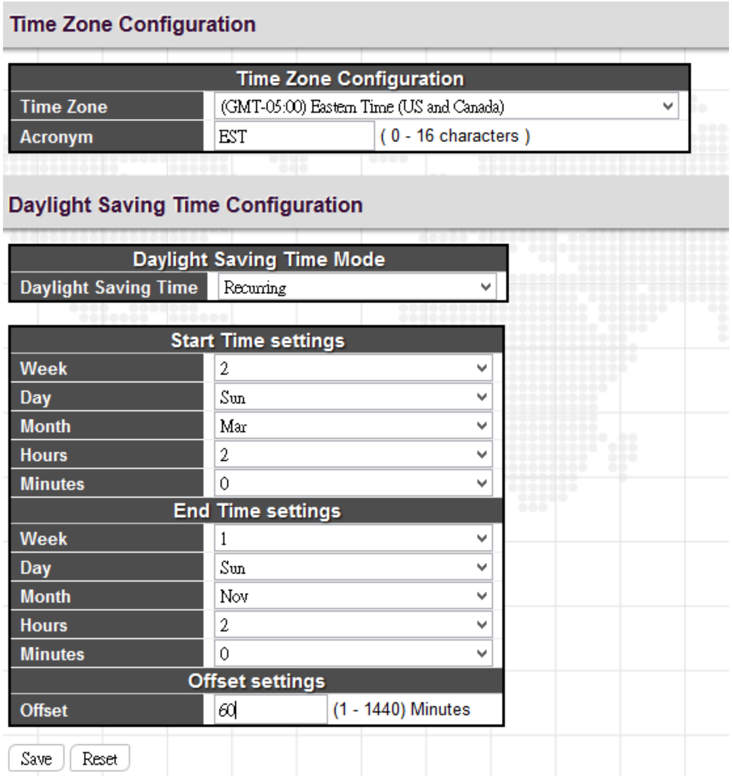
**Disabled:** Disable NTP client mode operation.

**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.




The setting example above is for Eastern Standard Time in the United States. Daylight savings time starts on the second Sunday in March at 2:00AM. Daylight savings ends on the first Sunday in November at 2:00AM. The daylight savings time offset is 60 minutes (1 hour).

***<u>Time Zone Configuration</u>***

**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.

***<u>Daylight Saving Time Configuration</u>***

**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:**

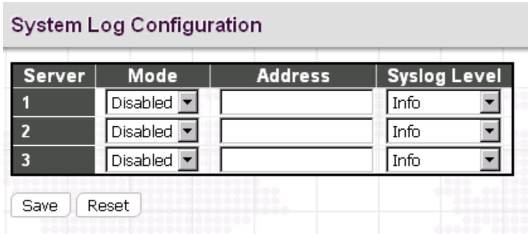
**Start time settings:** Select the starting week, day, month, year, hours, and minutes.

**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 System Log 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:

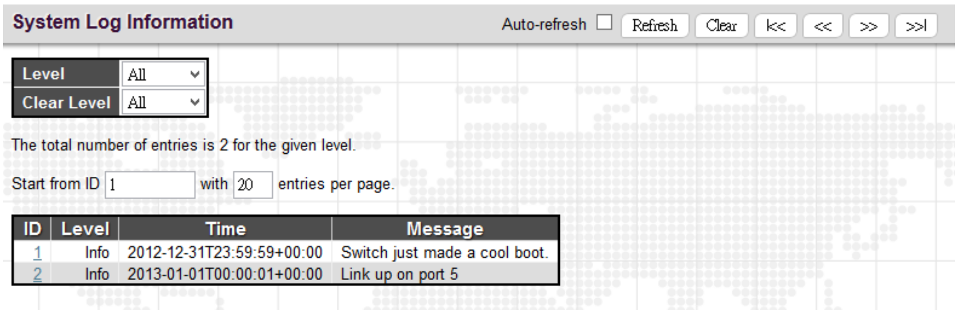
**Info:** Send information, warnings and errors.

**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.

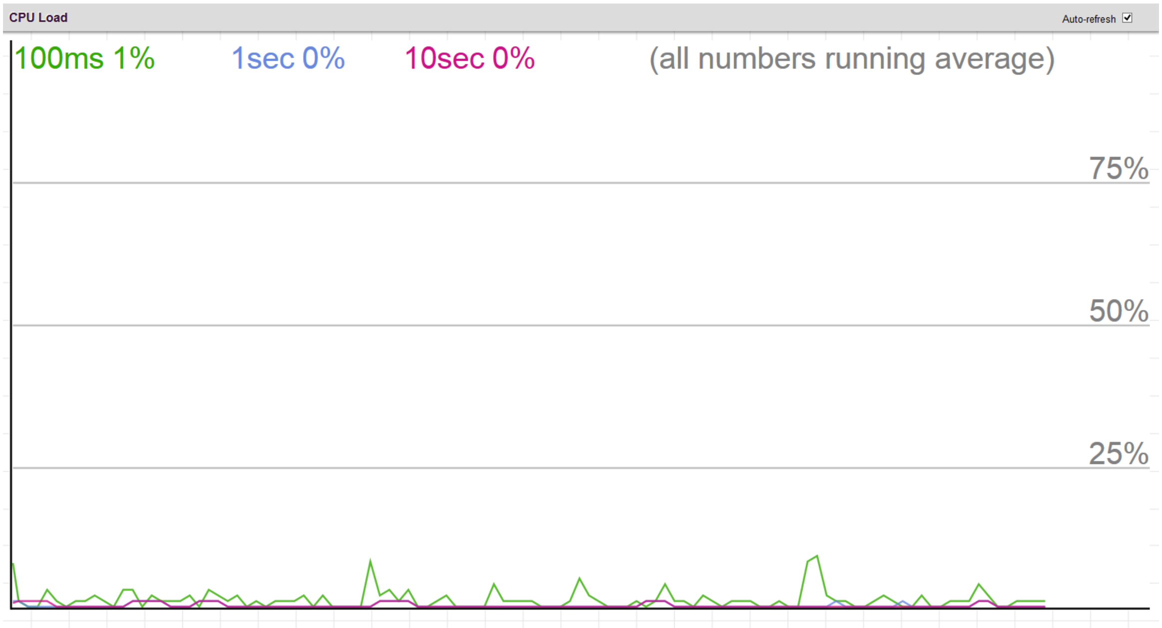
### *4.2.9 System Detailed Log*

Displays individual log records.


View each log, by ID number.

### *4.2.10 System CPU Load*

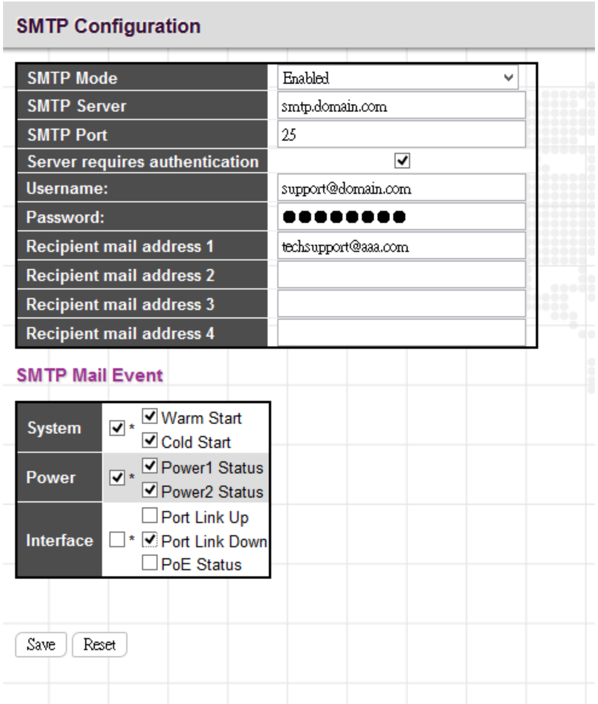
This page displays the CPU load, using an SVG graph.




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.

### *4.2.11 System SMTP*

Configure the email alert system.




***SMTP Configuration***

**SMTP Mode:** Set the SMTP mode operation. Possible modes are:

**Enabled:** Enable SMTP client mode operation.

**Disabled:** Disable SMTP client mode operation.

**SMTP Server:** Set the SMTP server IP address (this is the server that will forward email).

**SMTP Port:** Set the SMTP port number. The default SMTP port is 25.

**Server requires authentication:** Check this box if your server requires authentication. In most cases, this is required and the following must be entered.

**Username:** Enter the valid authentication username for SMTP server

**Password:** Enter the authentication password for username of SMTP server

**Recipient mail address:** Up to four recipient's E-mail addresses may be entered to be sent alert emails.

***SMTP Mail Event***

These check boxes select what events will result in alert email messages being generated and sent.

**System:** Enable/disable the System group's mail events. Possible mail events are:

**Warm Start:** Enable/disable Warm Start mail event.

**Cold Start:** Enable/disable Cold Start mail event.

**Power:** Enable/disable the Power group's mail events. Possible mail events are:

**Power 1 Status:** Enable/disable Power 1 status mail event.

**Power 2 Status:** Enable/disable Power 2 status mail event.

**Interface:** Enable/disable the Interface group's mail events. Possible mail events are:

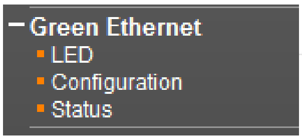
**Port Link Up:** Enable/disable Port Link up mail event.

**Port Link Down:** Enable/disable Port Link down mail event.

**PoE Status:** Enable/disable PoE Status mail event.

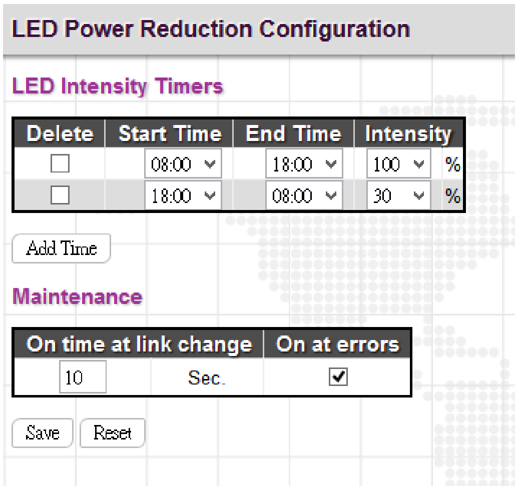
## 4.3 Green Ethernet

The configuration under the "Green Ethernet" menu includes a number of power saving techniques.




### *4.3.1 Green Ethernet LED*

Configure the LED light intensity to reduce power consumption.

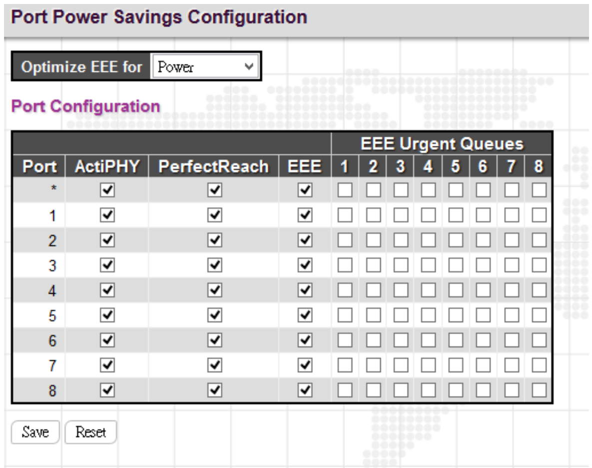



The LED light intensity may be adjusted in a percentage of intensity during programmable time periods. In the above setting example, the LED intensity has been adjusted to 50% during daylight hours and reduced to only 10% intensity during night hours.

The maintenance checkbox will bring LED intensity to 100% for 10 seconds in the event of any error (such as link down).

### 4.3.2 Green Ethernet Configuration

Configure EEE (Energy-Efficient Ethernet) as well as Ethernet power savings.




***<u>Port Power Savings Configuration</u>***

**Optimize EEE for:** Enables/disables the EEE function for this switch. The two options are:

**Power:** The EEE function is enabled. This is the default setting.

**Legacy:** EEE is not enabled.

***<u>Port Configuration</u>***

**ActiPHY™:** ActiPHY™ works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if an Ethernet cable is inserted. For ports with no cable connection, the PHY remains powered down to save energy.

**PerfectReach™:** PerfectReach™ is another power saving mechanism. PerfectReach™ works by determining the cable length and lowering the Ethernet transmit power for ports with short cables.

**EEE (Energy-Efficient Ethernet):** EEE is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE was developed through the IEEE802.3az task force of the Institute of Electrical and Electronic Engineers (IEEE). EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is called wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP (Link Layer Discovery Protocol) protocol. EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode. For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

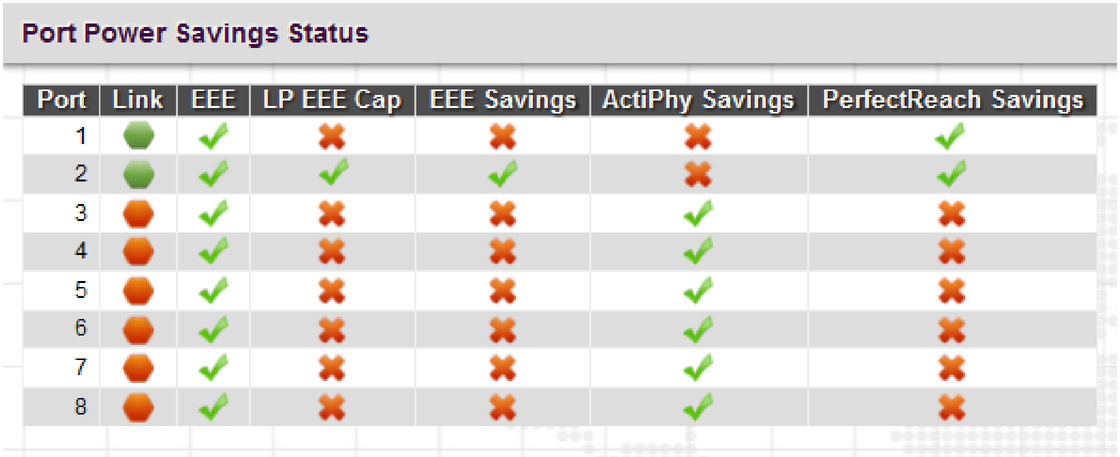
When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic. For traffic that should not be held back, urgent queues may be assigned to reduce latency yet still result in overall power saving.

**EEE Urgent Queues:** It is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

### *4.3.3 Green Ethernet Status*

Display the energy saving status for all ports.

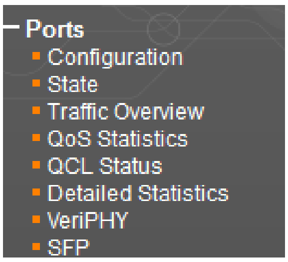

Port Power Savings Status

| Port | Link | EEE | LP EEE Cap | EEE Savings | ActiPhy Savings | PerfectReach Savings |
|---|---|---|---|---|---|---|
| 1 | ● | ✓ | ✗ | ✗ | ✗ | ✓ |
| 2 | ● | ✓ | ✓ | ✓ | ✗ | ✓ |
| 3 | ● | ✓ | ✗ | ✗ | ✓ | ✗ |
| 4 | ● | ✓ | ✗ | ✗ | ✓ | ✗ |
| 5 | ● | ✓ | ✗ | ✗ | ✓ | ✗ |
| 6 | ● | ✓ | ✗ | ✗ | ✓ | ✗ |
| 7 | ● | ✓ | ✗ | ✗ | ✓ | ✗ |
| 8 | ● | ✓ | ✗ | ✗ | ✓ | ✗ |

In the above we can see that port 1 is saving power through PerfectReach™ as the Ethernet cable is short. Our port 2 is connected to an EEE compliant device but with short cable, so we have savings both by EEE and PerfectReach™. Ports 3 through 8 are not linked to any devices, so they are saving power via ActiPHY™. It should be noted that Ethernet savings do not apply to the optical fiber ports, only to the electrical LAN ports.

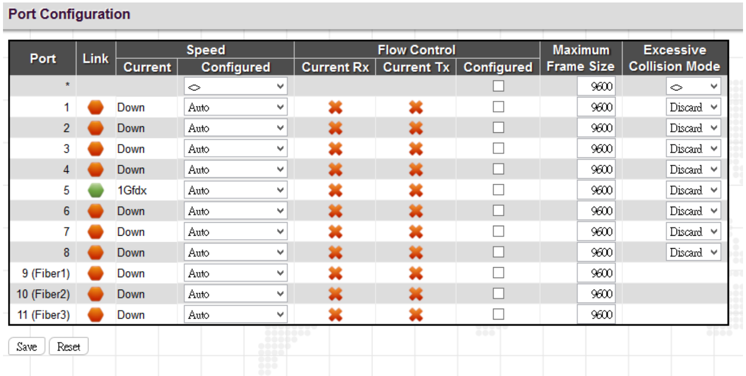
## 4.4 Ports

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



### *4.4.1 Ports Configuration*

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



Port Configuration

| Port | Link | Speed | | Flow Control | | | Maximum Frame Size | Excessive Collision Mode |
|---|---|---|---|---|---|---|---|---|
| | | Current | Configured | Current Rx | Current Tx | Configured | | |
| * | | | <> | | | ☐ | 9600 | <> |
| 1 | | Down | Auto | ✖ | ✖ | ☐ | 9600 | Discard |
| 2 | | Down | Auto | ✖ | ✖ | ☐ | 9600 | Discard |
| 3 | | Down | Auto | ✖ | ✖ | ☐ | 9600 | Discard |
| 4 | | Down | Auto | ✖ | ✖ | ☐ | 9600 | Discard |
| 5 | | 1Gfdx | Auto | ✖ | ✖ | ☐ | 9600 | Discard |
| 6 | | Down | Auto | ✖ | ✖ | ☐ | 9600 | Discard |
| 7 | | Down | Auto | ✖ | ✖ | ☐ | 9600 | Discard |
| 8 | | Down | Auto | ✖ | ✖ | ☐ | 9600 | Discard |
| 9 (Fiber1) | | Down | Auto | ✖ | ✖ | ☐ | 9600 | |
| 10 (Fiber2) | | Down | Auto | ✖ | ✖ | ☐ | 9600 | |
| 11 (Fiber3) | | Down | Auto | ✖ | ✖ | ☐ | 9600 | |

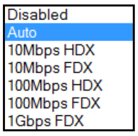
Save Reset

**Port:** This device is a industrial switch with 8 electrical LAN ports numbered 1~8 and 3 fiber optical ports (for SFP modules) numbered 9~11. Each logical port number is displayed in a row. The select all "*" port will apply actions on all ports.

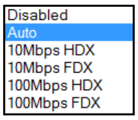
**Link:** The current link state for each port is displayed graphically. Green indicates the link is up and red that it is down.

**Current Speed:** This column provides the current link speed (10, 100, 1G) and duplex (fdx=Full Duplex, hdx=Half Duplex) of each port.

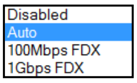
**Configured Speed:** This pull down selects any available link speed for the given switch port. Only speeds supported by the specific port are shown.




Options for **IGS-803SM**




Options for **IFS-803GSM**




Fiber options for **IFS/IGS-803**

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 (IGS-803 Series only).

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).

### 4.4.2 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 100M linked state, while "Amber" colored ports indicate a 1G linked state. "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.

### 4.4.3 Ports Traffic Overview

Displays a comprehensive overview of traffic on all ports.

**Port Statistics Overview** Auto-refresh ☐ Refresh Clear

| 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 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 28346 | 1804 | 3784030 | 1158847 | 0 | 0 | 0 | 0 | 9198 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 (Fiber1) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 (Fiber2) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 (Fiber3) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

The displayed counters are:

**Port:** The logical port (1~11) 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.

### 4.4.4 Ports QoS Statistics

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

**Queuing Counters** Auto-refresh ☐ Refresh Clear

| Port | Q0 | | Q1 | | Q2 | | Q3 | | Q4 | | Q5 | | Q6 | | Q7 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 28529 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1817 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 (Fiber1) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 (Fiber2) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 (Fiber3) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

The displayed counters are:

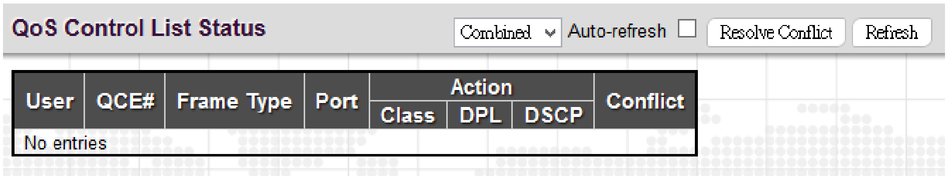
**Port:** The logical port for the settings contained in the same row.

**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.

### 4.4.5 Ports QCL Status

This page shows the QCL status by different QCL users.




Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

**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.

> **Class:** 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.

**Conflict:** Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications, it may happen that resources 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.

### 4.4.6 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.

Detailed Port Statistics for Switch 1 Port 8 — Port 8 — Auto-refresh ☐ — Refresh — Clear

| Receive Total | | Transmit Total | |
|---|---|---|---|
| Rx Packets | 127035408 | Tx Packets | 123449122 |
| Rx Octets | 12852911646 | Tx Octets | 40054887570 |
| Rx Unicast | 123460100 | Tx Unicast | 123449108 |
| Rx Multicast | 2240374 | Tx Multicast | 11 |
| Rx Broadcast | 1334934 | Tx Broadcast | 3 |
| Rx Pause | 0 | Tx Pause | 0 |
| Rx Bits Rate | 78370 | Tx Bits Rate | 268640 |
| Rx Utilization | 0.0 | Tx Utilization | 0.0 |
| **Receive Size Counters** | | **Transmit Size Counters** | |
| Rx 64 Bytes | 1388398 | Tx 64 Bytes | 74930 |
| Rx 65-127 Bytes | 123423703 | Tx 65-127 Bytes | 189320 |
| Rx 128-255 Bytes | 21177 | Tx 128-255 Bytes | 1040 |
| Rx 256-511 Bytes | 2200947 | Tx 256-511 Bytes | 123182530 |
| Rx 512-1023 Bytes | 1136 | Tx 512-1023 Bytes | 199 |
| Rx 1024-1526 Bytes | 47 | Tx 1024-1526 Bytes | 1103 |
| Rx 1527- Bytes | 0 | Tx 1527- Bytes | 0 |
| **Receive Queue Counters** | | **Transmit Queue Counters** | |
| Rx Q0 | 127035408 | 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 | 123449122 |
| **Receive Error Counters** | | **Transmit Error Counters** | |
| Rx Drops | 18962 | 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 | 2236654 | | |

<u>**Receive Total and Transmit Total**</u>

**Rx and Tx Packets:** The number of received and transmitted (good and bad) packets.

**Rx and Tx Octets:** The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

**Rx and Tx Unicast:** The number of received and transmitted (good and bad) unicast packets.

**Rx and Tx Multicast:** The number of received and transmitted (good and bad) multicast packets.

**Rx and Tx Broadcast:** The number of received and transmitted (good and bad) broadcast packets.

**Rx and Tx Pause:** A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE.

**Receive and Transmit Size Counters:** 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:** Displays the number of received and transmitted packets per input and output queue.

<u>***Receive Error Counters***</u>

**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.

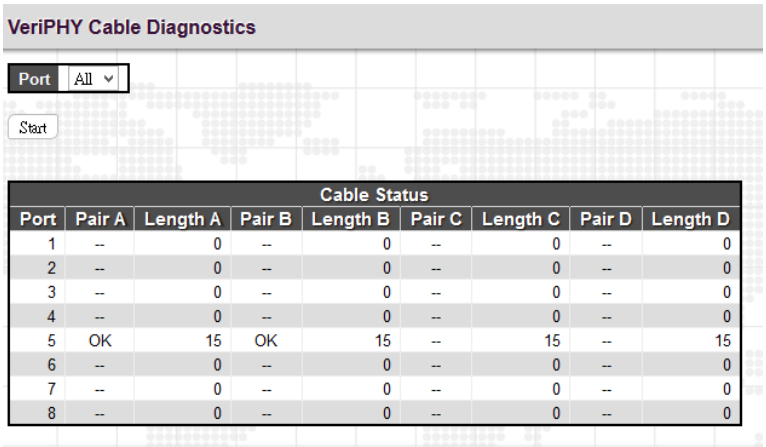
***Transmit Error Counters***

**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.

### *4.4.7 Ports VeriPHY™*

This page is used for running the VeriPHY™ Cable Diagnostics for 10/100 and 1G copper ports. Select which ports to run, or all. Click "Start".


VeriPHY Cable Diagnostics

Port All

Start

| Cable Status | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Port | Pair A | Length A | Pair B | Length B | Pair C | Length C | Pair D | Length D |
| 1 | -- | 0 | -- | 0 | -- | 0 | -- | 0 |
| 2 | -- | 0 | -- | 0 | -- | 0 | -- | 0 |
| 3 | -- | 0 | -- | 0 | -- | 0 | -- | 0 |
| 4 | -- | 0 | -- | 0 | -- | 0 | -- | 0 |
| 5 | OK | 15 | OK | 15 | -- | 15 | -- | 15 |
| 6 | -- | 0 | -- | 0 | -- | 0 | -- | 0 |
| 7 | -- | 0 | -- | 0 | -- | 0 | -- | 0 |
| 8 | -- | 0 | -- | 0 | -- | 0 | -- | 0 |

This will take approximately 5 seconds per port. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

**Port:** Port number.

**Pair:** The status of the cable pair.

**OK:** Correctly terminated pair

**Open:** Open pair

**Short:** Shorted pair

**Short A:** Cross-pair short to pair A

**Short B:** Cross-pair short to pair B

**Short C:** Cross-pair short to pair C

**Short D:** Cross-pair short to pair D

**Cross A:** Abnormal cross-pair coupling with pair A

**Cross B:** Abnormal cross-pair coupling with pair B

**Cross C:** Abnormal cross-pair coupling with pair C

**Cross D:** Abnormal cross-pair coupling with pair D

**Length:** The length (in meters) of the cable pair. The resolution is ±3 meters.

***NOTE:*** *VeriPHY is only applicable to the electrical ports. It is not applicable to the optical ports.*

### 4.4.8 Ports SFP

This page displays current SFP status for all three fiber ports.

**SFP and D/D Information**

| 9 (Fiber 1) | |
|---|---|
| Vendor Name | CTC UNION |
| Vendor Part Number | SFS-7020-WA-DD A |
| Fiber Type | Single |
| Wave Length | 1310 nm |
| Wave Length 2 | 1550 nm |
| Link Length | 20 km |
| TX Power | -6 dBm |
| RX Power | -40 dBm |
| RX Sensitivity | -32 dBm |
| Temperature | 38°C |

| 10 (Fiber 2) | |
|---|---|
| Vendor Name | CTC UNION |
| Vendor Part Number | SFS-7020-WB-DD A |
| Fiber Type | Single |
| Wave Length | 1550 nm |
| Wave Length 2 | 1310 nm |
| Link Length | 20 km |
| TX Power | -5 dBm |
| RX Power | -34 dBm |
| RX Sensitivity | -32 dBm |
| Temperature | 32°C |

| 11 (Fiber 3) |
|---|
| None |

**Vendor Name:** SFP vendor (manufacturer's) name.

**Vendor Part:** Manufacture's part number, provided by SFP vendor.

**Fiber Type:** Fiber type of either single or multi mode.

**Wave Length:** Laser wavelength Tx.

**Wave Length 2:** Laser wavelength Rx. (not all SFP support this reading)

**Link Length:** Link Length. (This is a marketing specification for this SFP module, not an actual measurement.)

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

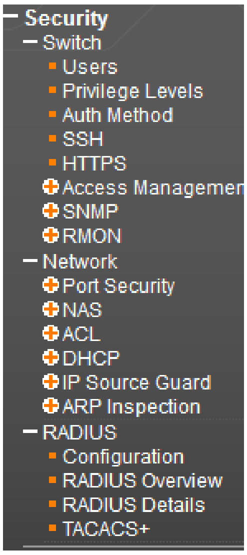
**RX Power:** The receive optical power is reported by SFP that support DDI.

**RX Sensitivity:** The Receive Sensitivity is reported by SFP that support DDI.

**Temperature:** The internal temperature is reported by SFP that support DDI.

## 4.5 Security

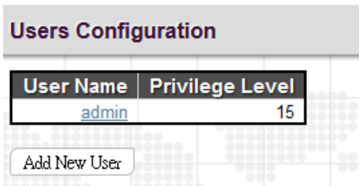
Under the security heading are three major icons, switch, network and RADIUS.




### *4.5.1 Switch*

#### *4.5.1.1 Users*

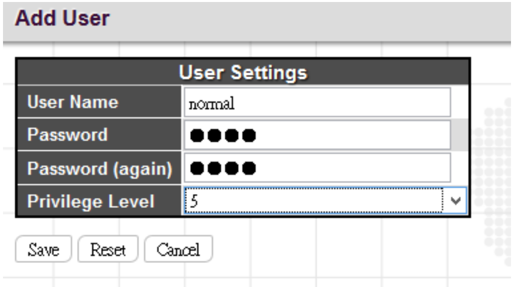
This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.




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.

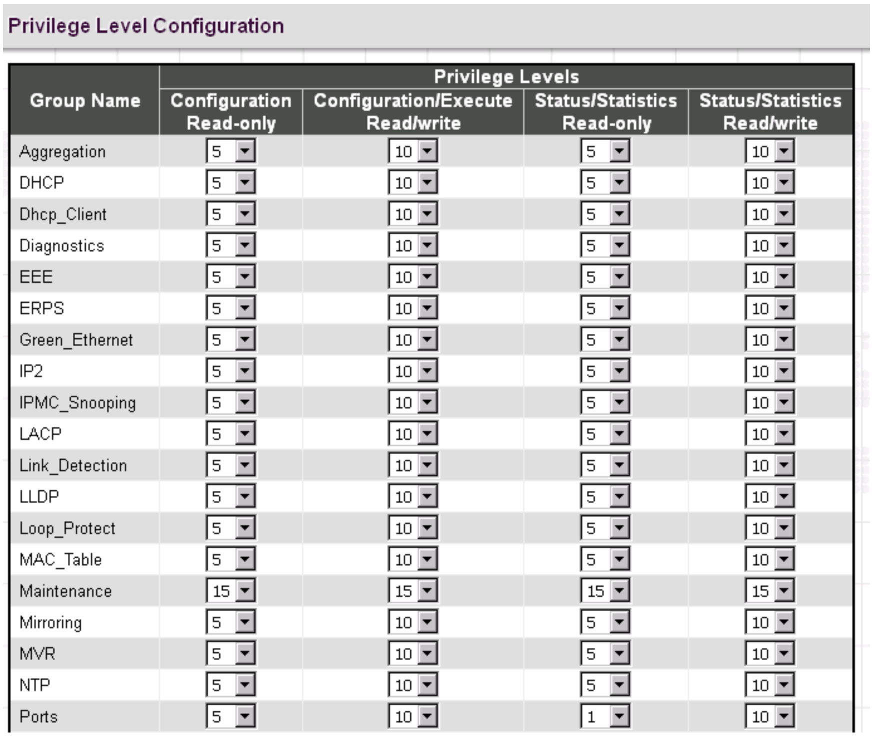
**Password:** Enter the password for this user account.

**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.

### *4.5.1.2 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 |
| DHCP | 5 | 10 | 5 | 10 |
| Dhcp_Client | 5 | 10 | 5 | 10 |
| Diagnostics | 5 | 10 | 5 | 10 |
| EEE | 5 | 10 | 5 | 10 |
| ERPS | 5 | 10 | 5 | 10 |
| Green_Ethernet | 5 | 10 | 5 | 10 |
| IP2 | 5 | 10 | 5 | 10 |
| IPMC_Snooping | 5 | 10 | 5 | 10 |
| LACP | 5 | 10 | 5 | 10 |
| Link_Detection | 5 | 10 | 5 | 10 |
| LLDP | 5 | 10 | 5 | 10 |
| Loop_Protect | 5 | 10 | 5 | 10 |
| MAC_Table | 5 | 10 | 5 | 10 |
| Maintenance | 15 | 15 | 15 | 15 |
| Mirroring | 5 | 10 | 5 | 10 |
| MVR | 5 | 10 | 5 | 10 |
| NTP | 5 | 10 | 5 | 10 |
| Ports | 5 | 10 | 1 | 10 |

**Group Name:** This name identifies the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:

**System:** Contact, Name, Location, Timezone, Daylight Saving Time, Log.

**Security:** Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.

**IP:** Everything except 'ping'.

**Port:** Everything except 'VeriPHY'.

**Diagnostics:** 'ping' and 'VeriPHY'.

**Maintenance:** CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

**Privilege Levels:** Every group has an authorization Privilege level for the following sub groups:

configuration read-only

configuration/execute read-write

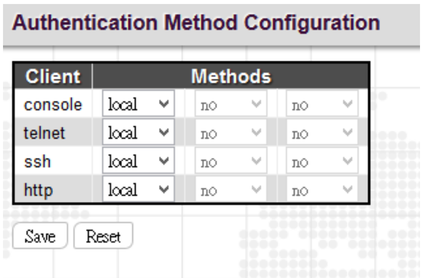
status/statistics read-only

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.

#### *4.5.1.3 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.




**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.

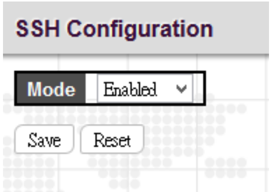
**radius:** Use remote RADIUS server(s) for authentication.

**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.*

### *4.5.1.4 SSH*

Configure SSH on this page.




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

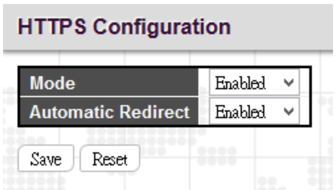
**Enabled:** Enable SSH mode operation. By default, SSH mode operation is enabled.

**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.*

### *4.5.1.5 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:

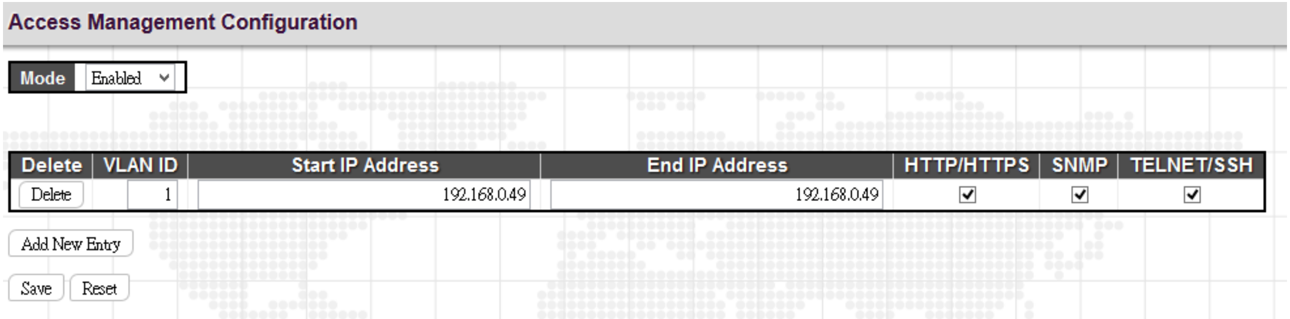
**Enabled:** Enable HTTPS redirect mode operation.

**Disabled:** Disable HTTPS redirect mode operation.

## *4.5.2 Access Management*

### *4.5.2.1 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.




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

**Enabled:** Enable access management mode operation.

**Disabled:** Disable access management mode operation.

**VLAN ID:** Indicates the VLAN ID for the access management entry.

**Start IP address:** Indicates the start IP address for the access management entry.

**End IP address:** Indicates the end IP address for the access management entry.

**HTTP/HTTPS:** 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 insert a new entry to the list.

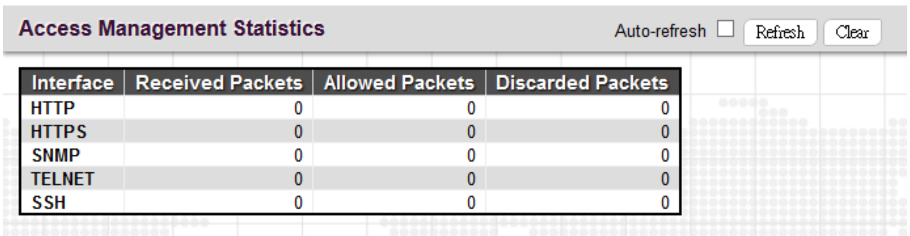
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

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

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

### *4.5.2.2 Access Management Statistics*

This page provides statistics for access management.




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

**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.

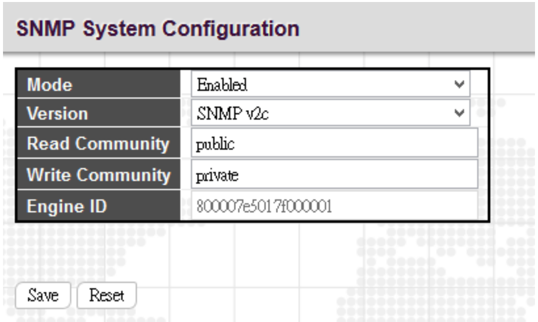
**Allowed Packets:** The number of allowed packets from the interface when access management mode is enabled.

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

## 4.5.3 SNMP

### 4.5.3.1 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.

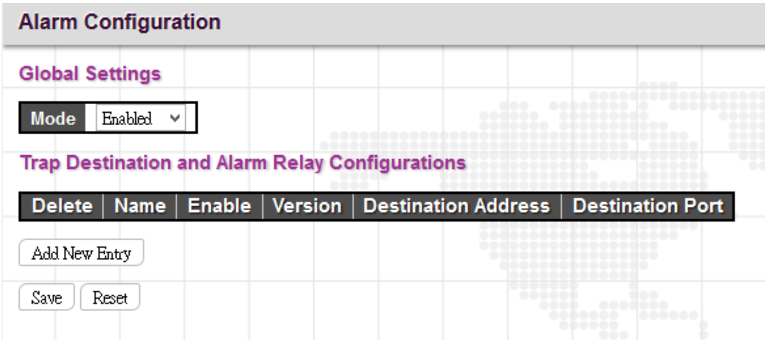
**Read Community:** Indicates the community read access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E.

**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.

### *4.5.3.2 Alarm Configuration*

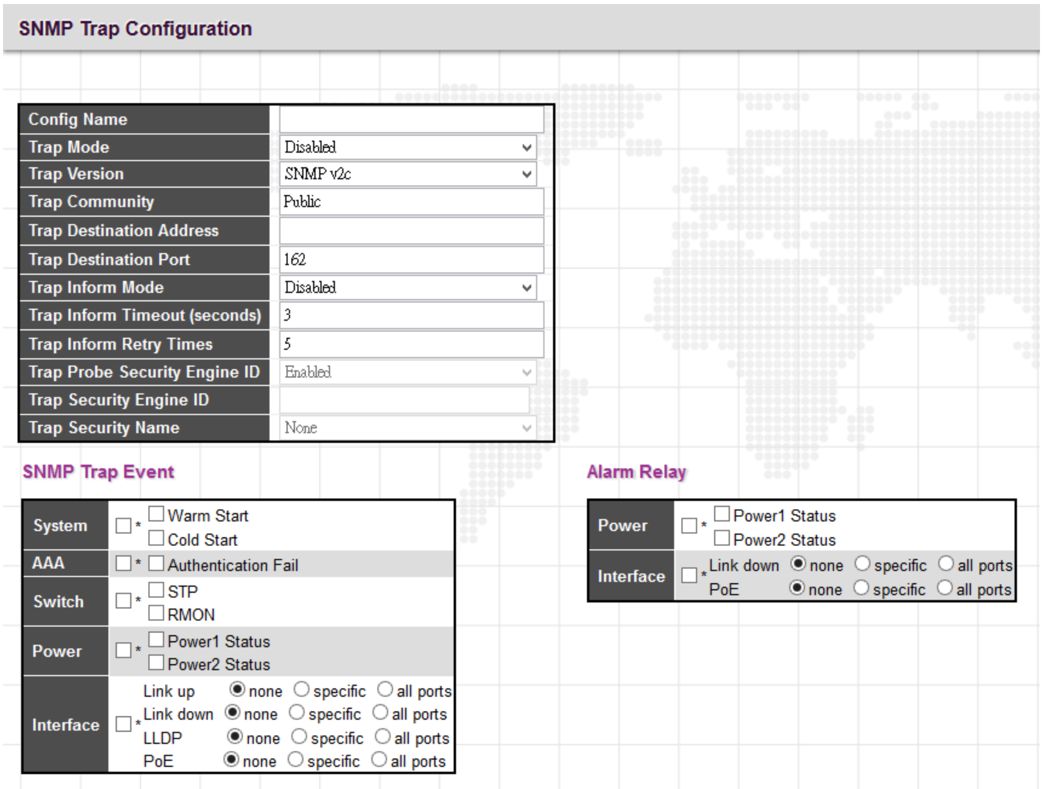
Configure SNMP trap on this page.




***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).

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

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

**STP:** Select the checkbox to enable STP trap. Clear to disable STP trap.

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

**Power:** Indicates the Power group's traps. Possible trap event are:

**Power 1 Status:** Select the checkbox to enable Power 1 status trap. Clear the checkbox to disable Power 1 status trap.

**Power 2 Status:** Select the checkbox to enable Power 2 status trap. Clear the checkbox to disable Power 2 status trap.

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

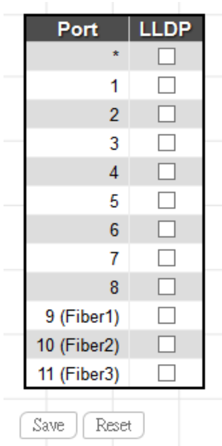
**Link Up:** none/specific/all ports Link up trap.

**Link Down:** none/specific/all ports Link down trap.

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

**PoE:** none/specific/all ports PoE status trap. This option is for PoE models only.

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




After completing all the trap settings, click the "Save" button.

***Alarm Relay***

**Power:** Indicates the Power group's alarm relay. Possible options are:

**Power 1 Status:** Select the checkbox to enable Power 1 status alarm relay function. Once power 1 fails, the alarm relay contacts are open and Fault LED indicator is on in amber. Clear the checkbox to disable Power 1 status alarm relay.

**Power 2 Status:** Select the checkbox to enable Power 2 status alarm relay function. Once power 2 fails, the alarm relay contacts are open and Fault LED indicator is on in amber. Clear the checkbox to disable Power 2 status alarm relay.

**Interface:** Indicates the Interface group's alarm relay. Possible options are:

**Link Down:** none/specific/all ports Link down alarm relay. Once link down occurs on the selected interfaces, the alarm relay contacts are open, Fault LED indicator is on in amber.  Clear the checkbox to disable alarm relay function.

**PoE:** none/specific/all ports PoE status alarm relay. This option is for PoE models only. Once PoE function fails on the selected interfaces, the alarm relay contacts are open, Fault LED indicator is on in amber. Clear the checkbox to disable alarm relay function.

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

| Port | Link down | PoE |
|---|---|---|
| * | ☐ | ☐ |
| 1 | ☑ | ☐ |
| 2 | ☑ | ☐ |
| 3 | ☑ | ☐ |
| 4 | ☑ | ☑ |
| 5 | ☑ | ☑ |
| 6 | ☑ | ☑ |
| 7 | ☑ | ☐ |
| 8 | ☑ | ☐ |
| 9 (Fiber1) | ☑ | |
| 10 (Fiber2) | ☑ | |
| 11 (Fiber3) | ☑ | |

***NOTE:** For more information about alarm relay circuit on the terminal block, please see [Power & Alarm]() section.*

### *4.5.3.3 SNMPv3 Community Configuration*

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

**SNMPv3 Community Configuration**

| Delete | Community | Source IP | Source Mask |
|---|---|---|---|
| ☐ | public | 0.0.0.0 | 0.0.0.0 |
| ☐ | private | 0.0.0.0 | 0.0.0.0 |

Add New Entry | Save | Reset

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

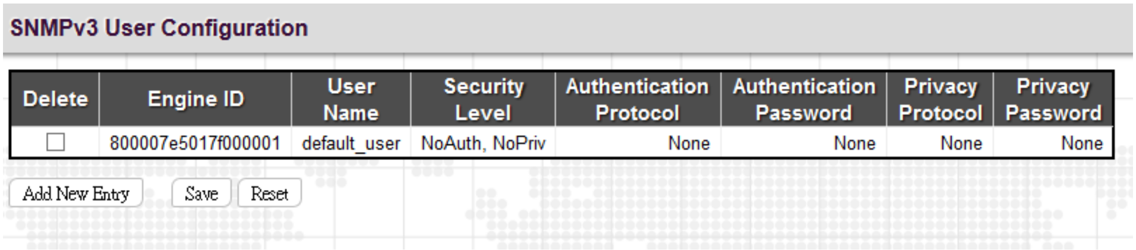
**Community:**  Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string. This string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

### 4.5.3.4 SNMPv3 User Configuration

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




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

**Engine ID:** An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it is a remote user.

**User Name:** A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 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.

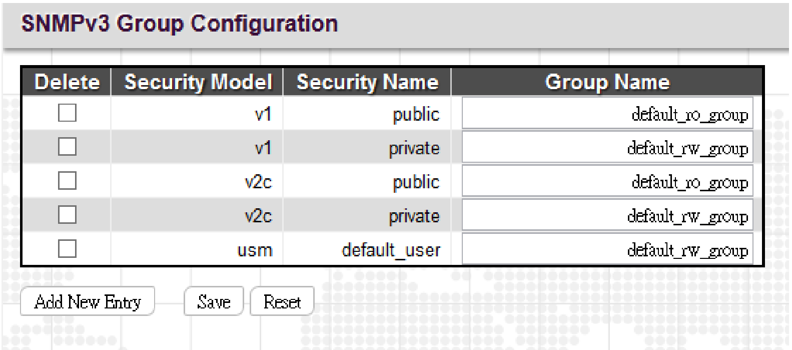
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

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

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

### 4.5.3.5 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.

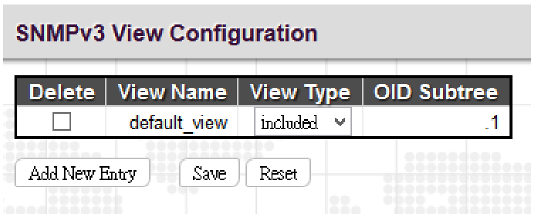
**usm:** User-based Security Model (USM) for SNMPv3.

**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.

### 4.5.3.6 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:

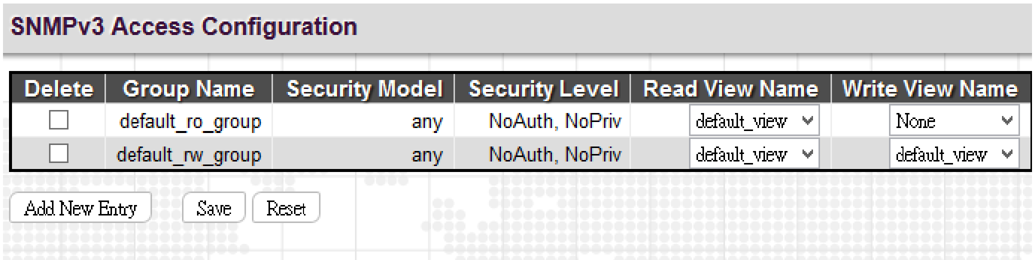
**included:** An optional flag to indicate that this view subtree should be included.

**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(*).

### *4.5.3.7 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.

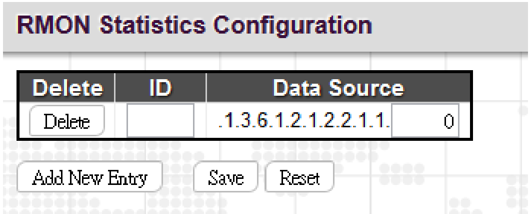
**Read View Name:** The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

**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.

## 4.5.4 RMON

### 4.5.4.1 RMON Statistics Configuration

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



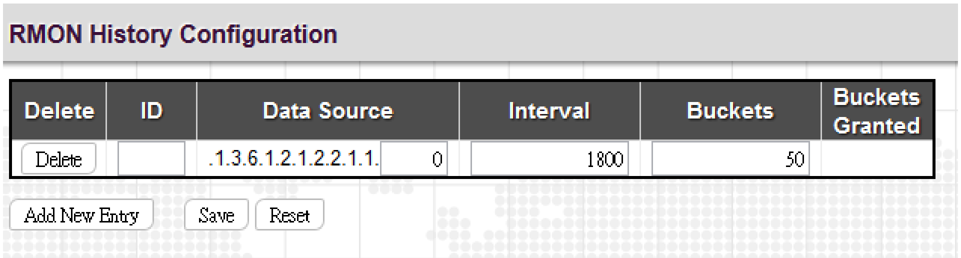

**Delete:** Check to delete the entry. It will be deleted during the next save.

**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.

### 4.5.4.2 RMON 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 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.

**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.

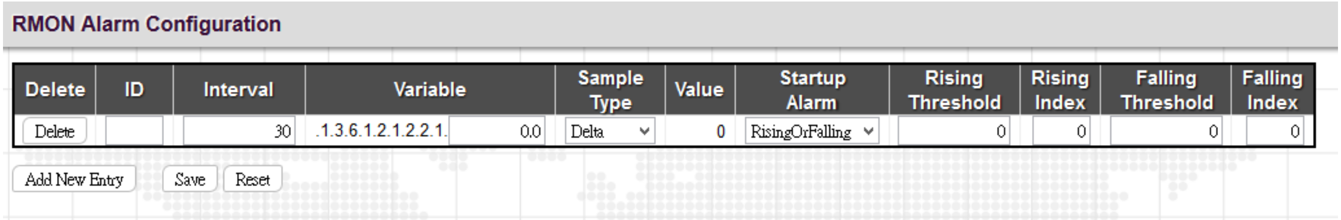
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

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

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

### 4.5.4.3 RMON 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.

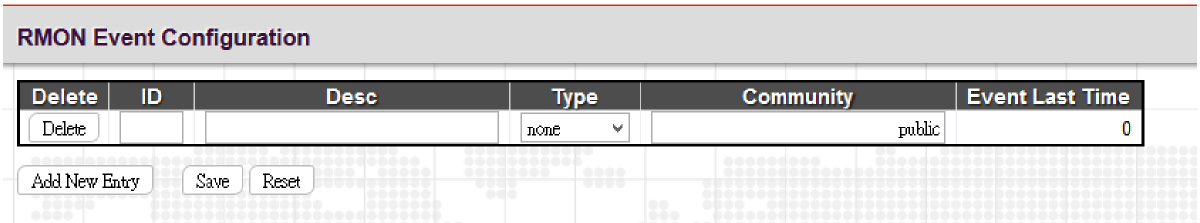
Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

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

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

### 4.5.4.4 RMON Event Configuration

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




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

**ID:** Specify an ID index. The range is 1~65535.

**Desc:** Enter 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.

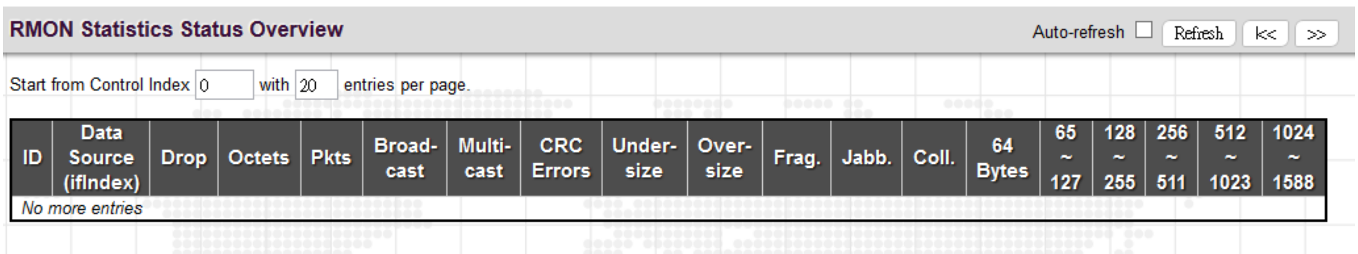
**logandtrap:** Logs an event and sends a trap message.

**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.

### 4.5.4.5 RMON Statistics Overview

This RMON statistics overview page shows interface statistics. All values displayed have been accumulated since the last system reboot and are shown as counts per second. The system will automatically refresh every 60 seconds by default.



**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.

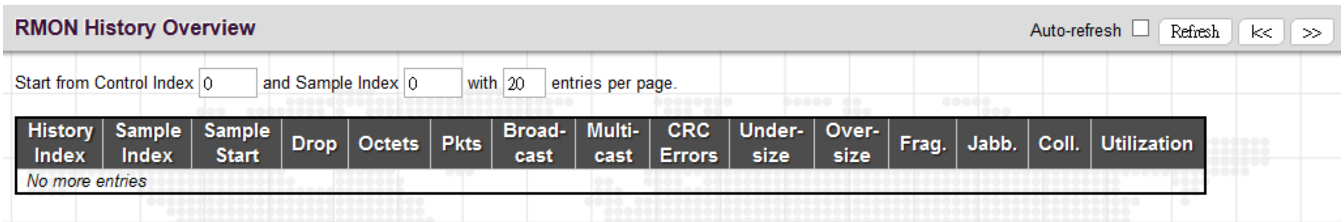
**Jabb.:** The number of frames which size is larger than 64 octets received with invalid CRC.

**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.

### *4.5.4.6 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.

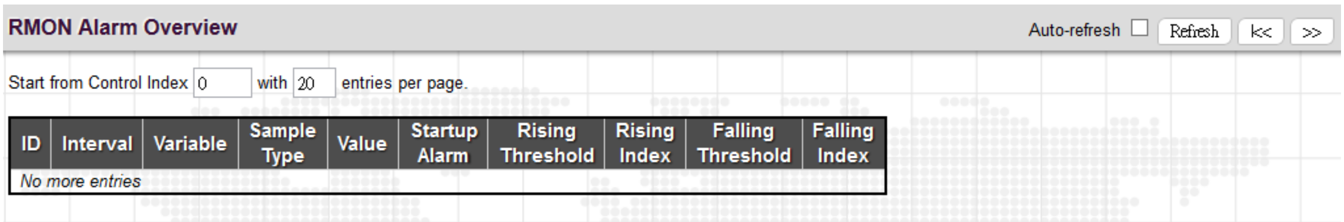
**Frag.:** The number of frames which size is less than 64 octets received with invalid CRC.

**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.

### *4.5.4.7 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.

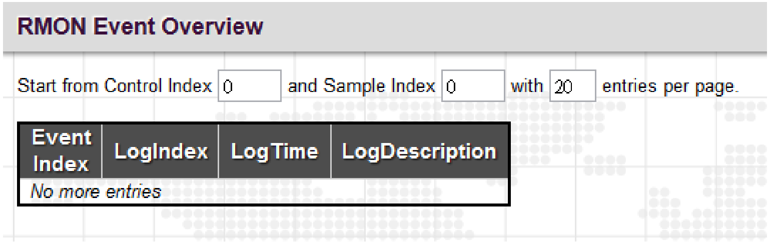
**Rising Threshold:** If the current value is greater than the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated.

**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.

### 4.5.4.8 Event Overview




**Event Index:** Display the event entry index.

**Log Index**: Display the log entry index.

**Log Time**: Display Event log time.

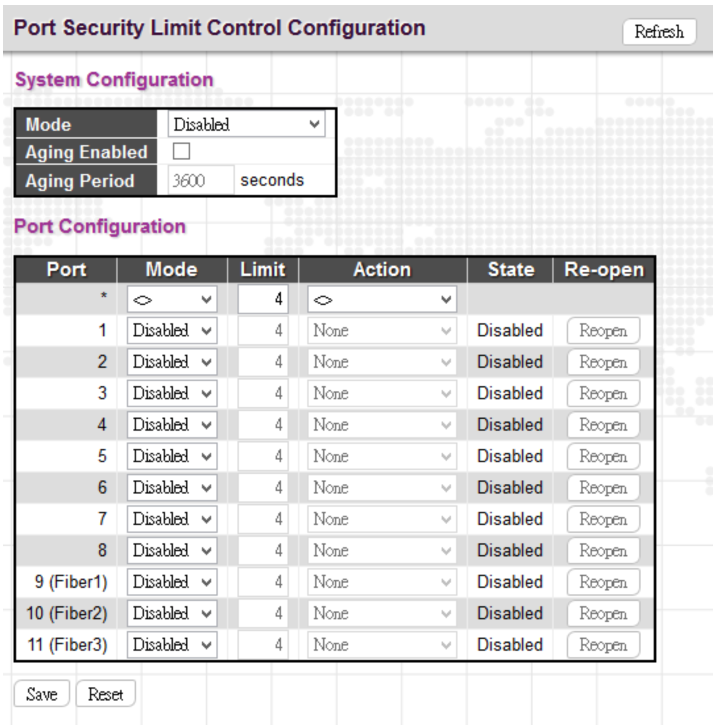
**Log Description:** Display Event description.

## 4.5.5 Network

### 4.5.5.1 Port Security

Port Security Limit Control can restrict the number of users that can access the switch based on users' MAC address and VLAN ID on a per port basis. Once the number of users that wants to access the switch exceeds the specified number, a selected action will be taken immediately.

#### 4.5.5.1.1 Limit Control



***System Configuration***

**Mode:** Enable or disable port security limit control globally. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

**Aging Enabled:** If enabled, secured MAC addresses are subject to aging as discussed under Aging Period. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

**Aging Period:** If Aging Enabled is checked, then the aging period can be set up with the desired value. By default, the aging period is set to 3600 seconds. The allowed range is 10~10,000,000 second.

***Port Configuration***

**Port:** Display the port number. “Port *” rules apply to all ports.

**Mode:** Enable or disable port security limit control on a per port basis. To make limit control function work, port security limit control needs to be enabled globally and on a port.

**Limit:** The maximum number of MAC addresses that can be secured on this port. The number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

**Action:** If the limit is exceeded, the selected action will take effect.

**None:** Do not allow more than the specified limit of MAC addresses to access on a port. No action is further taken.

**Trap:** If Limit + 1 MAC addresses are seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit is exceeded.

**Shutdown:** If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new addresses will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:
* Boot the switch
* Disable and re-enable Limit Control on the port or the switch
* Click the “Reopen” button

**Trap & Shutdown:** If Limit + 1 MAC addresses is seen on the port, both the “Trap” and the “Shutdown” actions described above will be taken.

**State:** Display the current state of the port from the port security limit control's point of view. The displayed state might be one of the following:

**Disabled:** Limit control is either globally disabled or disabled on a port.

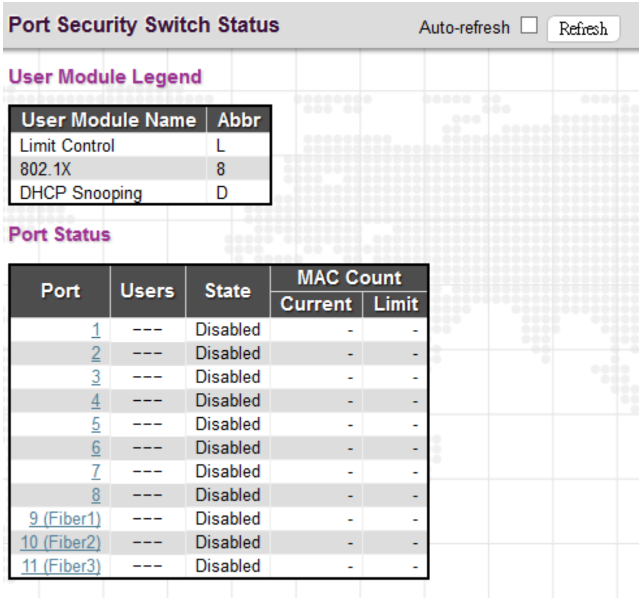
**Ready:** The limit is not reached yet.

**Limit Reached:** The limit is reached on a port. This state can only be shown if Action is set to None or Trap.

**Shutdown:** The port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

**Re-open Button:** If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section. Note that clicking the Reopen button causes the page to be refreshed, so non-committed changes will be lost.

#### 4.5.5.1.2 Switch Status


Port Security Switch Status Auto-refresh Refresh

User Module Legend

| User Module Name | Abbr |
|---|---|
| Limit Control | L |
| 802.1X | 8 |
| DHCP Snooping | D |

Port Status

| Port | Users | State | MAC Count | |
|---|---|---|---|---|
| | | | Current | Limit |
| 1 | --- | Disabled | - | - |
| 2 | --- | Disabled | - | - |
| 3 | --- | Disabled | - | - |
| 4 | --- | Disabled | - | - |
| 5 | --- | Disabled | - | - |
| 6 | --- | Disabled | - | - |
| 7 | --- | Disabled | - | - |
| 8 | --- | Disabled | - | - |
| 9 (Fiber1) | --- | Disabled | - | - |
| 10 (Fiber2) | --- | Disabled | - | - |
| 11 (Fiber3) | --- | Disabled | - | - |

***User Module Legend***

**User Module Name:** The full name of a module that may request Port Security services.

**Abbr**: This column is the abbreviation for the user module used in the “Users” column in the “Port Status”.

***Port Status***

**Port:** Port number. Click a particular port number to see its port status.

**Users:** Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter has enabled port security.

**State:** This shows the current status of a port. It can be one of the following states:

**Disabled:** No user modules are currently using the Port Security service.

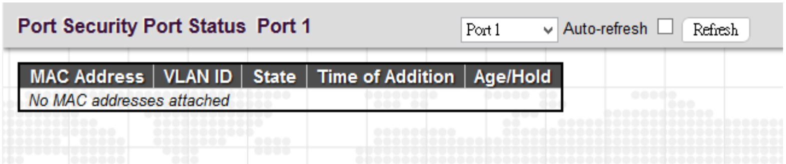
**Ready:** The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

**Limit Reached:** The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

**Shutdown:** The Port Security service is enabled by at least the Limit Control user module and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration page.

**MAC Count (Current/Limit):** The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

#### *4.5.5.1.3 Port Status*




This page shows MAC addresses learned on a particular port.

**MAC Address:** When "Port Security Limit Control" is enabled globally and on a port, MAC addresses learned on a port show in here.

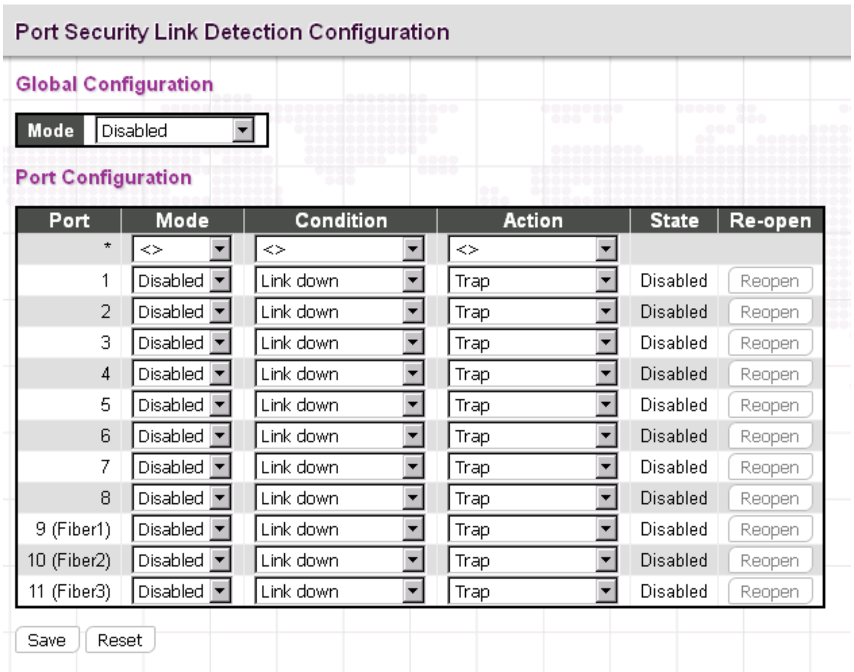
**VLAN ID:** Display VLAN ID that is seen on this port.

**State:** Display whether the corresponding MAC address is forwarding or blocked. In the blocked state, it will not be allowed to transmit or receive traffic.

**Time of Addition:** Display the date and time when this MAC address was seen on the port.

**Age/Hold:** If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address is still forwarding traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

#### *4.5.5.1.4 Link Detection*



***Global Configuration***

**Mode:** Enable or disable link detection function globally.

***Port Configuration***

**Mode:** Enable or disable link detection function on a per port basis.

**Condition:** Select a link condition that applies to the selected action.

**Link down:** If the link is changed from up to down, the device will trigger the selected action.

**Link up:** If the link is changed from down to up, the device will trigger the selected action.

**Link down and up:** If the link is changed from up to down and then up again, the device will trigger the selected action.

**Action:** When the selected link condition occurs on the corresponding port, the action selected will be triggered.

**Trap:** If the selected link condition occurs on a port, a SNMP trap will be sent.

**Shutdown:** If the selected link condition occurs on a port, the corresponding port will be shutdown. When the port is shutdown, there are four ways to open or activate the shutdown port.

(1) Reboot the switch.
(2) Disable and re-enable on the shutdown port.
(3) Select other link conditions or action modes.
(4) Click the "Reopen" button on the shutdown port to open the port.

**Trap + Shutdown:** If the selected link condition occurs on a port, a SNMP trap will be sent and the corresponding port will be shutdown. When the port is shutdown, there are four ways to open the port.

(1) Reboot the switch.
(2) Disable and re-enable on the shutdown port.
(3) Select other link conditions or action modes.
(4) Click the "Reopen" button on the shutdown port to open the port.

**State:** This field displays the current state of the corresponding port. It may display one of the following states:

**Disabled:** The link detection function is globally disabled or the corresponding port mode is disabled.

**Ready:** The link detection function is globally enabled and the corresponding port is enabled as well. However, the action is not yet triggered.

**Trap Event:** The link detection "Trap" action is triggered.

**Shutdown:** The link detection "Shutdown" or "Trap & Shutdown" action is triggered.

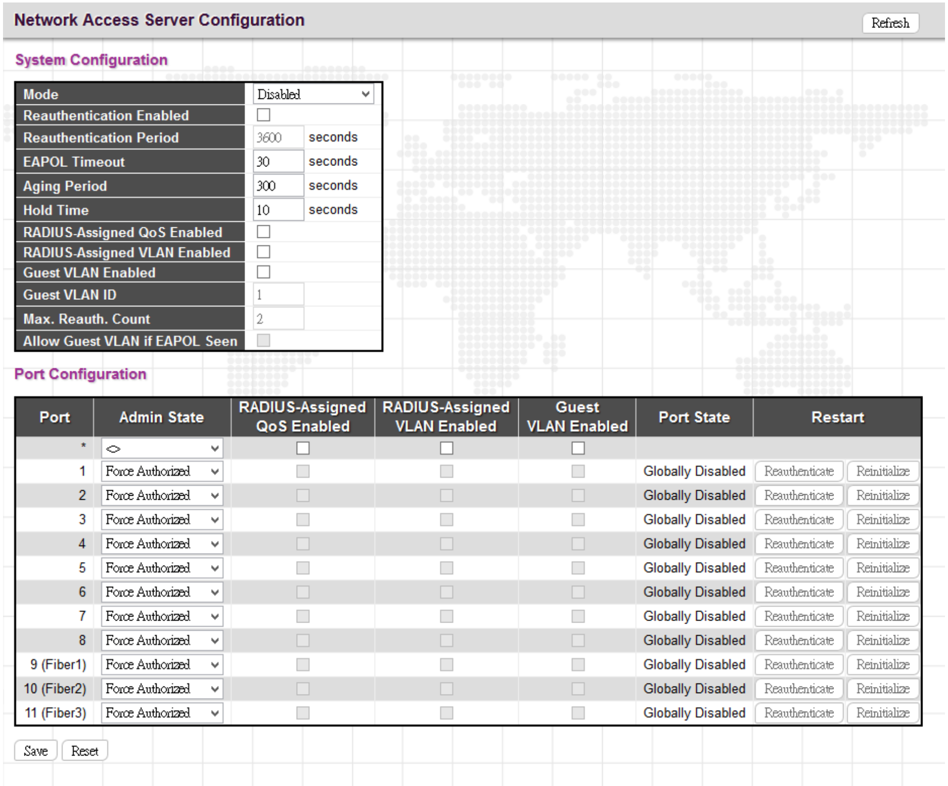
**Reopen:** Click on the re-open button to open or activate the shutdown port. This button works only when the port is in "Shutdown" state.

### *4.5.5.2 NAS*

Network Access Server configuration is useful to the networking environment that wants to authenticate clients (supplicants) before they can access resources on the protected network. To effectively control access to unknown clients, 802.1X defined by IEEE provides a port-based authentication procedure that can prevent unauthorized access to a network by requiring users to first submit credentials for authentication purposes.

A switch interconnecting clients and radius server usually acts as an authenticator and uses EAPOL (Extensible Authentication Protocol over LANs) to exchange authentication protocol messages with clients and a remote RADIUS authentication server to verify user identity and user's access right. This section is for setting up authenticator's configurations either on the system or on a per port basis. To configure backend server, please go to RADIUS configuration page.

#### *4.5.5.2.1 Configuration*




***System Configuration***

**Mode:** Enable 802.1X and MAC-based authentication globally on the switch. If globally disabled, all ports are allowed to forward frames.

**Reauthentication Enabled:** Select the checkbox to set clients to be re-authenticated after an interval set in "Reauthentication Period" field. Re-autentication can be used to detect if a new device is attached to a switch port.

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

**EAPOL Timeout:** Specify the time that the switch waits for a supplicant response during an authentication session before transmitting a Request Identify EAPOL packet. By default, it is set to 30 seconds. The allowed range is 1~65535 seconds.

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

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

**Radius-Assigned QoS Enabled:** Select the checkbox to globally enable RADIUS assigned QoS.

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

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

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

**Guest VLAN ID:** This VLAN ID is functional only when Guest VLAN is enabled. This is the value that a port’s Port VLAN ID is set to if a port is moved into the Guest VLAN. The range is 1~4095.

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

**Allow Guest VLAN if EAPOL Seen:** The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.

***Port Configuration***

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

**Admin State:** Select the authentication mode on a port. This setting works only when NAS is globally enabled. The following modes are available:

> **Force Authorized:** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
>
> **Force Unauthorized:** In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
>
> **Port-Based 802.1X:** This mode requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
>
> **Single 802.1X:** In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one

supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the “Port Security” module is used to secure a supplicant's MAC address once successfully authenticated.

**Multi 802.1X:** In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the “Port Security” module.

**MAC-based Auth.:** Unlike port-based 802.1X, MAC-based authentication do not transmit or receive EAPOL frames. In MAC-based authentication, the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

**RADIUS-Assigned QoS Enabled:** Select the checkbox to enable RADIUS-Assigned QoS on a port.

**Radius-Assigned VLAN Enabled:** Select the checkbox to enable RADIUS-Assigned VLAN on a port.

**Guest VLAN Enabled:** Select the checkbox to enable Guest VLAN on a port.

**Port State:** Display the current state of the port from 802.1X authentication point of view. The possible states are as follows:

**Globally Disabled:** 802.1X and MAC-based authentication are globally disabled.

**Link Down:** 802.1X and MAC-based authentication are enabled but there is no link on a port.

**Authorized:** The port is forced in authorized mode and the supplicant is successfully authorized.

**Unauthorized:** The port is forced in unauthorized mode and the supplicant is not successfully authorized by the RADIUS server.

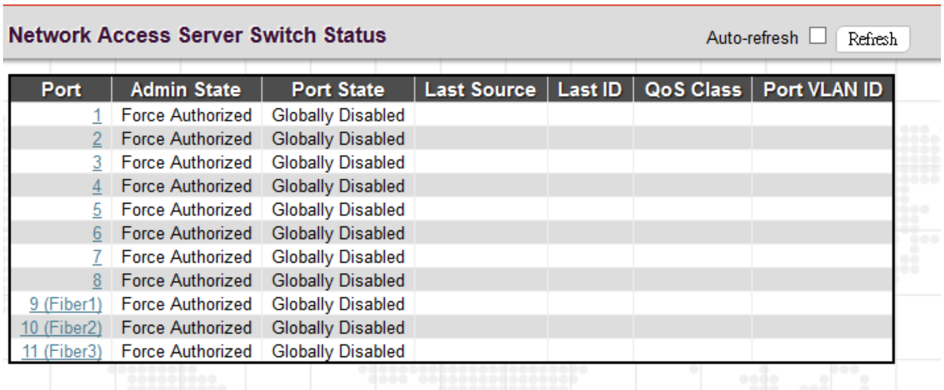
**X Auth/Y Unauth:** The port is in a multi-supplicant mode. X clients are authorized and Y are unauthorized.

**Restart:** Restart client authentication using one of the methods described below. Note that the restart buttons are only enabled when the switch’s authentication mode is globally enabled (under System Configuration) and the port's Admin State is an EAPOL-based or MACBased mode. Clicking these buttons will not cause settings changed on the page to take effect.

**Reauthenticate:** Schedules reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

**Reinitialize**: This forces the reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

#### *4.5.5.2.2 Switch Status*



Network Access Server Switch Status    Auto-refresh ☐ Refresh

| Port | Admin State | Port State | Last Source | Last ID | QoS Class | Port VLAN ID |
|---|---|---|---|---|---|---|
| 1 | Force Authorized | Globally Disabled | | | | |
| 2 | Force Authorized | Globally Disabled | | | | |
| 3 | Force Authorized | Globally Disabled | | | | |
| 4 | Force Authorized | Globally Disabled | | | | |
| 5 | Force Authorized | Globally Disabled | | | | |
| 6 | Force Authorized | Globally Disabled | | | | |
| 7 | Force Authorized | Globally Disabled | | | | |
| 8 | Force Authorized | Globally Disabled | | | | |
| 9 (Fiber1) | Force Authorized | Globally Disabled | | | | |
| 10 (Fiber2) | Force Authorized | Globally Disabled | | | | |
| 11 (Fiber3) | Force Authorized | Globally Disabled | | | | |

**Port:** The port number. Click a port to view the detailed NAS statistics.

**Admin State:** Display the port’s current administrative state.

**Port Status:** Display the port state.

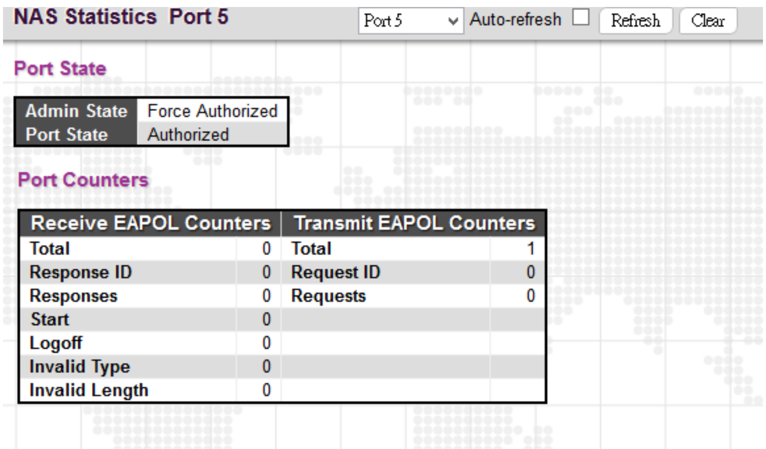
**Last Source:** The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication.

**Last ID:** The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication.

**QoS Class:** Display the QoS class that NAS assigns to the port.  This field is left blank if QoS is not set by NAS.

**Port VLAN ID:** The VLAN ID of the port assigned by NAS. This field is left blank if VLAN ID is not set by NAS.

#### *4.5.5.2.3 Port Statistics*



NAS Statistics  Port 5    Port 5    Auto-refresh ☐ Refresh Clear

Port State

| | |
|---|---|
| Admin State | Force Authorized |
| Port State | Authorized |

Port Counters

| Receive EAPOL Counters | | Transmit EAPOL Counters | |
|---|---|---|---|
| Total | 0 | Total | 1 |
| Response ID | 0 | Request ID | 0 |
| Responses | 0 | Requests | 0 |
| Start | 0 | | |
| Logoff | 0 | | |
| Invalid Type | 0 | | |
| Invalid Length | 0 | | |

***<u>Port State</u>***

**Admin State:** Display the port’s current administrative state.

**Port Status:** Display the port state.

***Receive EAPOL Counters***

**Total:** The number of valid EAPOL frames of any type that has been received by the switch.

**Response ID:** The number of valid EAPOL Response Identity frames that have been received by the switch.

**Responses:** The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.

**Start:** The number of EAPOL Start frames that have been received by the switch.

**Logoff:** The number of valid EAPOL Logoff frames that have been received by the switch.

**Invalid Type:** The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.

**Invalid Length:** The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.

***Transmit EAPOL Counters***

**Total:** The number of EAPOL frames of any type that has been transmitted by the switch.

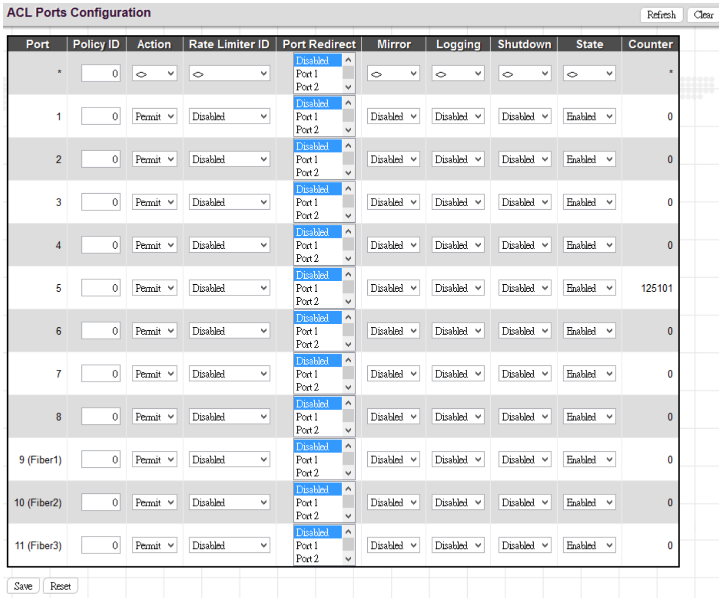
**Request ID:** The number of valid EAPOL Request Identity frames that have been received by the switch.

**Requests:** The number of valid EAPOL request frames (other than Request Identity frames) that have been received by the switch.

### *4.5.5.3 ACL*

ACL is a sequential list established to allow or deny users to access information or perform tasks on the network. In this switch, users can establish rules applied to port numbers to permit or deny actions or restrict rate limit.

#### *4.5.5.3.1 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.

#### *4.5.5.3.2 Rate Limiters*

**ACL Rate Limiter Configuration**

| Rate Limiter ID | Rate | Unit |
|---|---|---|
| * | 1 | <> |
| 1 | 1 | pps |
| 2 | 1 | pps |
| 3 | 1 | pps |
| 4 | 1 | pps |
| 5 | 1 | pps |
| 6 | 1 | pps |
| 7 | 1 | pps |
| 8 | 1 | pps |
| 9 | 1 | pps |
| 10 | 1 | pps |
| 11 | 1 | pps |
| 12 | 1 | pps |
| 13 | 1 | pps |
| 14 | 1 | pps |
| 15 | 1 | pps |
| 16 | 1 | pps |

Save Reset

**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.

#### *4.5.5.3.3 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.

**Access Control List Configuration** Auto-refresh Refresh Clear Remove All

| Ingress Port | Policy / Bitmask | Frame Type | Action | Rate Limiter | Port Redirect | Mirror | Counter | |
|---|---|---|---|---|---|---|---|---|
| 1 | Any | Any | Permit | Disabled | Disabled | Disabled | 0 | |

**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.

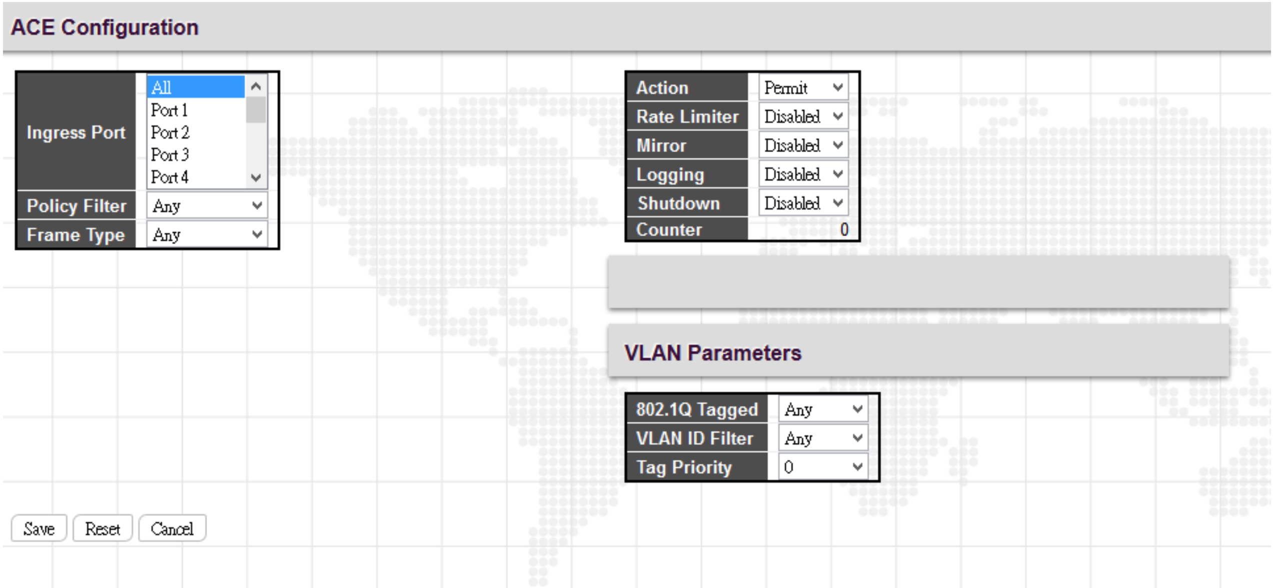
**Rate Limiter:** Display rate limiter is enabled or disabled when matched frames are found.

**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 the plus sign to add a new ACE entry.




***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.

***<u>IP Parameters</u>***

**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.

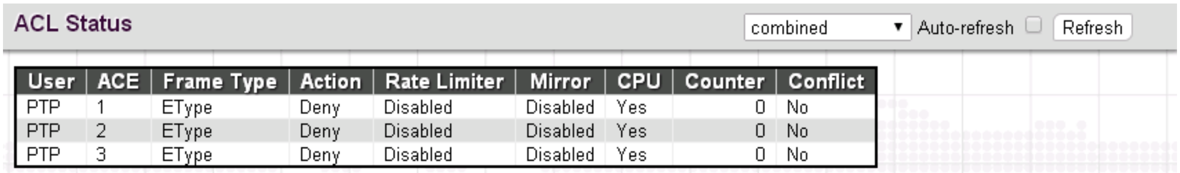
***<u>IPv6 Parameters</u>***

**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.

#### *4.5.5.3.4 ACL Status*




| User | ACE | Frame Type | Action | Rate Limiter | Mirror | CPU | Counter | Conflict |
|---|---|---|---|---|---|---|---|---|
| PTP | 1 | EType | Deny | Disabled | Disabled | Yes | 0 | No |
| PTP | 2 | EType | Deny | Disabled | Disabled | Yes | 0 | No |
| PTP | 3 | EType | Deny | Disabled | Disabled | Yes | 0 | No |

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

**User:** Display the ACL user.

**ACE:** Display ACE entry ID.

**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.

**Port Redirect:** Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

**Mirror:** Specify the mirror operation of this port. The allowed values are:

**Enabled:** Frames received on the port are mirrored.

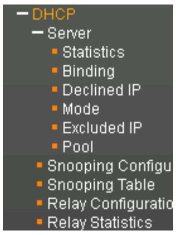
**Disabled:** Frames received on the port are not mirrored. The default value is "Disabled".

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

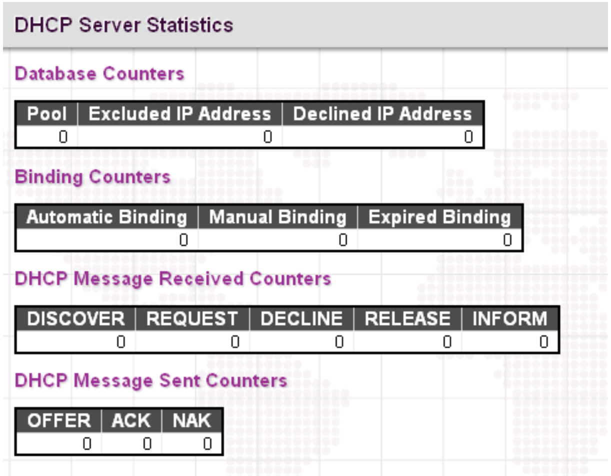
**Counter:** The counter indicates the number of times the ACE was hit by a frame.

**Conflict:** Indicate the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

### *4.5.5.4 DHCP*



#### *4.5.5.4.1 DHCP Server Statistics*




***Database Counters***

**Pool:** The number of pool that has been configured.

**Excluded IP Address:** The number of excluded IP address.

**Declined IP Address:** The number of declined IP address.

***Binding Counters***

**Automatic Binding:** The number of bindings with network-type pools.

**Manual Binding:** The number of bindings that the network engineer assigns an IP address to a client. In other words, the pool is of host type.

**Expired Binding:** The number of bindings that their lease time expired or they are cleared from Automatic or Manual type bindings.

***DHCP Message Received Counters***

**Discover:** The number of DHCP DISCOVER messages received.

**Request:** The number of DHCP REQUEST messages received.

**Decline:** The number of DHCP DECLINE messages received.

**Release:** The number of DHCP RELEASE messages received.

**Inform:** The number of DHCP INFORM messages received.

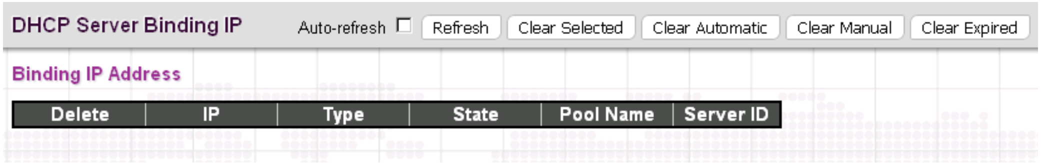
***DHCP Message Sent Counters***

**OFFER:** The number of DHCP OFFER messages sent.

**ACK:** The number of DHCP ACK messages sent.

**NAK:** The number of DHCP NAK messages sent.

#### *4.5.5.4.2 DHCP Server Binding IP*




**IP:** The IP address allocated to DHCP client.

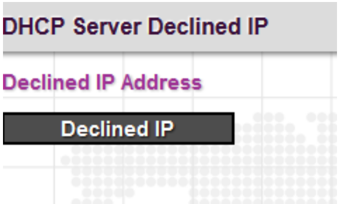
**Type:** The type of binding method. This field can be "Automatic", "Manual" or "Expired".

**State:** The state of binding. Possible states are "Committed", "Allocated", or "Expired".

**Pool Name:** The pool that generates the binding.

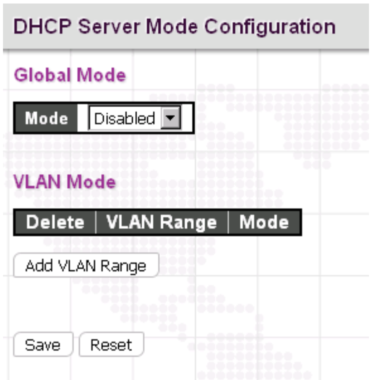
**Server ID:** The server IP address to create the binding.

#### *4.5.5.4.3 DHCP Server Declined IP*




**Declined IP:** Displays a list of declined IP addresses.

#### *4.5.5.4.4 DHCP Server Mode Configuration*




***Global Mode***

**Mode:** Enable or disable DHCP server mode. When enabled, this device can act as a DHCP server and provide IP address to clients that request for one.

***VLAN Mode***

Click "Add VLAN Range" to create a new entry.

**VLAN Range:** Enter the VLAN Range in which DHCP server is enabled or disabled. The starting VLAIN ID must be smaller than or equal to the ending VLAN ID. If there is only one VLAN ID, then it can be entered either in starting or ending VLAN ID field.

**Mode:** Indicates the operation mode per VLAN.

**Enabled:** Enable DHCP server per VLAN.

**Disabled:** Disable DHCP server per VLAN.

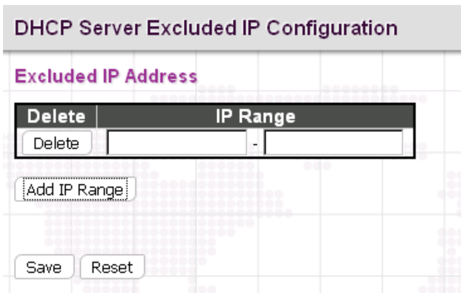
---

***NOTE:*** *If you would like to disable DHCP server on an existing VLAN range, then follow the steps below.*

1. *Add one "Add VLAN Range" entry.*
2. *Enter the VLAN range that you want to disable.*
3. *Choose "Disabled" mode.*
4. *Click "Save" to apply the change.*

---

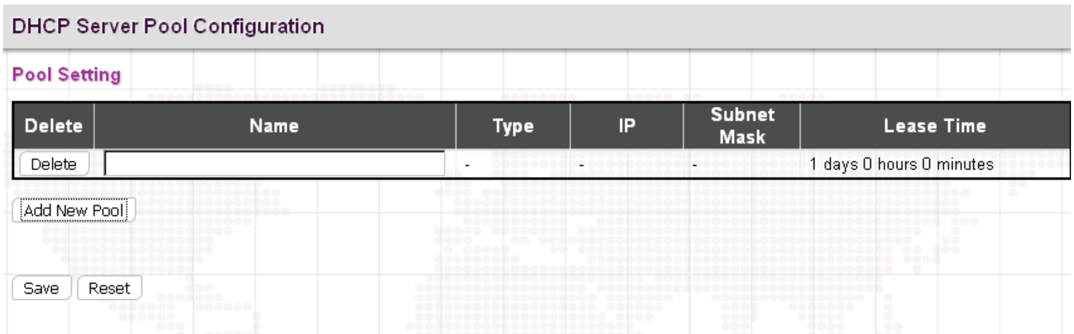
#### *4.5.5.4.5 DHCP Server Excluded IP Configuration*




Click "Add IP Range" to set up IP pool range.

**IP Range:** Enter the starting and ending IP address that are not allocated to DHCP clients. The starting IP address must be smaller or equal to the ending IP address. If there is only one excluded IP address, it can be entered either in starting or ending IP address field. The total Excluded IP address ranges can be supported is 16.

#### *4.5.5.4.6 DHCP Server Pool Configuration*




Click "Add New Pool" to add a new entry to the list. The maximum entries supported are 640.

**Name:** Enter the pool name for this entry. All printable characters are supported except white space. Click on the pool name after save to configure its detailed settings.

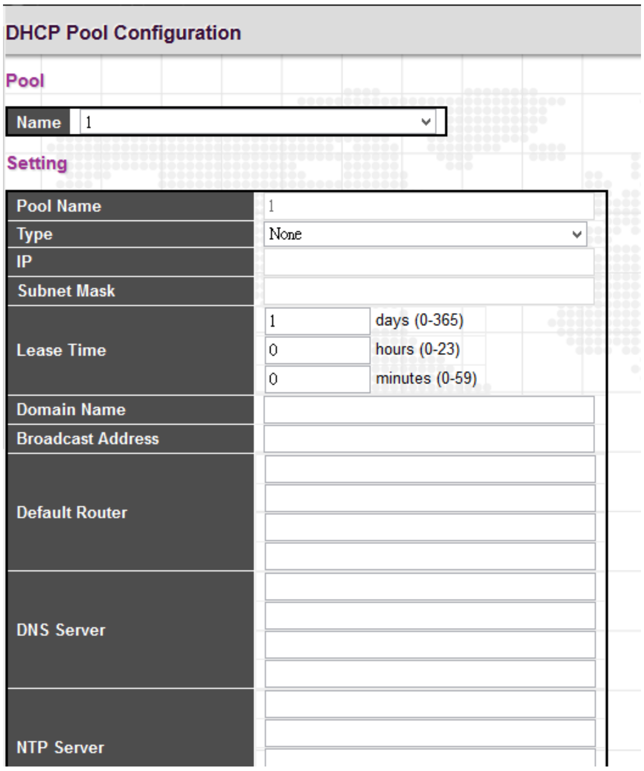
**Type:** Display which type the pool is. The displayed options include Network and Host. If "-" is displayed, it means this field has not been defined yet.

**IP:** Display network number of the DHCP address pool. If "-" is displayed, it means this field has not been defined yet.

**Subnet Mask:** Display subnet mask of the DHCP address pool. If "-" is displayed, it means this field has not been defined yet.

**Lease Time:** Display the lease time of the configured pool.

Click on the pool name to configure its detailed settings.




***Pool***

**Name:** Select the pool name that you want to configure from the pull-down menu.

***Setting***

**Pool Name:** Display the pool name for this configured entry.

**Type:** Select the pool type.

> **Network:** The pool defines a pool of IP addresses to service more than one DHCP client.
>
> **Host:** The pool services for a specific DHCP client identified by client identifier or hardware address.

**IP:** Specify the network IP of the DHCP address pool.

**Subnet Mask:** Specify subnet mask of the DHCP address pool.

**Lease Time:** Specify lease time that a client needs to send requests to the DHCP server for renewed IP address. If all are 0's, then it means the lease time is infinite.

**Domain Name:** Specify the domain name that a client use when resolving hostname via DNS.

**Broadcast Address:** Specify the broadcast address in use on the client's subnet.

**Default Router:** Specify a list of IP addresses for routers on the clients' subnet.

**DNS Server:** Specify a list of Domain Name System name servers available to the client.

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

**NetBios Node Type:** Select NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002.

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

**NetBIOS Name Server:** Specify a list of NBNS name servers listed in order of preference.

**NIS Domain Name:** Specify the name of the client's NIS domain.

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

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

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

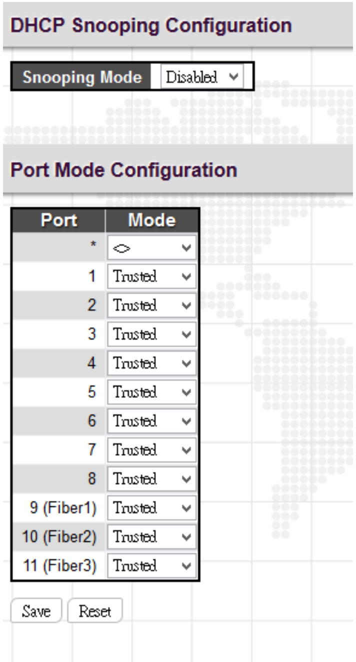
**Client Name:** Specify the name of client to be used when the pool is the type of host.

**Vendor 1~8 Class Identifier:** Specify to be used by DHCP client to optionally identify the vendor type and configuration of a DHCP client. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier.

**Vendor 1~8 Specific Information:** Specify vendor specific information according to option 60 vendor class identifier.

#### *4.5.5.4.7 Snooping Configuration*

DHCP Snooping allows the switch to protect a network from attacking by other devices or rogue DHCP servers. When DHCP Snooping is enabled on the switch, it can filter IP traffic on insecure (untrusted) ports that the source addresses cannot be identified by DHCP Snooping. The addresses assigned to connected clients on insecure ports can be carefully controlled by either using the dynamic binding registered with DHCP Snooping or using the static binding configured with IP Source Guard.




***<u>DHCP Snooping Configuration</u>***

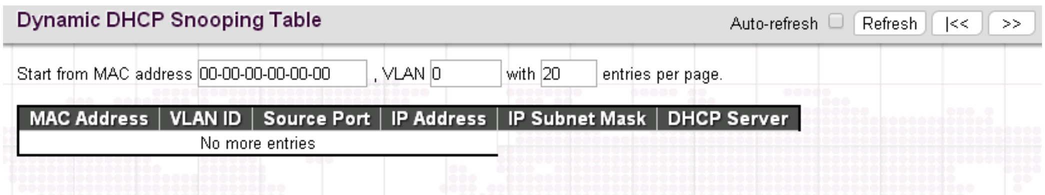
**Snooping Mode:** Enable or disable DHCP Snooping function globally. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

***Port Mode Configuration***

**Port:** Port number. "Port *" rules apply to all ports.

**Mode:** Select the DCHP Snooping port mode. Ports can be set to either “Trusted” or “Untrusted”.

### *4.5.5.4.8 Snooping Table*




DHCP clients who obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Items displayed include the following:

**MAC Address:** Client hardware MAC address

**VLAN ID:** VLAN number of the client interface

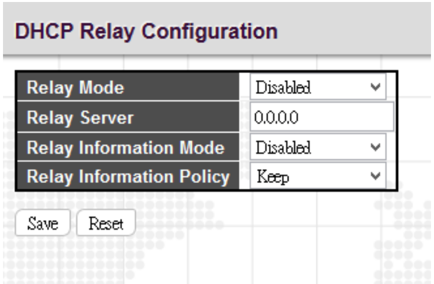
**Source Port:** The port number of the client that binds with IP address.

**IP Address:** Client IP address assigned from the DHCP server.

**IP Subnet Mask**: Client IP subnet mask.

**DHCP Server:** The DHCP Server that assigns IP address.

#### *4.5.5.4.9 Relay Configuration*




**Relay Mode:** Enable or disable the DHCP relay function.

**Relay Server**: Enter DHCP server IP address that is used by the switch's DHCP relay agent.

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

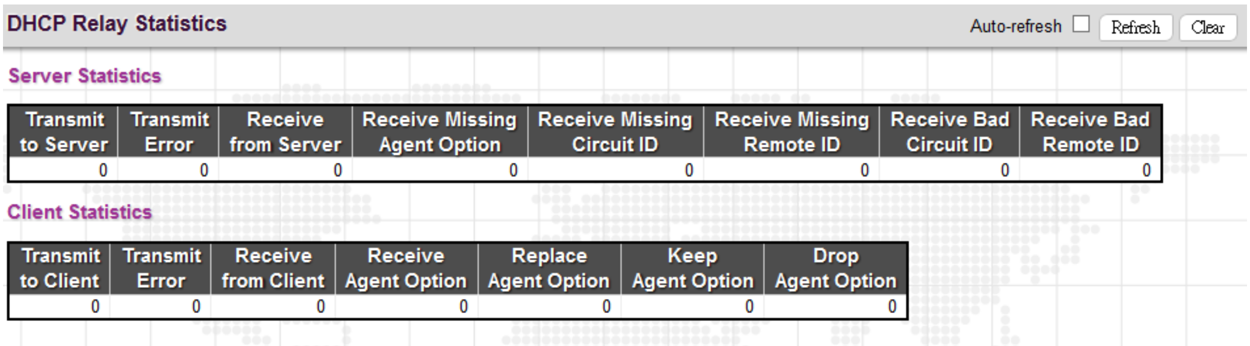
**Relay Information Policy:** Select Relay Information policy for DHCP client that includes option 82 information.

**Replace:** Replace the DHCP client packet information with the switch's relay information. This is the default setting.

**Keep:** Keep the client's DHCP information.

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

#### *4.5.5.4.10 Relay Statistics*




***<u>DHCP Relay Statistics</u>***

**Transmit to Server:** The number of packets that are relayed from client to server.

**Transmit Error:** The number of packets that resulted in errors while being sent to clients.

**Receive from Client:** The number of packets received from server.

**Receive Missing Agent Option:** The number of packets received without agent information options.

**Receive Missing Circuit ID:** The number of packets received with the Circuit ID option missing.

**Receive Missing Remote ID:** The number of packets received with the Remote ID option missing.

**Receive Bad Circuit ID:** The number of packets whose Circuit ID option did not match known circuit ID.

**Receive Bad Remote ID:** The number of packets whose Remote ID option did not match known Remote ID.

***Client Statistics***

**Transmit to Client:** The number of relayed packets from server to client.

**Transmit Error:** The number of packets that resulted in error while being sent to servers.

**Receive from Client**: The number of received packets from server.

**Receive Agent Option:** The number of received packets with relay agent information option.

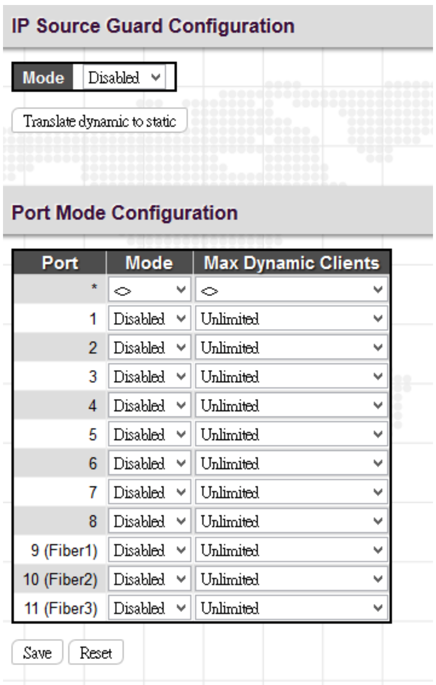
**Replace Agent Option:** The number of packets which were replaced with relay agent information option.

**Keep Agent Option:** The number of packets whose relay agent information was retained.

**Drop Agent Option:** The number of packets that were dropped which were received with relay agent information.

### *4.5.5.5 IP Source Guard*

#### *4.5.5.5.1 Configuration*




***IP Source Guard Configuration***

**Mode:** Enable or disable IP source guard globally.

**Translate dynamic to static:** Click this button to translate dynamic entries to static ones.

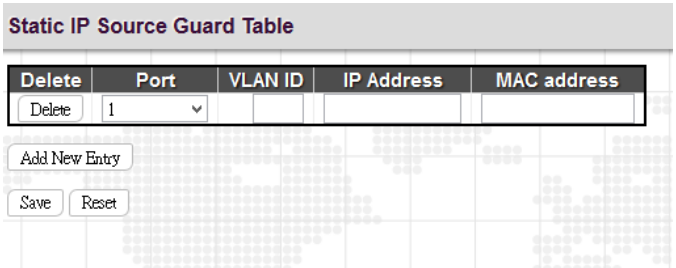
***Port Mode Configuration***

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

**Mode:** Enable or disable IP source guard on a port. Please note that to make IP source guard work, both global mode and port mode must be enabled.

**Max Dynamic Clients:** Select the maximum number of dynamic clients that can be learned on a port. The available options are 0, 1, 2, unlimited. If the port mode is enabled and the maximum number of dynamic clients is equal 0, the switch will only forward IP packets that are matched in static entries for a given port.

#### *4.5.5.5.2 Static Table*




**Port:** Select a port to which a static entry is bound.

**VLAN ID:** Enter VLAN ID that has been configured.

**IP Address:** Enter a valid IP address.

**MAC Address:** Enter a valid MAC address.

Click the “Add New Entry” button to insert an entry to the table.

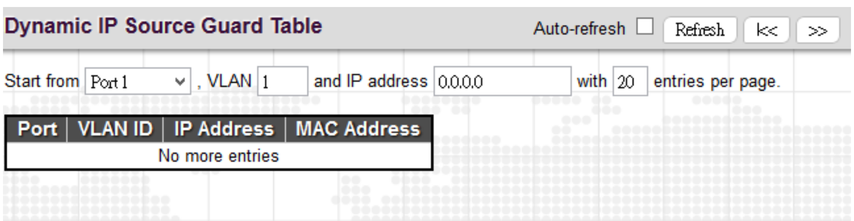
Select the “Delete” checkbox to remove the entry during the next save.

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

Click the “Reset” button to restore settings to default settings or previously configured settings.

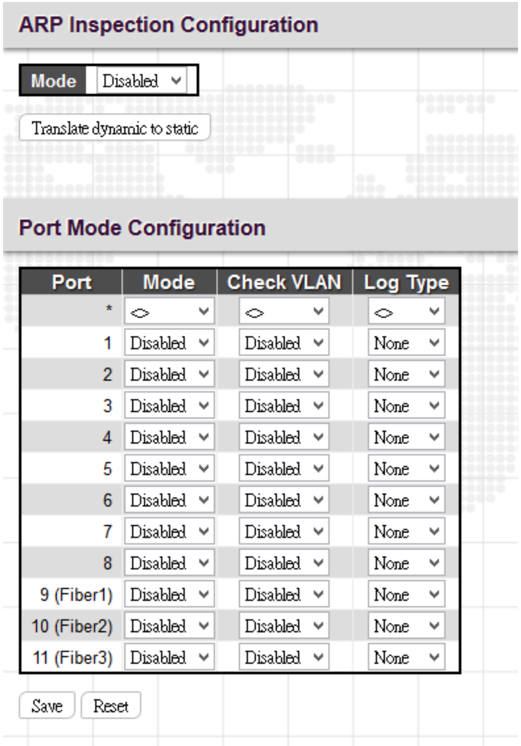
#### *4.5.5.5.3 Dynamic Table*

The Dynamic IP Source Guard table shows entries sorted by port, VLAN ID, IP address and MAC address. By default, each page displays 20 entries. However, it can display 999 entries by entering the number in “entries per page” input field.



### *4.5.5.6 ARP inspection*

#### *4.5.5.6.1 Port Configuration*




***<u>ARP Inspection Configuration</u>***

**Mode:** Enable or disable ARP inspection function globally.

***<u>Port Mode Configuration</u>***

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

**Mode:** Enable or disable ARP Inspection on a port. Please note that to make ARP inspection work, both global mode and port mode must be enabled.

**Check VLAN:** Enable or disable check VLAN operation.

**Log Type:** There are four log types available.

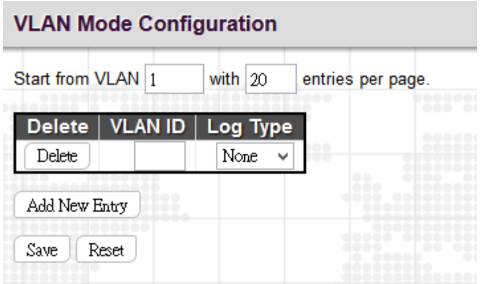
**None:** Log nothing.

**Deny:** Log denied entries.

**Permit:** Log permitted entries.

**All:** Log all entries.

#### *4.5.5.6.2 VLAN Configuration*




**VLAN ID:** Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.

**Log Type:** There are four log types available.

**None:** Log nothing.

**Deny:** Log denied entries.

**Permit:** Log permitted entries.

**All:** Log all entries.

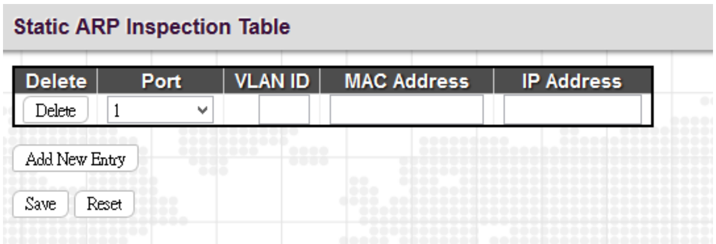
Click the “Add New Entry” button to insert an entry to the table.

Select the “Delete” checkbox to remove the entry during the next save.

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

Click the “Reset” button to restore settings to default settings or previously configured settings.

#### *4.5.5.6.3 Static Table*




**Port:** Select a port to which a static entry is bound.

**VLAN ID:** Specify a configured VLAN ID.

**MAC Address:** Specify an allowed source MAC address in ARP request packets.

**IP Address:** Specify an allowed source IP address in ARP request packets.

Click the “Add New Entry” button to insert an entry to the table.

Select the “Delete” checkbox to remove the entry during the next save.

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

Click the “Reset” button to restore settings to default settings or previously configured settings.

#### *4.5.5.6.4 Dynamic Table Configuration*


**Port:** The port number of this entry.

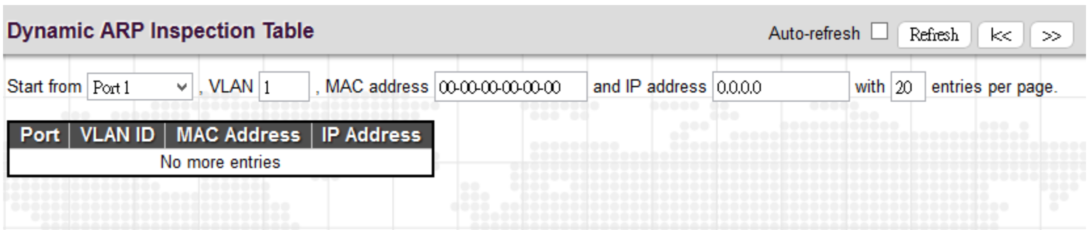
**VLAN ID:** VLAN ID in which the ARP traffic is permitted.

**MAC Address**: User MAC address of this entry.

**IP Address:** User IP address of this entry.

**Translate to static:** Click the button to translate the dynamic entry to static one.

#### *4.5.5.6.5 Dynamic Table Status*



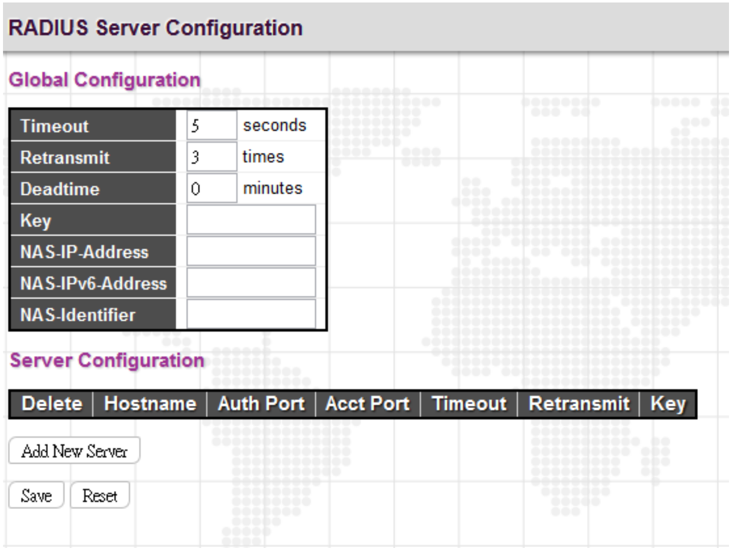

**Port:** The port number of this entry.

**VLAN ID:** VLAN ID in which the ARP traffic is permitted.

**MAC Address:** User MAC address of this entry.

## 4.5.6 RADIUS

### 4.5.6.1 Configuration




***<u>Global Configuration</u>***

**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 1440minutes.

**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.

***<u>Sever Configuration</u>***

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

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

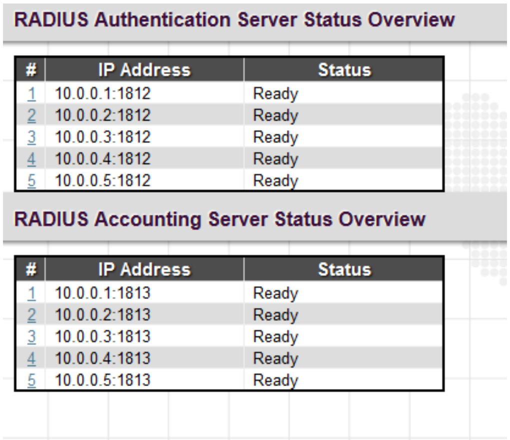
**Acct Port:** The UDP port to be used on the RADIUS server for accounting.

**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.

### 4.5.6.2 RADIUS Overview



RADIUS Authentication Server Status Overview

| # | IP Address | Status |
|---|---|---|
| 1 | 10.0.0.1:1812 | Ready |
| 2 | 10.0.0.2:1812 | Ready |
| 3 | 10.0.0.3:1812 | Ready |
| 4 | 10.0.0.4:1812 | Ready |
| 5 | 10.0.0.5:1812 | Ready |

RADIUS Accounting Server Status Overview

| # | IP Address | Status |
|---|---|---|
| 1 | 10.0.0.1:1813 | Ready |
| 2 | 10.0.0.2:1813 | Ready |
| 3 | 10.0.0.3:1813 | Ready |
| 4 | 10.0.0.4:1813 | Ready |
| 5 | 10.0.0.5:1813 | Ready |

**#:** The number of Authentication & Accounting server. Five Authentication & Accounting servers are supported. Click on the number to view each server's details.

**IP Address:** The configured IP address and UPD port number.

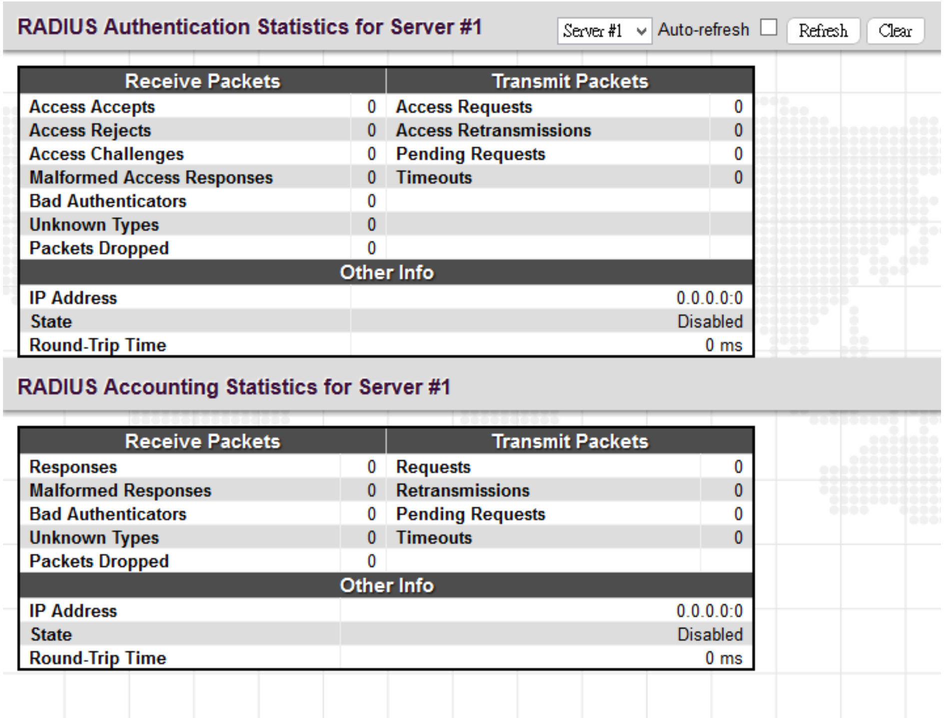
**Status:** The current state of RADIUS authentication server. Displayed states include the following:

**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.

### 4.5.6.3 RADIUS Details



**RADIUS Authentication Statistics for Server #1**

Server #1 Auto-refresh Refresh Clear

| Receive Packets | | Transmit Packets | |
|---|---|---|---|
| Access Accepts | 0 | Access Requests | 0 |
| Access Rejects | 0 | Access Retransmissions | 0 |
| Access Challenges | 0 | Pending Requests | 0 |
| Malformed Access Responses | 0 | Timeouts | 0 |
| Bad Authenticators | 0 | | |
| Unknown Types | 0 | | |
| Packets Dropped | 0 | | |

| Other Info | |
|---|---|
| IP Address | 0.0.0.0:0 |
| State | Disabled |
| Round-Trip Time | 0 ms |

**RADIUS Accounting Statistics for Server #1**

| Receive Packets | | Transmit Packets | |
|---|---|---|---|
| Responses | 0 | Requests | 0 |
| Malformed Responses | 0 | Retransmissions | 0 |
| Bad Authenticators | 0 | Pending Requests | 0 |
| Unknown Types | 0 | Timeouts | 0 |
| Packets Dropped | 0 | | |

| Other Info | |
|---|---|
| IP Address | 0.0.0.0:0 |
| State | Disabled |
| Round-Trip Time | 0 ms |

***<u>RADIUS Authentication Statistics for Server</u>***

**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.

***<u>RADIUS Accounting Statistics for Server</u>***

**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.

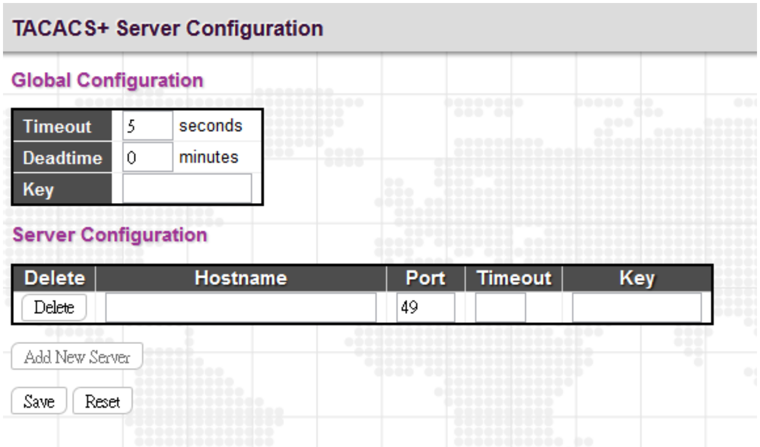
**Not Ready:** The server is enabled, but IP communication is not yet up and running.

**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.

### *4.5.6.4 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 1440 minutes.

**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.

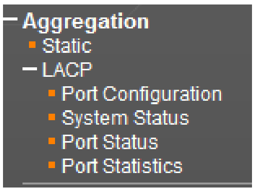
**Timeout:** If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

**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.

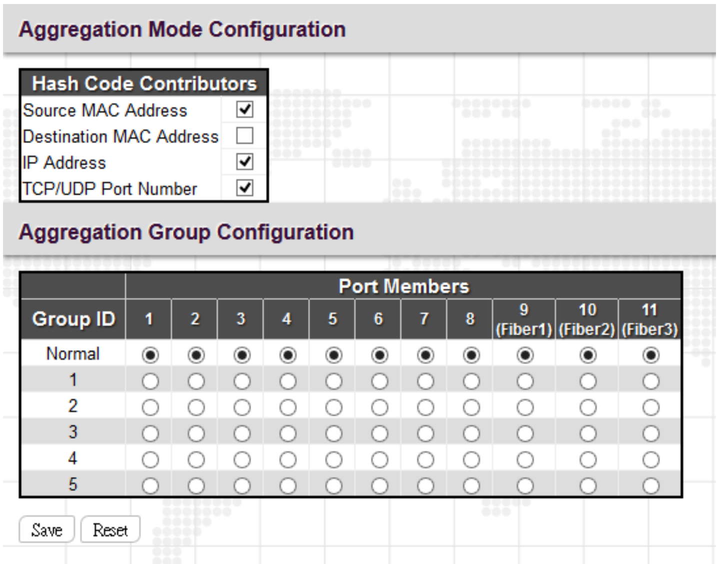
## 4.6 Aggregation

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.




### 4.6.1 Static




***<u>Aggregation Mode Configuration</u>***

**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.

***<u>Aggregation Group Configuration</u>***

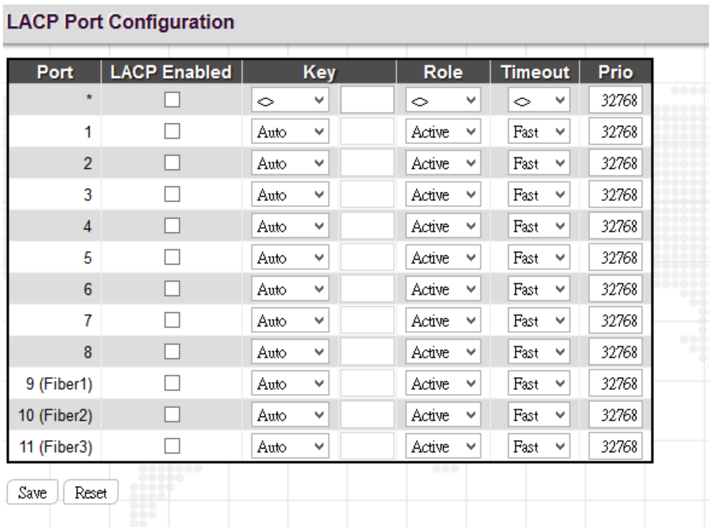
**Group ID:** Trunk ID number. “Normal” means that no aggregation is used. Five aggregation groups are available for use. Each group contains at least 2 to 10 links (ports). Please note that each port can only be used once in Group ID 1~5.

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

## 4.6.2 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.

### 4.6.2.1 Port Configuration



**LACP Port Configuration**

| Port | LACP Enabled | Key | | Role | Timeout | Prio |
|---|---|---|---|---|---|---|
| * | ☐ | <> | | <> | <> | 32768 |
| 1 | ☐ | Auto | | Active | Fast | 32768 |
| 2 | ☐ | Auto | | Active | Fast | 32768 |
| 3 | ☐ | Auto | | Active | Fast | 32768 |
| 4 | ☐ | Auto | | Active | Fast | 32768 |
| 5 | ☐ | Auto | | Active | Fast | 32768 |
| 6 | ☐ | Auto | | Active | Fast | 32768 |
| 7 | ☐ | Auto | | Active | Fast | 32768 |
| 8 | ☐ | Auto | | Active | Fast | 32768 |
| 9 (Fiber1) | ☐ | Auto | | Active | Fast | 32768 |
| 10 (Fiber2) | ☐ | Auto | | Active | Fast | 32768 |
| 11 (Fiber3) | ☐ | Auto | | Active | Fast | 32768 |

Save Reset

**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.

### *4.6.2.2 System Status*

**LACP System Status**

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

**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.

### *4.6.2.3 Port Status*

**LACP Status**

| Port | LACP | Key | Aggr ID | Partner System ID | Partner Port | Partner Prio |
|---|---|---|---|---|---|---|
| 1 | No | - | - | - | - | - |
| 2 | No | - | - | - | - | - |
| 3 | No | - | - | - | - | - |
| 4 | No | - | - | - | - | - |
| 5 | No | - | - | - | - | - |
| 6 | No | - | - | - | - | - |
| 7 | No | - | - | - | - | - |
| 8 | No | - | - | - | - | - |
| 9 (Fiber1) | No | - | - | - | - | - |
| 10 (Fiber2) | No | - | - | - | - | - |
| 11 (Fiber3) | Yes | 3 | - | - | - | - |

**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.

#### 4.6.2.4 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 |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 |
| 9 (Fiber1) | 0 | 0 | 0 | 0 |
| 10 (Fiber2) | 0 | 0 | 0 | 0 |
| 11 (Fiber3) | 747 | 747 | 0 | 0 |

**Port:** The port number.

**LACP Received:** The number of LACP packets received on a port.

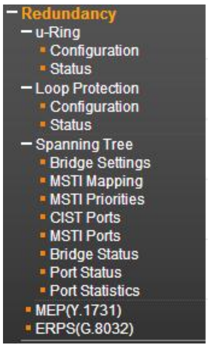
**LACP Transmitted:** The number of LACP packets transmitted by a port

**Discarded:** The number of unknown and illegal packets that have been discarded on a port.

## 4.7 Redundancy

Designing redundant paths that can protect networks from unexpected failovers is extremely important in mission-critical networks that need to provide uninterrupted services. However, redundant paths mean that possible loops may occur in networks and bring down networks eventually if they are not treated carefully. In practice, several loop protection methods are implemented to ensure that networks function normally without loops and recover as soon as possible when a point of failure occurs. The most popular ones are STP (802.1d), RSTP (802.1w) and MSTP (802.1s). For industrial applications, the proprietary u-Ring and ERPS (G.8032) are highly recommended since they can achieve faster recovery time than any STP protocol.

In this section, the redundancy-related functions will be introduced individually. The functions covered in this section can be seen from the “Redundancy” menu.

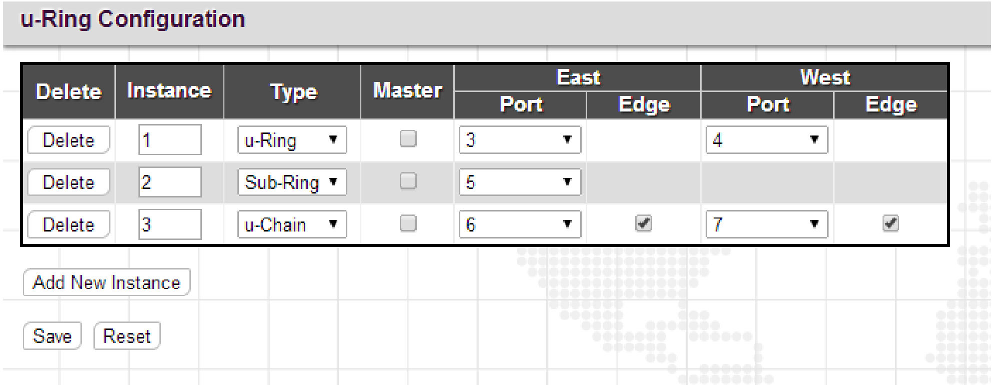



### 4.7.1 u-Ring

u-Ring is a proprietary redundancy technology that supports 250 units in a ring topology and can bring redundant paths into service within 10 ms when link failures occur. Compared with spanning tree protocol, u-Ring achieves faster recovery time on the network and is more flexible and scalable in network architecture. u-Ring redundancy technology can automatically self identifies the ring Master (the user-defined Master is also supported) and then block a port resided in Master device for backup purposes. Once the disconnection is detected on the network, u-Ring can bring backup ports back into “forwarding” mode so that the disconnected path can keep contact with the whole network.

For more information about u-Ring configurations, please see Appendix A: u-Ring Configuration Procedure guide.

### *4.7.1.1 Configuration*



u-Ring Configuration

| Delete | Instance | Type | Master | East | | West | |
|---|---|---|---|---|---|---|---|
| | | | | Port | Edge | Port | Edge |
| Delete | 1 | u-Ring | ☐ | 3 | | 4 | |
| Delete | 2 | Sub-Ring | ☐ | 5 | | | |
| Delete | 3 | u-Chain | ☐ | 6 | ☑ | 7 | ☑ |



Click “Add New Instance” button to add a new entry.

**Instance:** The instance number. The total instances supported are 5.

**Type:** u-Ring supports 3 ring types. They are explained below individually.

**u-Ring:** u-Ring type is used in a closed ring topology. All participating devices must support u-Ring redundancy technology.

Figure 1. Single ring

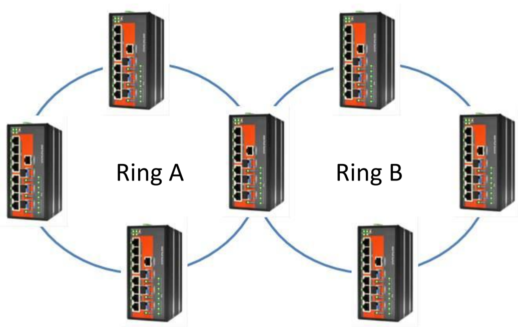




Figure 2. Two rings

**u-Chain:** u-Chain type is used when u-Ring supported devices interconnect to a network or devices that does not support u-Ring redundancy technology.

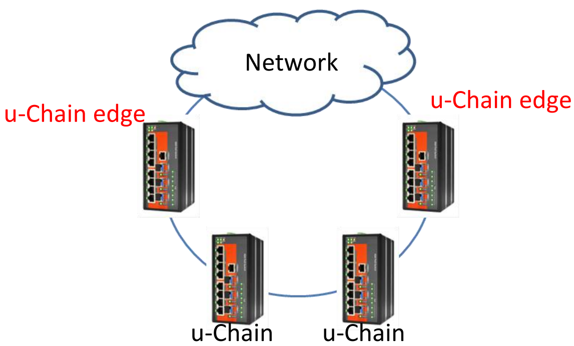




Figure 3. u-Chain ring connects to a network

**Sub-Ring:** Sub-Ring is used in an open ring and only has one node. In a networking topology, Sub-Ring type must co-exist with u-Ring type or u-Chain type. No third-party devices are used in this ring type.

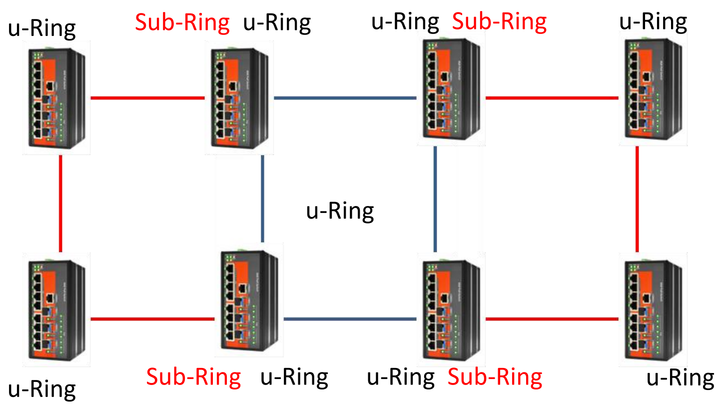



Figure 4. Sub-Ring

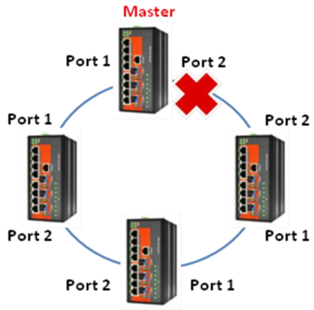
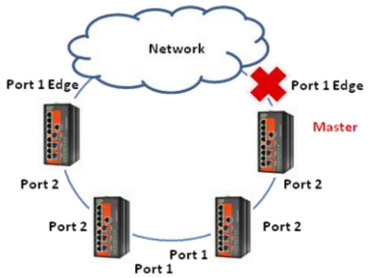
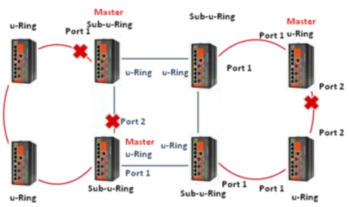
**Master:** The Master is generally used to decide which segment acts as a backup path. The user can manually select the checkbox to set the device in a ring as a Master. However, if all devices' Master checkboxes are left unchecked, the u-Ring protocol will assign one of the devices in the ring as the Master depending on their MAC address. The election process is explained below in "Determining a Master and blocking a port".

**Port:** Select the west and east port from the pull-down menu.

**Edge:** This field appears only when you select u-Chain type. Select the checkbox to set the selected port as a u-Chain edge port.

**Determining a Master and blocking a port**

| | u-Ring | u-Chain | Sub-Ring |
|---|---|---|---|
| **Step 1. Determining a Master** | ● Manually select the Master in a ring.<br><br>● If several devices are set to Master, the u-Ring redundancy protocol decides the Master in a ring depending on devices' MAC address. The device with the **biggest MAC address** becomes the Master in a ring.<br><br>● If no device in a ring is set to Master, the u-Ring redundancy protocol decides the Master in a ring depending on devices' MAC address. The device with the **biggest MAC address** becomes the Master in a ring. | ● Manually select the Master in a ring.<br><br>●The device with a configured **edge port** that has the **biggest MAC address** is selected as the Master.<br><br>● If the Master is mis-assigned to the device that does not have an edge, the u-Ring redundancy protocol will ignore this mis-configuration.<br><br>*Note: When selecting u-Chain type, only the devices with an edge port or edge ports are eligible to be elected as the Master.* | ●Manually select the Master in a ring.<br><br>● If several devices are set to Master, the u-Ring redundancy protocol decides the Master in a ring depending on devices' MAC address. The device with the **biggest MAC address** becomes the Master in a ring.<br><br>● If no device in a ring is set to Master, the u-Ring redundancy protocol decides the Master in a ring depending on devices' MAC address. The device with the **biggest MAC address** becomes the Master in a ring. |
| **Step 2. Blocking a port** | The port with **higher port number** in Master device is blocked. | ● The edge port in Master device is blocked. | The port with **higher port number** in Master device is blocked. |

<table>
<tr><td></td><td></td><td>● If the Master has two edge ports, the port with higher port number is blocked.</td><td></td></tr>
<tr><td>Example</td><td>
</td><td>
</td><td>
</td></tr>
</table>

### *4.7.1.2 Status*

**u-Ring Status**

| Instance | Type | Role | East Port | | | West Port | | | Healthy |
|---|---|---|---|---|---|---|---|---|---|
| | | | Number | State | Edge | Number | State | Edge | |
| 1 | u-Ring | Master | 8 | Blocking | --- | 7 | Forwarding | --- | ● |

**Instance:** The instance number.

**Type:** Display the type of redundancy ring.

**Role:** This field can be Master or Slave (paths in Slave device will not be blocked).

**East & West Port Number:** The configured port number in a instance.

**East & West Port State:** The current state of the configured port in a ring. The displayed state can be one of the following:

**Forwarding:** The path is in normal transmission.

**Blocking:** The path is blocked and acts as  a backup path.

**Down:** No physical connection.

**East & West Port Edge:** This field shows whether the configured port is an edge port or not.

**Healthy:** This field graphically displays the current ring status.

**:** The path is never ringed.

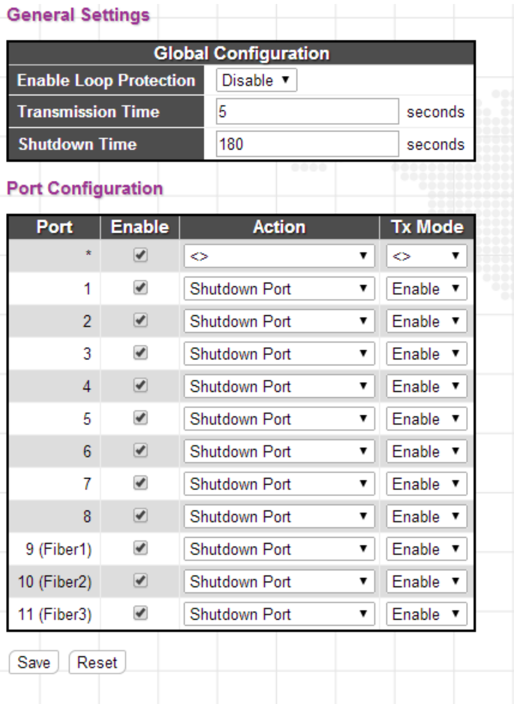
**:** The  Master is elected and backup path is blocked. The network with a redundant path works normally.

**:**  The physical link or connection in the ring is down. The status of backup path is changed from “blocked” to “forwarding” status when one of the forwarding paths is down.

### 4.7.2 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.

#### 4.7.2.1 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. “Port *” 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.

### 4.7.2.2 Status

**Loop Protection Status**

| Port | Action | Transmit | Loops | Status | Loop | Time of Last Loop |
|---|---|---|---|---|---|---|
| 1 | Shutdown+Log | Enabled | 0 | Down | - | - |
| 2 | Shutdown+Log | Enabled | 0 | Down | - | - |
| 3 | Shutdown | Enabled | 0 | Down | - | - |
| 4 | Shutdown | Enabled | 0 | Down | - | - |
| 5 | Shutdown | Enabled | 0 | Up | - | - |
| 6 | Shutdown | Enabled | 0 | Down | - | - |
| 7 | Shutdown | Enabled | 0 | Down | - | - |
| 8 | Shutdown | Enabled | 0 | Down | - | - |
| 9 (Fiber1) | Shutdown | Enabled | 0 | Down | - | - |
| 10 (Fiber2) | Shutdown | Enabled | 0 | Down | - | - |
| 11 (Fiber3) | Shutdown | Enabled | 0 | Down | - | - |

**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.

## 4.7.3 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.

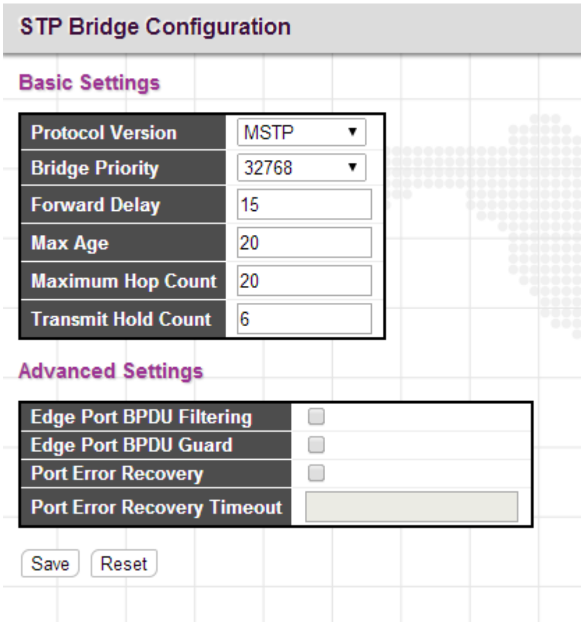
To solve problems causing by bridge loops, spanning tree allows a network design to include redundant links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manually enabling/disabling these backup links.

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.

### *4.7.3.1 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.

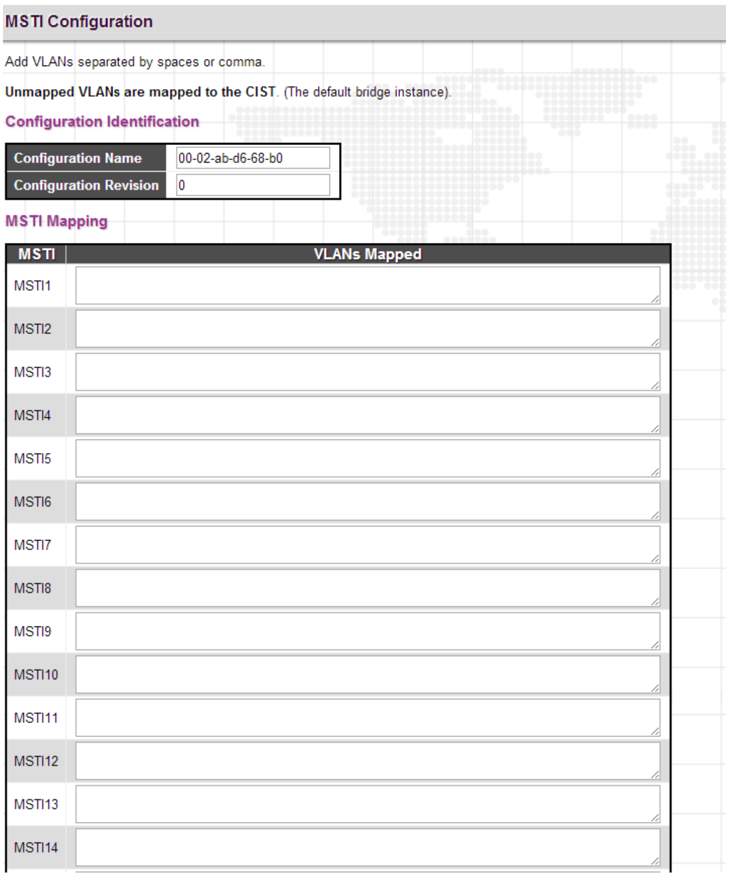
**Edge Port BPDU Guard:** Edge ports generally connect directly to PC, file servers or printers. Therefore, edge ports are configured to allow rapid transition. Under normal situations, edge ports should not receive configuration BPDUs. However, if they do, this probably is due to malicious attacks or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

### *4.7.3.2 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.

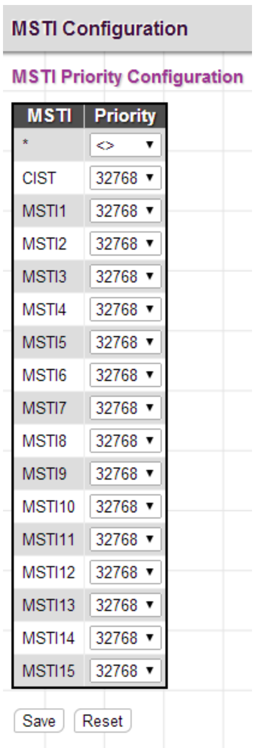
**Configuration Revision:** The revision number for this MSTI. The allowed range is 0~65535.

***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.

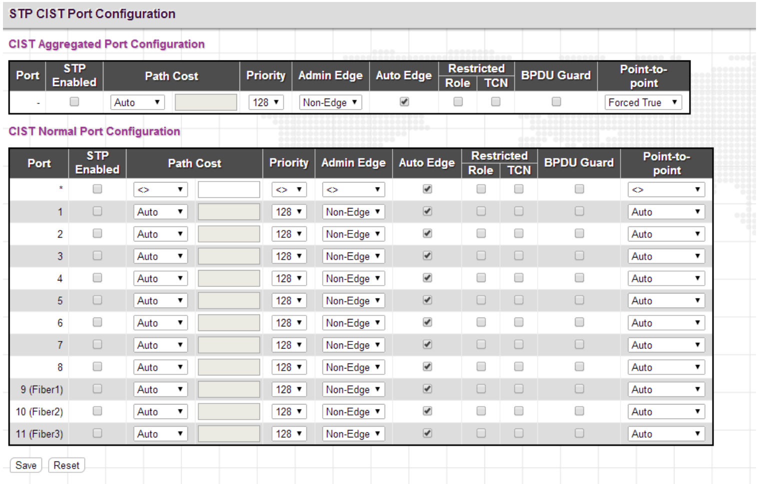
### *4.7.3.3 MSTI Priorities*




**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.

### 4.7.3.4 CIST Ports




***<u>CIST Aggregated Port Configuration</u>***

**Port:** The port number.

**STP Enabled:** Enable STP function

**Path Cost:** Path cost is used to determine the best path between devices. If “Auto” mode is selected, the system automatically detects the speed and duplex mode to decide the path cost. Select “Specific”, if you want to use user-defined value. Valid values are 1 to 200000000. Please note that path cost takes precedence over port priority.

**Priority:** Select port priority.

**Admin Edge:** If an interface is attached to end nodes, you can set it to “Edge”.

**Auto Edge:** Select the checkbox to enable this feature. When enabled, a port is automatically determined to be at the edge of the network when it receives no BPDUs.

**Restricted Role:** If enabled, this causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority.

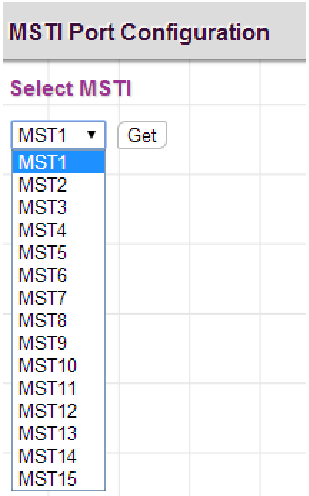
**Restricted TCN:** If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports.

**BPDU Guard:** This feature protects ports from receiving BPDUs. It can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state. If enabled, the port will disable itself upon receiving valid BPDU's.

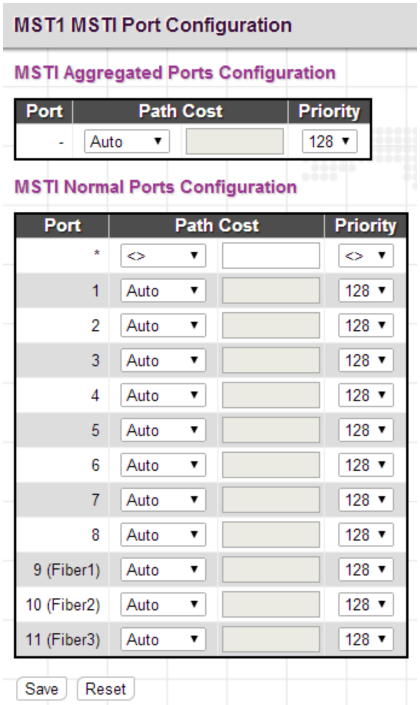
**Point-to-Point:** Select the link type attached to an interface.

> **Auto:** The switch automatically determines whether the interface is attached to a point-to-point link or shared medium.
>
> **Forced True:** It is a point-to-point connection.
>
> **Forced False:** It is a shared medium connection.

### *4.7.3.5 MSTI Ports*




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

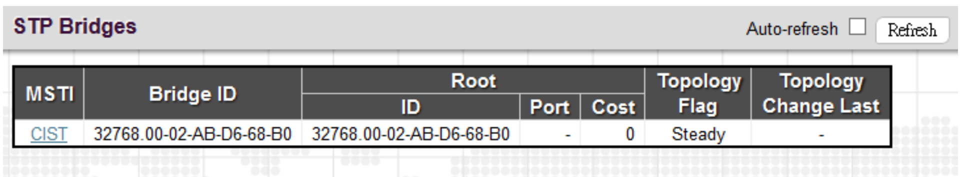



**Port:** The port number.

**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.

### *4.7.3.6 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.

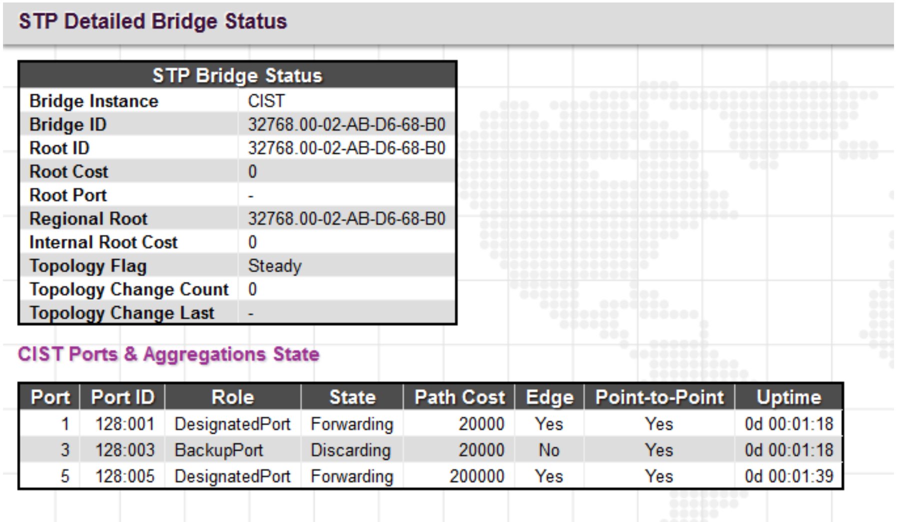
**Root Port:** The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

**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

| STP Bridge Status | |
|---|---|
| Bridge Instance | CIST |
| Bridge ID | 32768.00-02-AB-D6-68-B0 |
| Root ID | 32768.00-02-AB-D6-68-B0 |
| Root Cost | 0 |
| Root Port | - |
| Regional Root | 32768.00-02-AB-D6-68-B0 |
| Internal Root Cost | 0 |
| Topology Flag | Steady |
| Topology Change Count | 0 |
| Topology Change Last | - |

CIST Ports & Aggregations State

| Port | Port ID | Role | State | Path Cost | Edge | Point-to-Point | Uptime |
|---|---|---|---|---|---|---|---|
| 1 | 128:001 | DesignatedPort | Forwarding | 20000 | Yes | Yes | 0d 00:01:18 |
| 3 | 128:003 | BackupPort | Discarding | 20000 | No | Yes | 0d 00:01:18 |
| 5 | 128:005 | DesignatedPort | Forwarding | 200000 | Yes | Yes | 0d 00:01:39 |

***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.

### *4.7.3.7 Port Status*

**STP Port Status**

| Port | CIST Role | CIST State | Uptime |
|---|---|---|---|
| 1 | DesignatedPort | Forwarding | 0d 00:02:34 |
| 2 | Disabled | Discarding | - |
| 3 | BackupPort | Discarding | 0d 00:02:34 |
| 4 | Disabled | Discarding | - |
| 5 | DesignatedPort | Forwarding | 0d 00:02:55 |
| 6 | Disabled | Discarding | - |
| 7 | Disabled | Discarding | - |
| 8 | Disabled | Discarding | - |
| 9 (Fiber1) | Disabled | Discarding | - |
| 10 (Fiber2) | Disabled | Discarding | - |
| 11 (Fiber3) | Disabled | Discarding | - |

**Port:** The port number.

**CIST Role:** The role assigned by Spanning Tree Algorithm. Roles can be “Designated Port”, “Backup Port”, “Root Port” or “Non-STP”.

**CIST State:** Display the current state of a port. The CIST state must be one of the following:

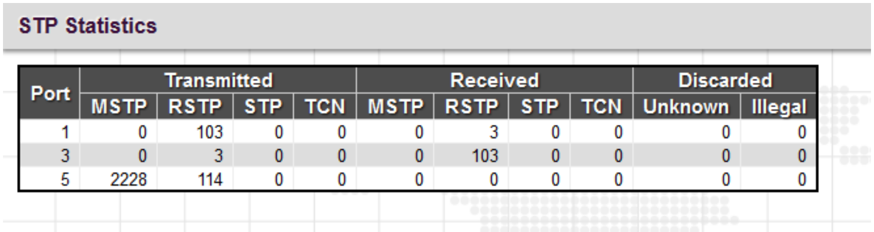
**Discarding:** Ports only receive BPDU messages but do not forward them.

**Learning:** Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses

**Forwarding:** Ports forward packets and continue to learn addresses.

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

### *4.7.3.8 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 |

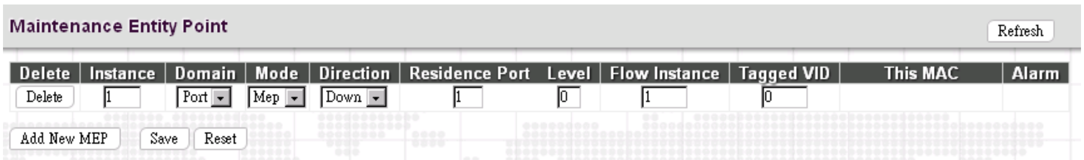
**Port:** Display the port number.

**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.

## *4.7.4 MEP*




**Instance:** Specify the MEP instance ID. After saving an entry, click the number of each instance to further configure details of this MEP entry.

**Domain (Port):** This is a MEP in the Port Domain. 'Flow Instance' is a Port.

**Mode:** Select either Mep (Maintenance Entity End Point) or Mip (Maintenance Entity Intermediate Point).

**Direction:** Select the traffic direction either Down or Up for monitoring on a residence port.

**Down:** This is a Down (Ingress) MEP - monitoring ingress OAM and traffic on 'Residence Port'.

**Up:** This is an Up (Egress) MEP - monitoring egress OAM and traffic on 'Residence Port'.

**Residence Port:** Specify a port to monitor.

**Level:** The MGP level of this MEP.

**Flow Instance:** The MEP related to this flow.

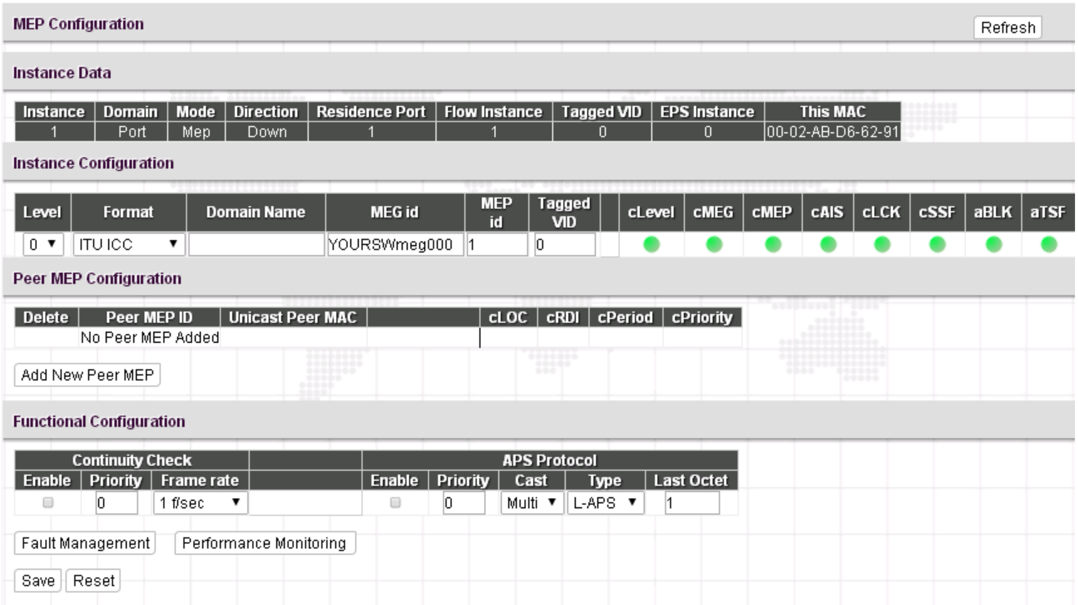
**Tagged VID:** A C-tag or S-tag (depending on VLAN port type) is added with this VID. Entering “0” means no tag will be added.

**This MAC:** The MAC of this MEP (can be used by other MEP when unicast is selected).

**Alarm:** There is an active alarm on the MEP.

Delete: Remove the entry from the table.

Click the instance number to configure detailed settings of MEP.




### *Instance Data*

The details of the current instance item.

### *Instance Configuration*

**Level:** Select a MEP level. The allowed range is 0~7.

**Format:** Two formats are available.

> **ITU ICC:** This is defined by ITU in Y.1731 ANNEX A. “Domain Name” is not used. MEG id must be maximum 13 characters.
>
> **IEEE String:** This is defined by IEEE in 802.1ag. “Domain Name” can be maximum 16 characters. “MEG ID” (Short MA Name) can be maximum 16 characters.
>
> **ITU CC ICC:** This is defined by ITU in Y.1731. “Domain Name” is not used. MEG id must be maximum 15 characters.

**ICC/Domain Name:** Depending on the format selected, enter ITU ICC or IEEE Maintenance Domain Name.

**MEG id:** This is either ITU UMC (MEG ID value [7-13]) or IEEE Short MA Name depending on “Format”.

**MEP id:** This value will become the transmitted two byte CCM MEP ID.

**Tagged VID:** This C-port tag is added to the OAM PDU and is only applicable to port MEP.

***MEP STATE***

**cLevel:** Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.

**cMEG:** Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.

**cMEP:** Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.

**cAIS:** Fault Cause indicating that AIS PDU is received.

**cLCK:** Fault Cause indicating that LCK PDU is received.

**cSSF:** Fault Cause indicating that server layer is indicating Signal Fail.

**aBLK:** The consequent action of blocking service frames in this flow is active.

**aTSF:** The consequent action of indicating Trail Signal Fail to-wards protection is active.

***Peer MEP Configuration***

Click the “Add New Peer MEP” button to create a new entry.

Click the “Delete” button to remove an entry from the table.

**Peer MEP ID:** The peer MEP ID of the target MEP. This is used only when Unicast Peer MAC is all zeros.

**Unicast Peer MAC:** The target switch or device’s unicast MAC address. You can specify unicast MAC address in “xx-xx-xx-xx-xx-xx”, “xx.xx.xx.xx.xx.xx” or “xxxxxxxxxxxx” format where x is a hexadecimal digit.

***NOTE:*** *When “Peer MEP ID” field is configured, the device can auto-negotiate the neighboring device’s MAC address. Therefore, the user can set “Unicast Peer MAC” field to all zeros “00-00-00-00-00-00” for initial configurations.*

**cLOC:** Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP

**cRDI:** Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.

**cPeriod:** Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.

**cPriority:** Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.

***Functional Configuration***

**Continuity Check**

**Enable:** Select the checkbox to enable Continuity Check that CCM PDU is transmitted and received. The CCM PDU is always transmitted as Multicast Class 1.

**Priority:** The priority to be inserted as PCP bits in TAG (if any).

**Frame rate:** Select the transmitting frame rate of CCM PDU.

**APS Protocol**

**Enable:** Select the checkbox to enable APS (Automatic Protection Switching) protocol.

**Priority:** The priority to be inserted as PCP bits in TAG (if any).

**Cast:** Select whether APS PDU transmitted unicast or multicast. The unicast MAC will be taken from the "Unicast Peer MAC" configuration. Unicast is only valid for L-APS type. The R-APS PDU is always transmistted with multicast MAC described in G.8032.

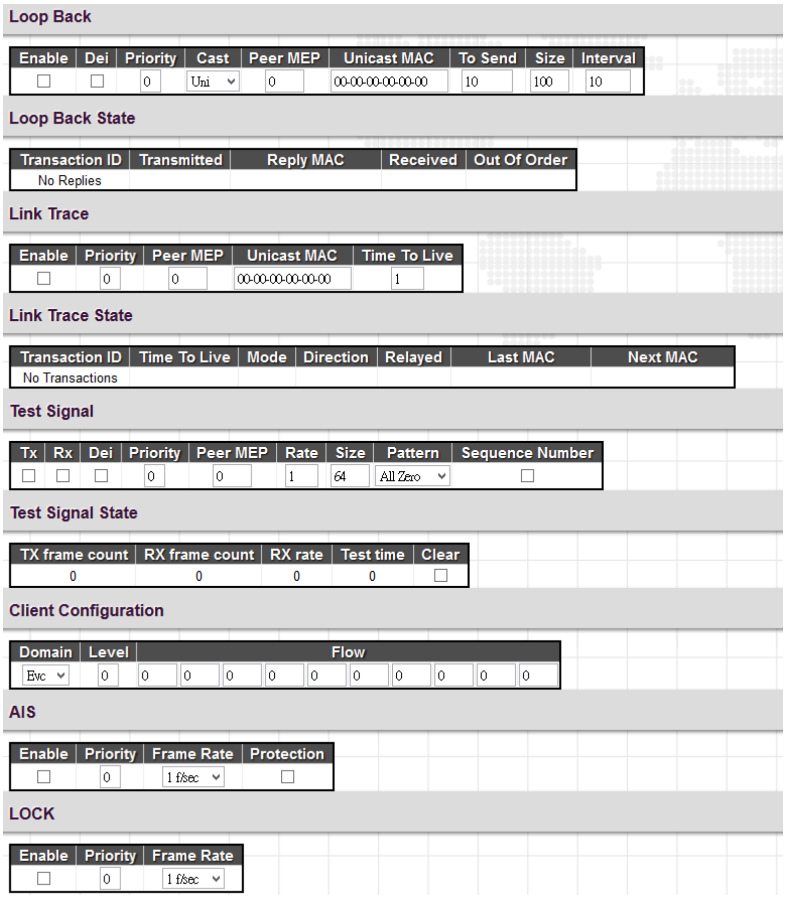
**Type:**

**R-APS:** APS PDU is transmitted as R-APS (this is for ERPS).

**L-APS:** APS PDU is transmitted as L-APS (this is for ELPS).

**Last Octet:** This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

***<u>Click the "Fault Management" button.</u>***




***<u>Loop Back</u>***

**Enable:** Select the checkbox to enable Loop Back based on transmitting and receiving LBM/LBR PDU. Loop Back is automatically disabled when all "To Send" LBM PDU has been transmitted.

**Dei:** The DEI to be inserted as PCP bits in TAG (if any).

**Priority:** The priority to be inserted as PCP bits in TAG (if any).

**Cast:** Select LBM PDU to be transmitted as unicast or multicast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop Back is possible.

**Peer MEP:** This is only used if the "Unicast MAC" is configured to all zero. The LBM unicast MAC will be taken from the "Unicast Peer MAC" configuration of this peer.

**Unicast MAC:** This is only used if NOT configured to all zero. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back to-wards a MIP.

**To Send:** The number of LBM PDU to send in one loop test. The value 0 indicate infinite transmission (test behaviour). This is HW based LBM/LBR and Requires VOE.

**Size:** The number of bytes in the LBM PDU Data Pattern TLV.

**Interval:** The interval between transmitting LBM PDU. In 10ms. in case 'To Send' != 0 (max 100 - '0' is as fast as possible) In 1us. in case 'To Send' == 0 (max 10.000)".

***Loop Back State***

**Transaction ID:** The transaction ID of the first LBM transmitted. For each LBM transmitted the transaction ID in the PDU is incremented.

**Transmitted:** The total number of LBM PDU transmitted.

**Reply MAC:** The MAC of the replying MEP/MIP. In case of multi-cast LBM, replies can be received from all peer MEP in the group. This MAC is not shown in case of "To Send"= 0.

**Received:** The total number of LBR PDU received from this "Reply MAC".

**Out of Order:** The number of LBR PDU received from this "Reply MAC" with incorrect "Transaction ID".

***Link Trace***

**Enable:** Select the checkbox to enable Link Trace based on transmitting and receiving LTM/LTR PDU. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2.

**Priority:** The priority to be inserted as PCP bits in TAG (if any).

**Peer MEP:** This is only used if the "Unicast MAC" is configured to all zero. The Link Trace Target MAC will be taken from the "Unicast Peer MAC" configuration of this peer.

**Unicast MAC:** This is only used if NOT configured to all zero. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC.

**Time To Live:** This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. PDU will not be forwarded when the TTL value reaches zero.

***Link Trace State***

**Transaction ID:** The transaction id is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated.

**Time To Live:** This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded.

**Mode:** This indicates if it was a MEP/MIP sending this LTR.

**Direction:** This indicates if MEP/MIP sending this LTR is ingress or egress.

**Relayed:** This indicates if MEP/MIP sending this LTR has relayed or forwarded the LTM.

**Last MAC:** The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding.

**Next MAC:** The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP.

***<u>Test Signal</u>***

**Tx/Rx:** Enable or disable test signal to send or receive TST PDU.

**Dei:** The DEI to be inserted as PCP bits in TAG (if any).

**Priority:** The priority to be inserted as PCP bits in TAG (if any).

**Peer MEP:** The TST frame destination MAC will be taken from the "Unicast Peer MAC" configuration of this peer.

**Rate:** The TST frame transmission bit rate - in Mega bits pr. second. Limit on Caracal is 400 Mbps. Limit on Serval is 1Gbps.

**Size:** The TST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes).

**Pattern:** The 'empty' TST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern.

**All Zero:** Pattern will be 00000000

**All One:** Pattern will be 11111111

**10101010:** Pattern will be 10101010

**Sequence Number:** Enable the sequence number feature.

***<u>Test Signal State</u>***

**TX frame count:** The number of transmitted TST frames since last 'Clear'.

**RX frame count:** The number of received TST frames since last 'Clear'.

**RX rate:** The current received TST frame bit rate in 100 Kbps. This is calculated on a 1 s. basis, starting when first TST frame is received after 'Clear'. The frame size used for this calculation is the first received after 'Clear'

**Test time:** The number of seconds passed since first TST frame received after last 'Clear'.

**Clear:** This will clear all Test Signal State. Transmission of TST frame will be restarted. Calculation of 'Rx frame count', 'RX rate' and 'Test time' will be started when receiving first TST frame.

***Client Configuration***

**Domain:** The domain of the client layer. It must be EVC.

**Level:** The client layer level which means that PDU transmitted in client layer flows will be on this level.

**Flow:** Client layer flow instance numbers. It must only be configured in case of Port MEP.

***AIS***

**Enable:** Enable or disable the insertion of AIS signal (AIS PDU transmission) in client layer flows.

**Priority:** On Caracal this priority is used in sink direction (client layer). On Serval, for each client EVC, the highest COS-ID (ECE Class) is used.

**Frame Rate:** Select the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731.

**Protection:** Select the checkbox to enable protection. This means that the first 3 AIS PDU is transmitted as fast as possible - in case of using this for protection in the end point.

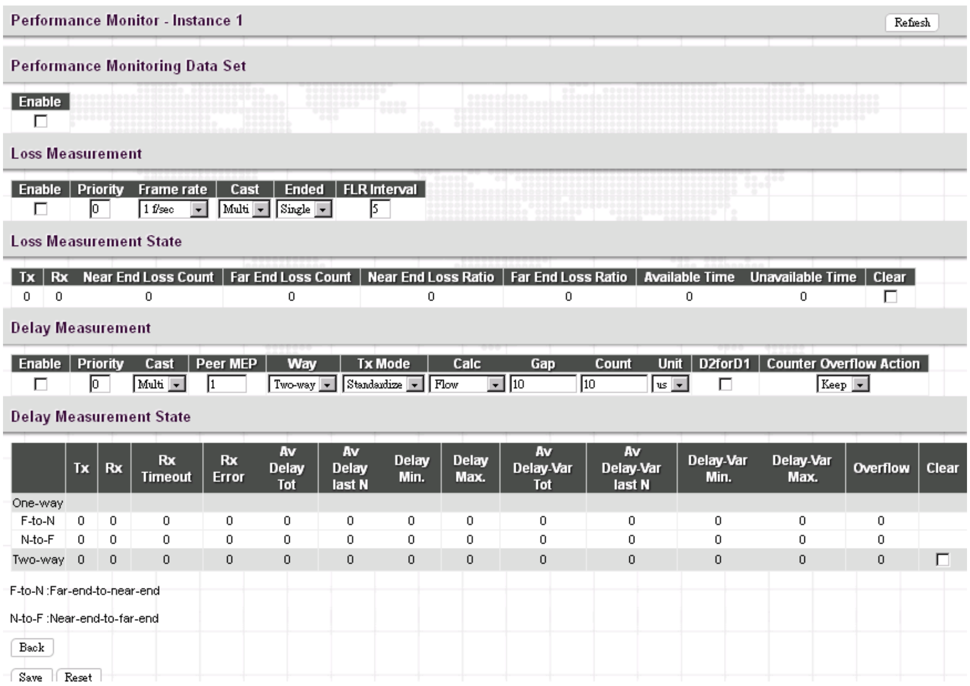
***Lock***

**Enable:** Enable or disable the insertion of LOCK signal (LCK PDU transmission) in client layer flows.

**Priority:** The priority to be inserted in MEP source direction. On Caracal, this priority is also used in sink direction (client layer). On Serval, for each client EVC, the highest COS-ID (ECE Class) is used.

**Frame Rate:** Select the frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.

**Click the "Performance Monitoring" button.**



**Enable:** When enabled, this MEP instance will contribute to the 'PM Data Set' gathered by the PM Session.

***Loss Measurement***

**Enable:** Loss Measurement based on transmitting/receiving CCM or LMM/LMR PDU can be enabled/disabled - see 'Ended'. This is only valid with one Peer MEP configured.

**Priority:** The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

**Frame rate:** Select the frame rate of CCM/LMM PDU. This is the inverse of transmission period as described in Y.1731. Selecting 300f/sec or 100f/sec is not valid. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

**Cast:** Selection of CCM or LMM PDU transmitted unicast or multicast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. In case of enable of Continuity Check and dual ended Loss Measurement both implemented on SW based CCM, 'Cast' has to be the same.

**Ended:**

**Single:** Single ended Loss Measurement implemented on LMM/LMR.

**Dual:** Dual ended Loss Measurement implemented on SW based CCM.

**FLR Interval:** This is the interval in seconds where the Frame Loss Ratio is calculated.

***Loss Measurement State***

**Near End Loss Count:** The accumulated near end frame loss count - since last 'clear'.

**Far End Loss Count:** The accumulated far end frame loss count - since last 'clear'.

**Near End Loss Ratio:** The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.

**Far End Loss Ratio:** The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.

**Clear:** Set of this check and save will clear the accumulated counters and restart ratio calculation.

***Delay Measurement***

**Enable:** Select the checkbox to enable Delay Measurement based on transmitting 1DM/DMM PDU. Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled.

**Priority:** The priority to be inserted as PCP bits in TAG (if any).

**Cast:** Selection of 1DM/DMM PDU transmitted unicast or multicast. The unicast MAC will be configured through 'Peer MEP'.

**Peer MEP:** This is only used if the 'Cast' is configured to Uni. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

**Way:** One-Way or Two-Way Delay Measurement implemented on 1DM or DMM/DMR, respectively.

**Tx Mode:**

**Standardize:** Y.1731 standardize way to transmit 1DM/DMR.

**Proprietary:** The proprietary way with follow-up packets to transmit 1DM/DMR.

**Calc:** This is only used if the 'Way' is configured to Two-way.

**Round trip:** The frame delay calculated by the transmitting and receiving timestamps of initiators. Frame Delay = RxTimeb-TxTimeStampf

**Flow:** The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay = (RxTimeb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf)

**Gap:** The gap between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535.

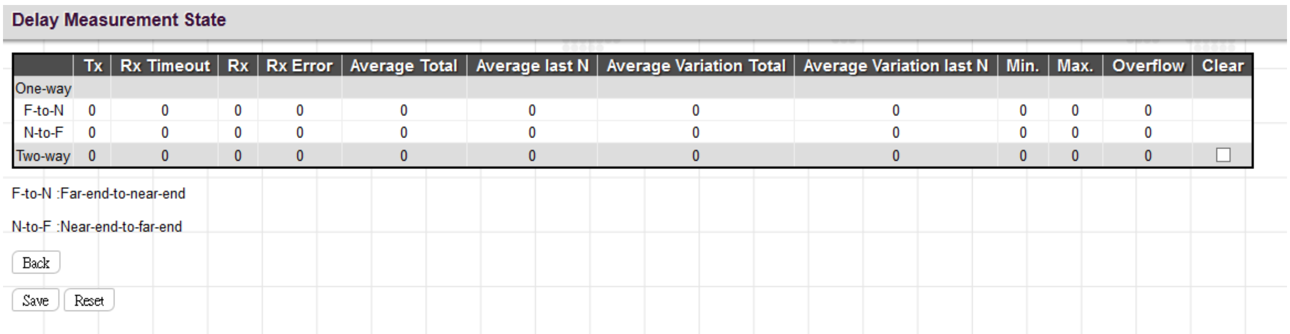
**Count:** The number of last records to calculate. The range is 10 to 2000.

**Unit:** The time resolution.

**D2forD1:** Enable to use DMM/DMR packet to calculate one-way DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both near-end-to-far-end and far-end-to-near-end one-way delay are calculated. When DMM or 1DM is received, only far-end-to-near-end one-way delay is calculated.

**Counter Overflow Action:** The action to counter when overflow happens.

***Delay Measurement State***



Delay Measurement State

| | Tx | Rx Timeout | Rx | Rx Error | Average Total | Average last N | Average Variation Total | Average Variation last N | Min. | Max. | Overflow | Clear |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| One-way | | | | | | | | | | | | |
| F-to-N | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| N-to-F | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Two-way | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ☐ |

F-to-N :Far-end-to-near-end

N-to-F :Near-end-to-far-end

Back

Save Reset

**Tx:** The accumulated transmit count - since last 'clear'.

**Rx Timeout:** The accumulated receive timeout count for two-way only - since last 'clear'.

**Rx:** The accumulated receive count - since last 'clear'.

**Rx Error:** The accumulated receive error count - since last 'clear'. The frame delay is larger than 1 second (timeout).

**Average Total:** The average delay - since last 'clear'. The unit is microsecond.

**Average last N:** The average delay of the last n packets - since last 'clear'. The unit is microsecond.

**Average Variation Total:** The average delay variation - since last 'clear'. The unit is microsecond.

**Average Variation last N:** The average delay variation of the last n packets - since last 'clear'. The unit is microsecond.

**Min.:** The minimum delay - since last 'clear'. The unit is microsecond.

**Max.:** The maximum delay - since last 'clear'. The unit is microsecond.

**Overflow:** The number of counter overflow - since last 'clear'.

**Clear:** Click the checkbox and save this setting will clear the accumulated counters.

### *4.7.5 ERPS*

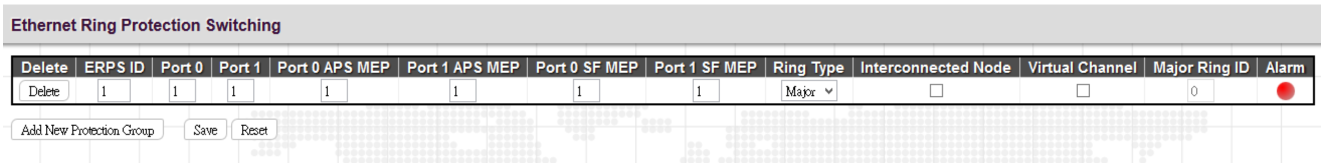
Ethernet Ring Protection Switching (ERPS), defined in ITU-T G8032, implements protection switching mechanism for Ethernet traffic in a ring topology. By performing ERPS function, potential loops in a network can be avoided by blocking traffic to flow to ring protection link (RPL) so as to protect the entire Ethernet ring.

In a ring topology that runs ERPS, only one switch is assigned as an owner that is responsible for blocking traffic in RPL so as to avoid loops. The switch adjacent to the RPL owner is called RPL neighbor node that is responsible for blocking its end of the RPL under normal condition. Other participating switches adjacent to RPL owner or neighbor in a ring are members or RPL next-neighbor nodes to this topology and normally forward receive traffic.

Nodes on the ring periodically use control messages called Ring Automatic Protection Switching message to ensure that a ring is up and loop-free. Once RPL owner misses poll packets or learns from fault detection packets, RPL owner detects signal failure (SF) in a ring. Upon learning of a fault, the RPL owner unblocks ring protection link (RPL) allowing protected VLAN traffic through.

ERPS, like STP, provides a loop-free network by using polling packets to detect faults. However, when a fault occurs, ERPS heals itself by sending traffic over a protected reverse path instead of making a calculation to find out the forwarding path. Because of this fault detection mechanism, ERPS can converge in less than 50 milliseconds and recover quickly to forward traffic.

The following sections will provide a reference to ERPS web configurations. For an actual setting example, please refer to Appendix B: G.8032 ERPS Configuration Procedure guide.




**ERPS ID:** Specify an ID for this group.

**Port 0:** Port 0 is also known as E port (East port) which is used by some of the other vendors. Specify the east port of the switch in the ring.

**Port 1:** Port 1 is also known as W port (West port) which is used by some of the other vendors. When this port is interconnected with the other sub-ring, "0" is used in this field to indicate that no west port is associated with this instance. Specify the west port of the switch in the ring.

**Port 0 APS MEP:** Specify the East APS PDU handling MEP.

**Port 1 APS MEP:** Specify the West APS PDU handling MEP. When interconnected with the other sub-ring, "0" is used in this field to indicate that no west APS MEP is associated with this instance.

**Port 0 SF MEP:** This is also known as East Signal Fail APS MEP. Assign the East Signal Fail reporting MEP in this field.

**Port 1 SF MEP:** This is also known as West Signal Fail APS MEP. When interconnected with the other sub-ring, “0” is used in this field to indicate that no west SF MEP is associated with this instance. Assign the West Signal Fail reporting MEP in this field.

**Ring Type:** Select the type of protection ring which can be either “major” ring or “sub” ring.

**Interconnected Node:** Select the checkbox to indicate that this is an interconnected node for this instance. Leave this checkbox unchecked if the configured instance is not interconnected.

**Virtual Channel:** Sub rings can either have virtual channel or not on the interconnected node. Select the checkbox if this instance is an interconnected node with virtual channel. Leave this checkbox unchecked if sub ring does not have virtual channel.

**Major Ring ID:** This field is used for an interconnected sub ring for sending topology change updates on major ring. If ring is set to major, this value is same as the protection group ID of this ring.

**Alarm:** When settings are complete, then the switch will show an alarm status on the ERPS.

Click the “Add New Protection Group” button to create a new entry.

Click the “Delete” button to remove a new entry.

Click “Save” to save changes.

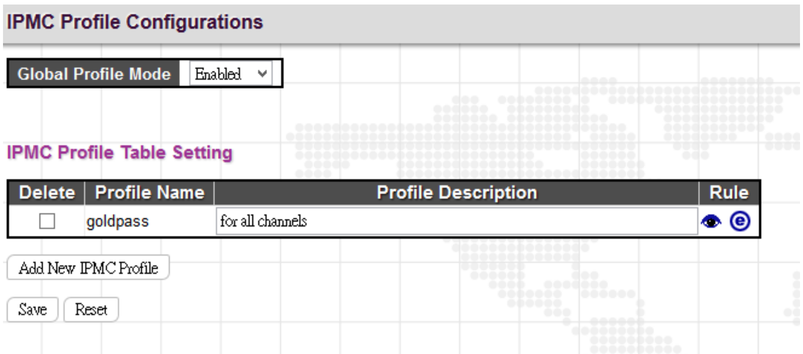
Click “Reset” to undo any changes made locally and restore changes to previously saved (default) values.

Click “Refresh” to manually refresh ERPS information.

## 4.8 IPMC Profile

The "IPMC Profile" includes the following two sub menus.


### *4.8.1 Profile Table*




***IPMC Profile Configuration***

**Global Profile Mode:** Enable or disable IPMC Profile feature globally.

***IPMC Profile Table Setting***

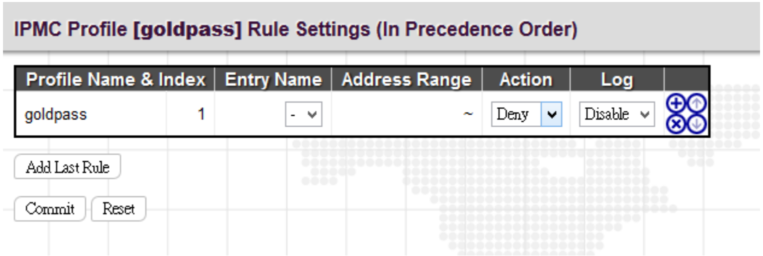
**Profile Name:** Enter a name for this profile.

**Profile Description:** Enter a brief description for this profile.

Click the "Add New IPMC Profile" to insert a new entry to the table.

Select the "Delete" checkbox to delete an entry.

Click the "e" button to edit this profile's detailed settings.




**Profile Name & Index:** Display the profile name and index.

**Entry Name:** The name used in specifying the address range. Only the existing profile address entries are selectable in the drop-down menu.

**Address Range:** Specify the multicast IP range. The available IP range is from 224.0.0.0~239.255.255.255

**Action:** Select the action taken upon receiving the Join/Report frame that has the group address matches the address range of the rule.

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

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

**Log:** Select the logging preference receiving the Join/Report frame that has the group address matches the address range of the rule.

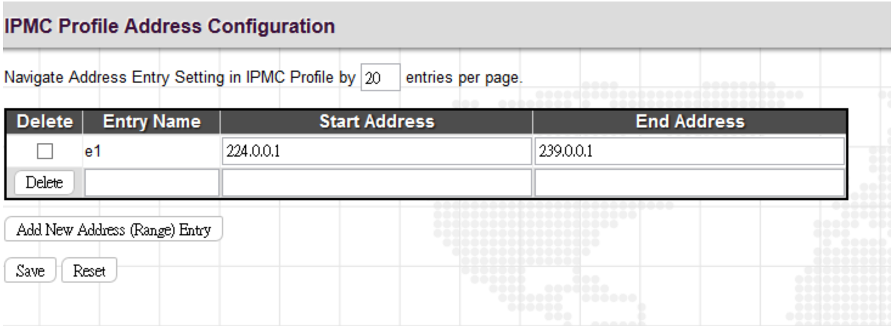
**Enable:** Corresponding information of the group address, that matches the range specified in the rule, will be logged.

**Disable:** Corresponding information of the group address, that matches the range specified in the rule, will not be logged.

You can manage rules and the corresponding precedence order by using the following buttons:

⊕: Insert a new rule before the current entry of rule.
⊗: Delete the current entry of rule.
↑: Moves the current entry of rule up in the list.
↓: Moves the current entry of rule down in the list.

### *4.8.2 Address Entry*




**Entry Name:** Enter a name which is used for indexing the address entry table.

**Start Address:** Enter the starting IPv4 or IPv6 multicast address used in this address range.

**End Address:** Enter the ending IPv4 or IPv6 multicast address used in this address range.

Click the "Add new Address (Range) Entry" button to insert a new entry.

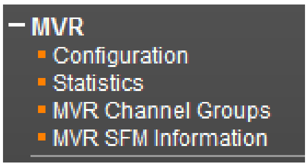
Select the "Delete" checkbox to delete an entry during the next save.

## 4.9 MVR

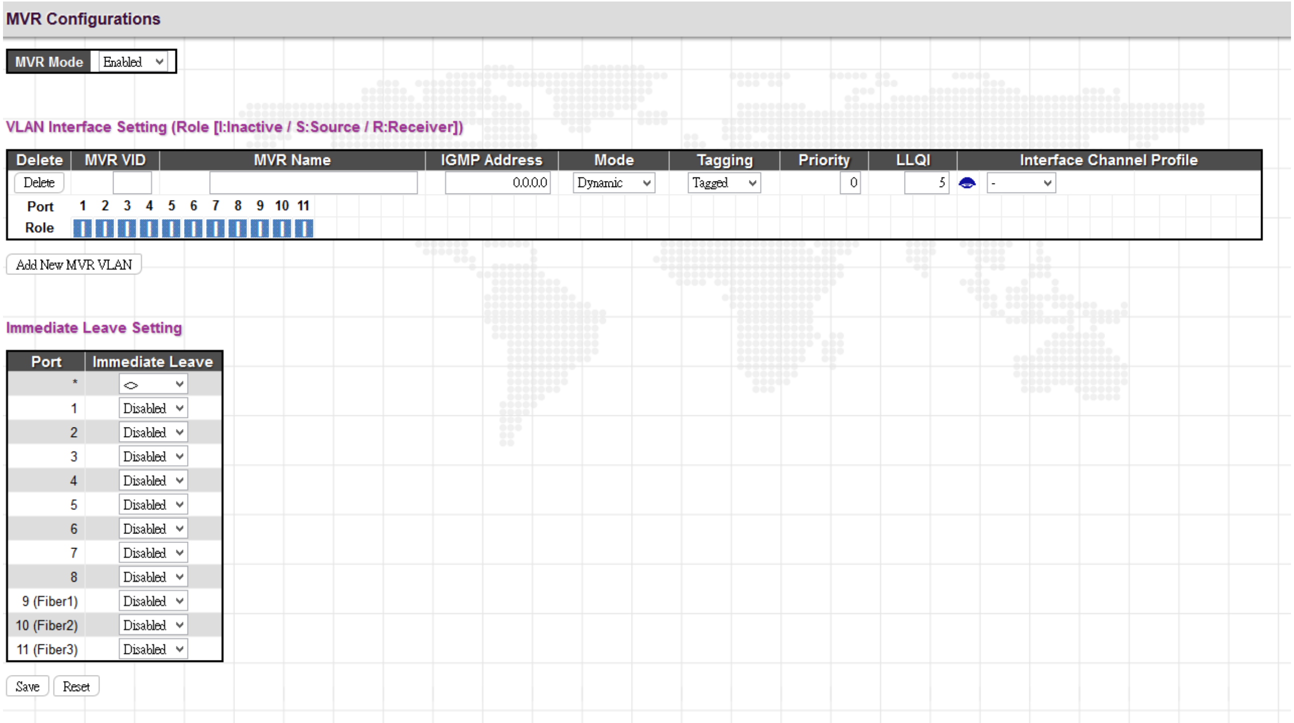
Multicast VLAN Registration protocol (MVR) allows a media server to transmit multicast stream in a single multicast VLAN when clients receiving multicast VLAN stream can reside in different VLANs. Clients in different VLANs intend to join or leave the multicast group simply by sending the IGMP Join or Leave message to a receiver port. The receiver port that belongs to one of the multicast groups can receive multicast stream from the media server.

MVR further isolates users who are not intended to receive multicast traffic and hence provide data security by VLAN segregation that allows only multicast traffic into other VLANs to which the subscribers belong. Even though common multicast streams are passed onto different VLAN groups from the MVR VLAN, users in different IEEE 802.1Q or private VLANs cannot exchange any information (except through upper-level routing services).

The “MVR” menu contains the following sub menus.



### 4.9.1 Configuration




***<u>MVR  Configurations</u>***

**MVR Mode:** Enable or disable MVR feature globally on this device.  Any multicast data from source ports will be sent to associated receiver ports registered in the table. By default, MVR feature is turned off.

***<u>VLAN Interface Setting</u>***

**MVR ID:** Specify multicast VLAN ID. Please note that MVR source ports are not recommended to be used as management VLAN ports. MVR source ports should be configured as members of the MVR VLAN, but MVR receiver ports should not be manually configured as members of this VLAN.

**MVR Name:** Optionally specify a user-defined name for this multicast VLAN. The maximum length of the MVR name string is 32. Both alphabets and numbers are allowed for use.

**IGMP Address:** Specify the IPv4 unicast address as source address used in IP header for IGMP control frames.

**Mode:**  Two MVR operation modes are provided.

**Dynamic:** MVR allows dynamic MVR membership reports on source ports. (This is the default mode.)

**Compatible:** MVR membership reports are forbidden on source ports.

**Tagging:** Specify whether IGMP/MLD control frames will be sent tagged with MVR VID or untagged.

**Priority:** Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0 -7.

**LLQI:** LLQI stands for Last Listener Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. By default, LLQI is set to 5 tenths of a second (0.5 second). The allowed range is 0~31744 tenths of a second.

**Interface Channel Profile:** Select an IPMC profile from the drop-down menu. Click the button to view a summary about the selected IPMC profile settings.

**Port Role:** Click the Port Role symbol to change the role status.

**Inactive (I):** By default, all ports are set to inactive. Inactive ports do not participate in MVR operations.

**Source (S):** Set a port (uplink ports) to source port. Source ports will receive and send multicast data. Subscribers can not directly be connected to source ports. Please also note that source ports cannot be management ports at the same time.

**Receiver (R):** Set a port to receiver port. Client or subscriber ports are configured to receiver ports so that they can issue IGMP/MLD messages to receive multicast data.

***<u>Immediate Leave Setting</u>***

**Port:** The port number. "Port *" rule applies to all ports.

**Immediate Leave:** Enable for disable immediate leave function. When enabled, the device immediately removes a port from a multicast stream as soon as it receives leave message for that group. This option only applies to an interface configured as MVR receivers.

### *4.9.2 MVR Statistics*

**MVR Statistics**

| VLAN ID | IGMP/MLD Queries Received | IGMP/MLD Queries Transmitted | IGMPv1 Joins Received | IGMPv2/MLDv1 Reports Received | IGMPv3/MLDv2 Reports Received | IGMPv2/MLDv1 Leaves Received |
|---|---|---|---|---|---|---|
| 200 | 0 / 0 | 0 / 0 | 0 | 0 / 0 | 0 / 0 | 0 / 0 |

This page displays MVR statistics information on queries, joins, reports and leaves messages.

**VLAN ID:** Display VLAN ID that is used for processing multicast traffic.

**IGMP/MLD Queries Received:** The number of received queries for IGMP and MLD.

**IGMP/MLD Queries Transmitted:** The number of transmitted queries for IGMP/MLD.

**IGMPv1 Joins Received:** The number of IGMPv1 received joins

**IGMPv2/MLDv1 Reports Received:** The number of IGMPv2 and MLDv1 received reports.

**IGMPv3/MLDv2 Reports Received:** The number of IGMPv3 and MLDv2 received reports.

**IGMPv2/MLDv1 Leaves Received:** The number of IGMPv2 and MLDv1 received leaves.

### *4.9.3 MVR Channel Groups*

**MVR Channels (Groups) Information**

Start from VLAN 1 and Group Address :: with 20 entries per page.

| VLAN ID | Groups | Port Members | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 (Fiber1) | 10 (Fiber2) | 11 (Fiber3) |
| *No more entries* | | | | | | | | | | | | |

Start from VLAN ____ and Group Address ________ with 20 entries per page.

This table displays MVR channels (groups) information and is sorted by VLAN ID.

**VLAN ID:** VLAN ID of the group.

**Groups:** Group ID

**Port Members:** Ports that belong to this group.

### *4.9.4 MVR SFM Information*

**MVR SFM Information**

Start from VLAN 1 and Group Address :: with 20 entries per page.

| VLAN ID | Group | Port | Mode | Source Address | Type | Hardware Filter/Switch |
|---|---|---|---|---|---|---|
| *No more entries* | | | | | | |

**VLAN ID:** VLAN ID of the group.

**Group:** The group address.

**Port:** Switch port number.

**Mode:** Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

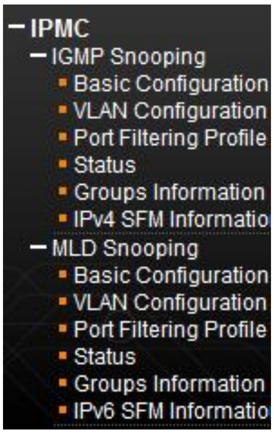
**Source Address:** The source IP Address. Currently, the system limits the total number of source IP addresses for filtering to be 128. When there is no source filtering address, "None" is shown in the Source Address field.

**Type:** Indicates the Type. It can be either Allow or Deny.

**Hardware Filter/Switch:** Indicate whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

## 4.10 IPMC

The "IPMC" menu includes IGMP Snooping and MLD Snooping sub menu. Select the appropriate menu to set up detailed configurations.




### *4.10.1 IGMP Snooping*

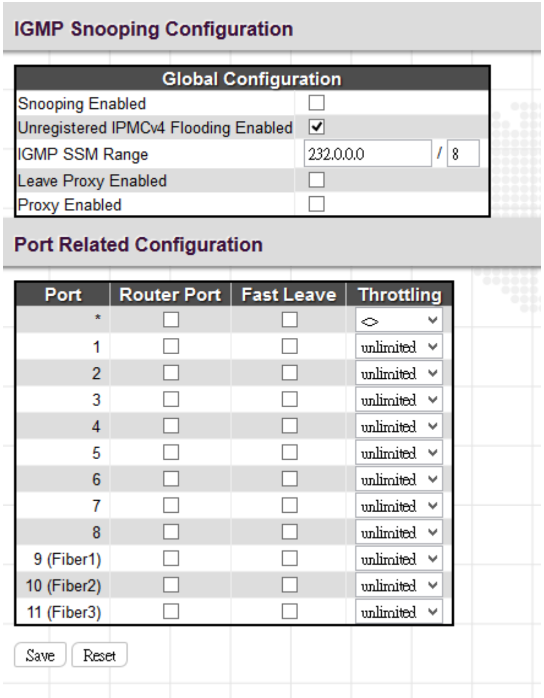
The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It can be used more efficiently when supporting activities, such as, online streaming video and gaming.

IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers by processing the layer 3 packets that IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch, it analyses all the IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch receives an IGMP report for a given multicast group from a host, the switch adds the host's port number to the multicast list for that group. When the switch hears an IGMP Leave, it removes the host's port from the table entry.

IGMP snooping can reduce multicast traffic from streaming and other bandwidth intensive IP applications more effectively. A switch using IGMP snooping will only forward multicast traffic to the hosts in that traffic. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also decreases the workload at the end hosts since their network cards (or operating system) will not receive and filter all the multicast traffic generated in the network.

### *4.10.1.1 Basic Configuration*




***IGMP Snooping Configuration: Global Configuration***

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

**Unregistered IPMCv4 Flooding Enabled:** Set forwarding mode for unregistered (not-joined) IP multicast traffic. Select the checkbox to flood traffic.

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

**Leave Proxy Enabled:** Suppresses leave messages unless received from the last member port in the group. IGMP leave proxy suppresses all unnecessary IGMP leave messages so that a non-querier switch forwards an IGMP leave packet only when the last dynamic member port leaves a multicast group.

**Proxy Enabled:** When enabled, the switch performs like "IGMP Snooping with Proxy Reporting" (as defined in DSL Forum TR-101, April 2006).

***Port Related Configuration***

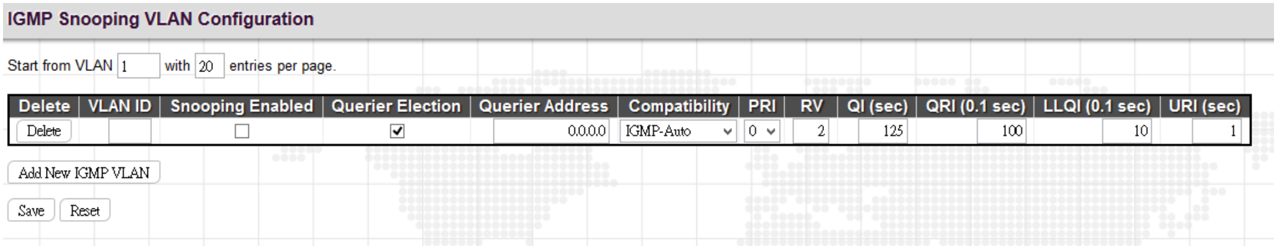
**Port:** The port number.

**Router Port:** Tick the checkbox on a given port to assign it as a router port. If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

**Fast Leave:** Enable fast leave function if the checkbox is ticked. When a leave packet is received, the switch immediately removes it from a multicast service without sending an IGMP group-specific (GS) query to that interface.

**Throttling:** This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new IGMP join reports will be dropped. By default, unlimited is selected. Other allowed options are 1~10

### *4.10.1.2 VLAN Configuration*




This page is used to configure IGMP Snooping for an interface.

Click the “Add New IGMP VLAN” button to add a new entry.

**VLAN ID:** Specify VLAN ID for IGMP snooping.

**Snooping Enabled:** Select the checkbox to enable snooping feature on an interface basis. When enabled, the switch will monitor network traffic on the specified interface to determine which hosts want to receive multicast services. If IGMP snooping is enabled globally and an interface’s IGMP snooping is enabled on an interface, IGMP snooping on an interface will take precedence. When disabled, snooping can still be configured on an interface. However, settings will only take effect until IGMP snooping is enabled globally.

**Querier Election:** Enable to join querier election in the VLAN. When disabled, it will act as an IGMP non-querier.

**Querier Address:** Specify the IPv4 unicast source address used in IP header for IGMP querier election. When the field is not specified, the switch uses the first available IPv4 management address of the IP interface associated with this VLAN.

**Compatibility:** This configures how hosts and routers take actions within a network depending on IGMP version selected. Available options are “IGMP-Auto”, “Forced IGMPv1”, “Forced IGMPv2”, “Forced IGMPv3”. By default, IGMP-Auto is used.

**PRI:** Select the priority of interface. This field indicates the IGMP control frame priority level generated by the system which is used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest). By default, interface priority value is set to 0.

**RV:** The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

**QI (sec):** The Query Interval is the interval between IGMP General Query messages sent by the Querier. The default Querier Interval is 125 seconds.

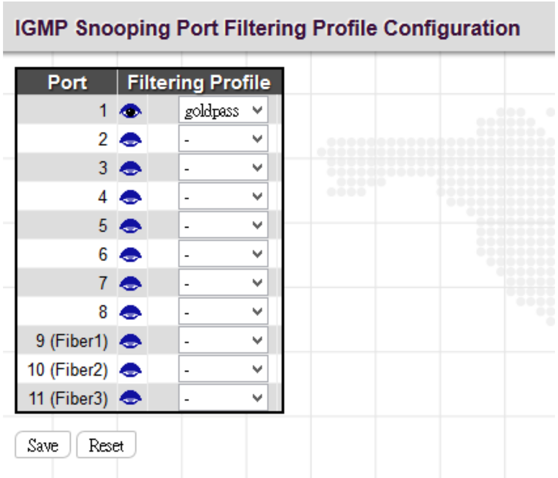
**QRI:** The Query Response Interval is the maximum amount of time that the IGMP router waits to receive a response to a General Query message. The QRI applies when the switch is acting as the querier and is used to inform other devices of the maximum time this system waits for a response to general queries. By default, RQI is set to 10 seconds. The allowed range is 0~31744 tenths of a second.

**LLQI:** The Last Listener Query Interval sets the interval that waits for a response to a group-specific or group-and-source specific query message.

**URI:** The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. By default, URI is set to 1 second. The allowed range for URI is 0 -31744 seconds.

### 4.10.1.3 Port Filtering Profile

The Port Filtering Configuration page is to filter specific multicast traffic on a per port basis. Before you select a filtering profile for filtering purposes, you must set up profiles in IPMC Profile page.

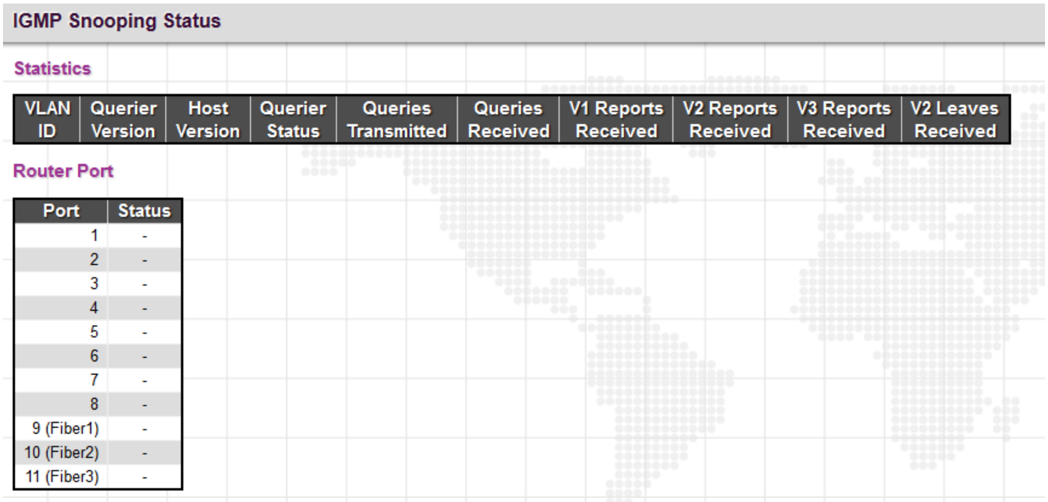



**Port:** The port number.

**Filtering Profile:** Select the configured multicast groups that are denied on a port. When a certain multicast group is selected on a port, IGMP join reports received on a port are dropped.

: Click the summary button to view details of the selected IPMC profile.

### 4.10.1.4 Status




***Statistics***

**VLAN ID:** The VLAN ID of this entry.

**Querier Version:** The current working Querier version.

**Host Version:** The current host version.

**Querier Status:** Show the Querier status that is either "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

**Queries Transmitted:** The number of queries transmitted.

**Queries Received:** The number of queries received.

**V1 Reports Received:** The number of Received V1 Reports.

**V2 Reports Received:** The number of Received V2 Reports.

**V3 Reports Received:** The number of Received V3 Reports.

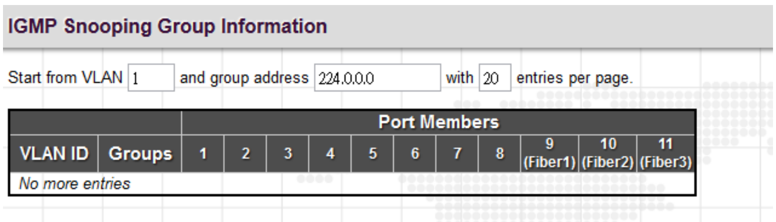
**V2 Leaves Received:** The number of Received V2 Leaves.

***Router Port***

**Port:** The port number.

**Status:** Indicate whether a specific port is a router port or not.

### *4.10.1.5 Groups Information*



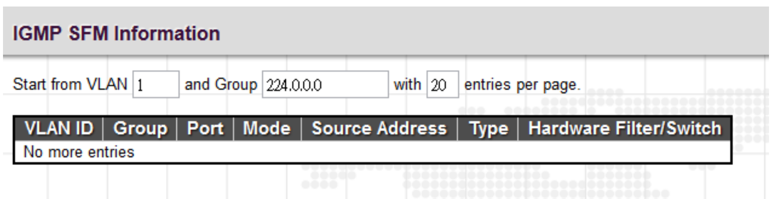

**VLAN ID:** Display the VLAN ID of the group.

**Groups:** Display the group address.

**Port Members:** Ports that belong to this group.

***NOTE:*** *The maximum number of IGMP Snooping groups can be learned is 32.*

### *4.10.1.6 IPv4 SFM Information*



**VLAN ID:** Display the VLAN ID of the group.

**Groups:** Display the IP address of a multicast group.

**Port:** The switch port number.

**Mode:** The filtering mode maintained per VLAN ID, port number and group address.

**Source Address:** The source IP address available for filtering.

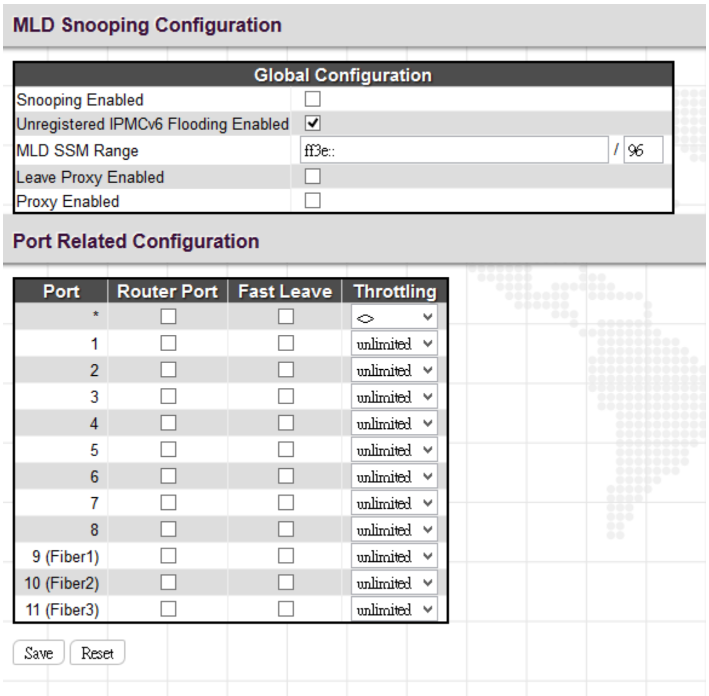
**Type:** Display either Allow or Deny type.

**Hardware Filter/Switch:** Indicates whether the data plane destined to the specific group address from the source IPv4 address can be handled by the chip or not.

## *4.10.2 MLD Snooping*

Multicast Listener Discovery (MLD) snooping, similar to IGMP snooping for IPv4, operates on IPv6 for multicast traffic. In other words, MLD snooping configures ports to limit or control IPv6 multicast traffic so that multicast traffic is forwarded to ports (or users) who want to receive it. In this way, MLD snooping can reduce the flooding of IPV6 multicast packets in the specified VLANs. Please note that IGMP Snooping and MLD Snooping are independent of each other. They can both be enabled and function at the same time.

### *4.10.2.1 Basic Configuration*




***<u>Global Configuration</u>***

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

**Unregistered IPMCv6 Flooding Enabled:** Set forwarding mode for unregistered (not-joined) IP multicast traffic. Select the checkbox to flood traffic.

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

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

**Proxy Enabled:** When MLD proxy is enabled, the switch exchanges MLD messages with the router on its upstream interface, and performs the host portion of the MLD task on the upstream interface as follows:

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

***Port Related Configuration***

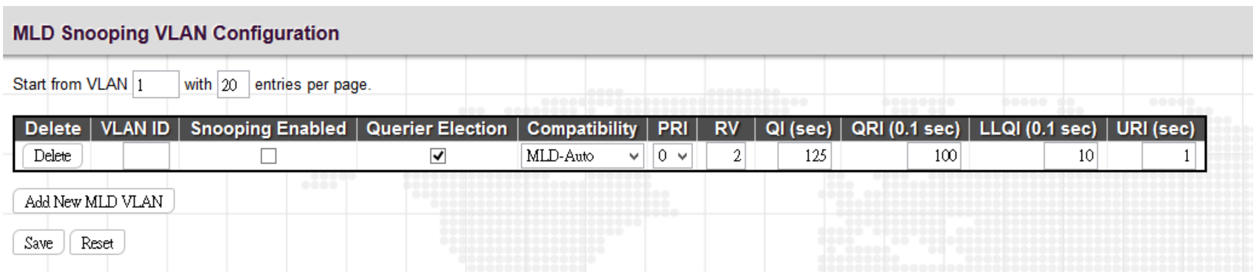
**Port:** The port number.

**Router Port:** Tick the checkbox on a given port to assign it as a router port. If MLD snooping cannot locate the MLD querier, you can manually designate a port which is connected to a known MLD querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

**Fast Leave:** Enable fast leave function if the checkbox is ticked. When a leave packet is received, the switch immediately removes it from a multicast service without sending a MLD group-specific (GS) query to that interface.

**Throttling:** This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new MLD join reports will be dropped. By default, unlimited is selected. Other allowed options are 1~10.

### *4.10.2.2 VLAN Configuration*




This page is used to configure MLD Snooping for an interface.

**VLAN ID:** Specify VLAN ID for MLD snooping.

**Snooping Enabled:** Select the checkbox to enable snooping feature on an interface basis. When enabled, the switch will monitor network traffic on the specified interface to determine which hosts want to receive multicast services.

**Querier Election:** Enable to join querier election in the VLAN. When enabled, the switch can serve as the MLDv2 querier in the bidding process with other competing multicast routers or switches. Once it becomes querier, it will be responsible for asking hosts periodically if they want to receive multicast traffic. When disabled, it will act as an IGMP non-querier.

**Compatibility:** This configures how hosts and routers take actions within a network depending on MLD version selected. Available options are “MLD-Auto”, “Forced MLDv1”and “Forced MLDv2”. By default, MLD-Auto is used.

**PRI:** Select the priority of interface. This field indicates the MLD control frame priority level generated by the system which is used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest). By default, interface priority value is set to 0.

**RV:** The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2. The allowed range is 1~255.

**QI (sec):** The Query Interval is the interval between IGMP General Query messages sent by the Querier. The default Querier Interval is 125 seconds. The allowed interval range is 1~31744 seconds.

**QRI:** The Query Response Interval is the maximum amount of time that the IGMP router waits to receive a response to a General Query message. The QRI applies when the switch is acting as the querier and is used to inform other devices of the maximum time this system waits for a response to general queries. By default, RQI is set to 10 seconds. The allowed range is 0~31744 tenths of a second.

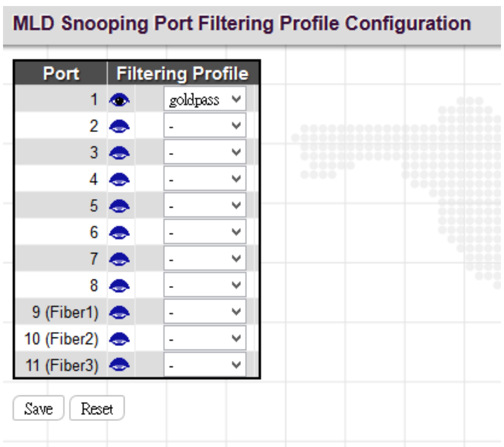
**LLQI:** The Last Listener Query Interval sets the interval that waits for a response to a group-specific or group-and-source specific query message.

**URI:** The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. By default, URI is set to 1 second. The allowed range for URI is 0~31744 seconds.

Click the “Add New MLD VLAN” button to add a new entry.

#### 4.10.2.3 Port Filtering Profile

The Port Filtering Configuration page is to filter specific multicast traffic on a per port basis. Before you select a filtering profile for filtering purposes, you must set up profiles in IPMC Profile page.

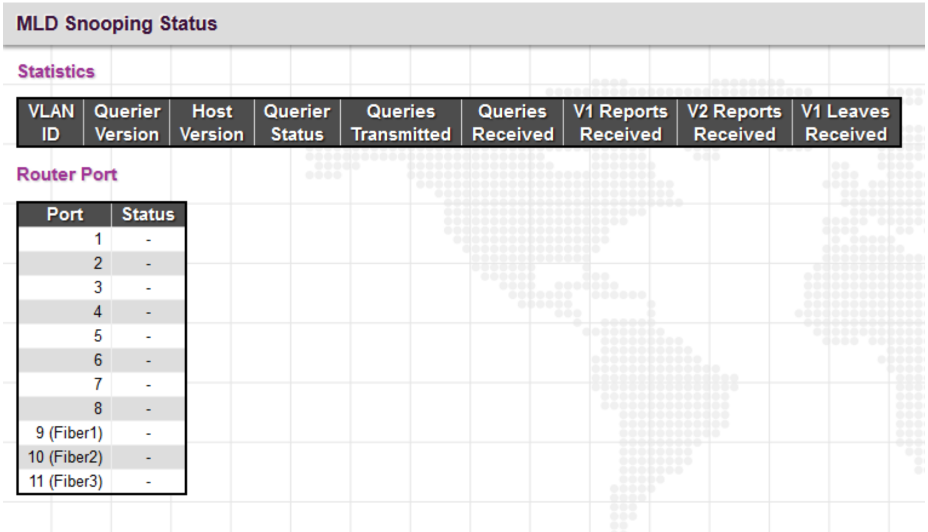



**Port:** List the number of each port.

**Filtering Profile:** Select the configured multicast groups that are denied on a port. When a certain multicast group is selected on a port, MLD join reports received on a port are dropped.

: Click the summary button to view details of the selected IPMC profile.

### *4.10.2.4 Status*



**MLD Snooping Status**

**Statistics**

| VLAN ID | Querier Version | Host Version | Querier Status | Queries Transmitted | Queries Received | V1 Reports Received | V2 Reports Received | V1 Leaves Received |
|---|---|---|---|---|---|---|---|---|

**Router Port**

| Port | Status |
|---|---|
| 1 | - |
| 2 | - |
| 3 | - |
| 4 | - |
| 5 | - |
| 6 | - |
| 7 | - |
| 8 | - |
| 9 (Fiber1) | - |
| 10 (Fiber2) | - |
| 11 (Fiber3) | - |

***<u>Statistics</u>***

**VLAN ID:** The VLAN ID of this entry.

**Querier Version:** The current working Querier version.

**Host Version:** The current host version.

**Querier Status:** Show the Querier status that is either "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

**Queries Transmitted:** The number of queries transmitted.

**Queries Received:** The number of queries received.

**V1 Reports Received:** The number of Received V1 Reports.

**V2 Reports Received:** The number of Received V2 Reports.

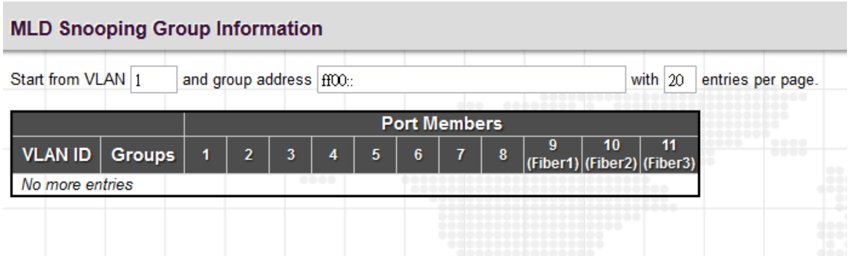
**V2 Leaves Received:** The number of Received V2 Leaves.

***<u>Router Port</u>***

**Port:** The port number.

**Status:** Indicate whether a specific port is a router port or not.

### 4.10.2.5 Groups Information



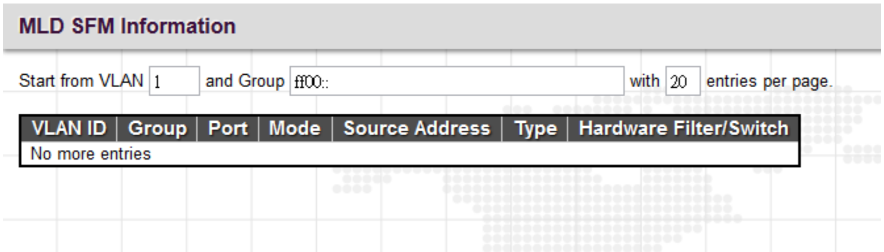

**VLAN ID:** Display the VLAN ID of the group.

**Groups:** Display the group address.

**Port Members:** Ports that belong to this group.

***NOTE:*** The maximum number of MLD Snooping groups can be learned is 32.

### 4.10.2.6 IPv6 SFM Information




**VLAN ID:** Display the VLAN ID of the group.

**Group:** Display the IP address of a multicast group.

**Port:** The switch port number.

**Mode:** The filtering mode maintained per VLAN ID, port number and group address.

**Source Address:** The source IP address available for filtering.

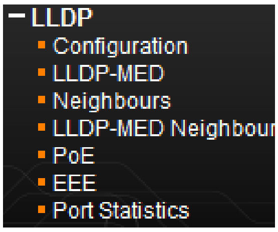
**Type:** Display either Allow or Deny type.

**Hardware Filter/Switch:** Indicates whether the data plane destined to the specific group address from the source IPv4 address can be handled by the chip or not.

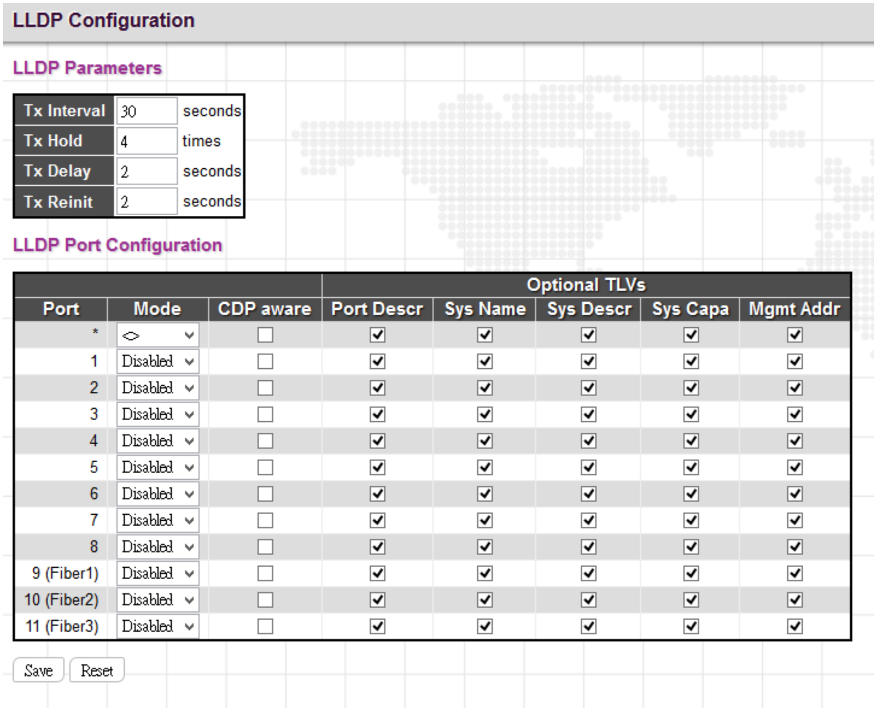
## 4.11 LLDP

LLDP (Link Layer Discovery Protocol) runs over data link layer which is used for network devices to send information about themselves to other directly connected devices on the network. By using LLDP, two devices running different network layer protocols can learn information about each other. A set of attributes referred to TLVs are used to discover neighbour devices. Details such as port description, system name, system description, system capabilities, management address can be sent and received on this device.

The "LLDP" menu contains the following sub menus. Select the appropriate menu to set up detailed configurations.




### *4.11.1 Configuration*



**LLDP Configuration**

**LLDP Parameters**

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

**LLDP Port Configuration**

| | | | Optional TLVs | | | | |
|---|---|---|---|---|---|---|---|
| Port | Mode | CDP aware | Port Descr | Sys Name | Sys Descr | Sys Capa | Mgmt Addr |
| * | <> | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 1 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 2 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 3 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 4 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 5 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 6 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 7 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 8 | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 9 (Fiber1) | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10 (Fiber2) | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 11 (Fiber3) | Disabled | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ |

Save Reset

***<u>LLDP Parameters</u>***

**Tx Interval:** Specify the interval between LLDP frames are sent to its neighbours for updated discovery information. The valid values are 5 - 32768 seconds. The default is 30 seconds.

**Tx Hold:** This setting defines how long LLDP frames are considered valid and is used to compute the TTL. Valid range is 2~10 times. The default is 4.

**Tx Delay:** Specify a delay between the LLDP frames that contain changed configurations. Tx Delay cannot be larger than 1/4 of the Tx interval value. The valid values are 1 - 8192 seconds.

**Tx Reinit:** Specify a delay between the shutdown frame and a new LLDP initialization. The valid values are 1~10 seconds.

***LLDP Port Configuration***

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

**Mode:** Select the appropriate LLDP mode.

**Disabled:** LLDP information will not be sent and LLDP information received from neighbours will be dropped.

**Enabled:** LLDP information will be sent and LLDP information received from neighbours will be analyzed.

**Rx Only:** The switch will analyze LLDP information received from neighbours.

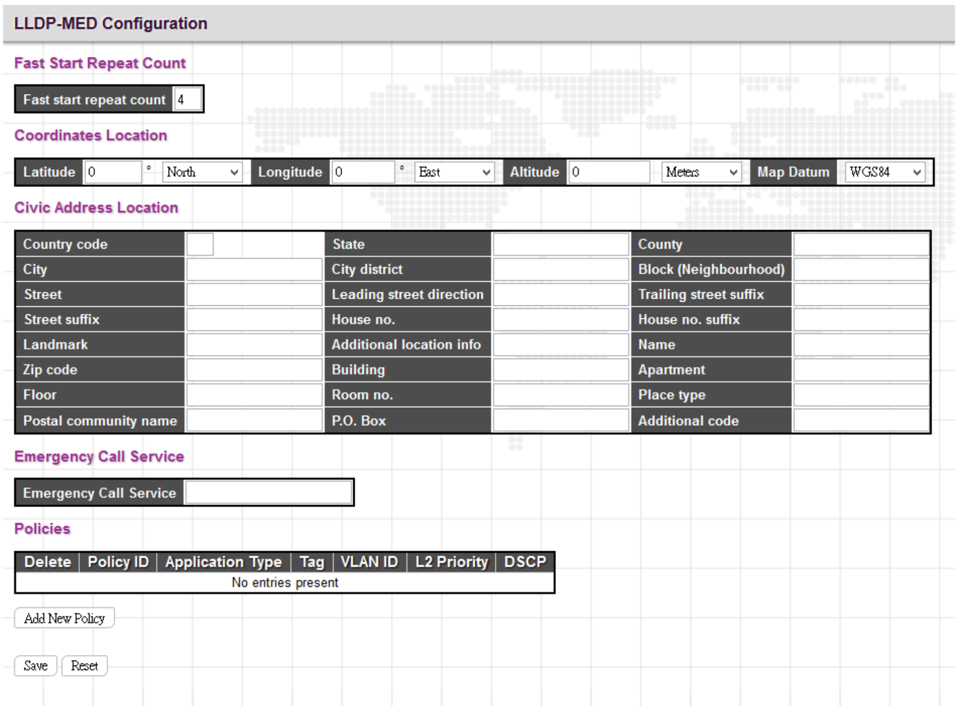
**Tx Only:** The switch will send out LLDP information but will drop LLDP information received from neighbours.

**CDP Aware:** CDP aware operation is used to decode incoming CDP (Cisco Discovery Protocol) frames. If enabled, CDP TLVs that can be mapped into a corresponding field in the LLDP neighbors table are decoded, all others are discarded. CDP TLVs are mapped into LLDP neighbors table as shown below:

**Optional TLVs:** LLDP uses several attributes to discover neighbour devices. These attributes contains type, length, and value descriptions and are referred to TLVs. Details such as port description, system name, system description, system capabilities, management address can be sent from this device. Uncheck the boxes if they are not appropriate to be known by other neighbour devices.

### *4.11.2 LLDP-MED*

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices such as switches. It specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, Power over Ethernet, inventory management and location information.



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

***Coordinates Location***

**Latitude:** Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.

**Longitude:** Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

**Altitude:** Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters).

**Meters:** Representing meters of Altitude defined by the vertical datum specified.

**Floors:** Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

**Map Datum:** The Map Datum is used for the coordinates given in these options:

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

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

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

***Civic Address Location***

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

**Country Code:** The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

**State:** National subdivisions (state, canton, region, province, prefecture).

**County:** County, parish, gun (Japan), district.

**City:** City, township, shi (Japan) - Example: Copenhagen.

**City District:** City division, borough, city district, ward, chou (Japan).

**Block (Neighbourhood):** Neighbourhood, block.

**Street:** Street - Example: Poppelvej.

**Leading street direction:** Example: N.

**Trailing street suffix:** Example: SW.

**Street suffix: Example:** Ave, Platz.

**House no.:** Example: 21.

**House no. suffix:** Example: A, 1/2.

**Landmark:** Landmark or vanity address - Example: Columbia University.

**Additional location info:** Example: South Wing.

**Name: Name (residence and office occupant)**: Example: Flemming Jahn.

**Zip code:** Postal/zip code - Example: 2791.

**Building:** Building (structure). Example: Low Library.

**Apartment:** Unit (Apartment, suite). Example: Apt 42.

**Floor:** Example: 4.

**Room no.:** Room number - Example: 450F.

**Place type:** Example: Office.

**Postal community name:** Example: Leonia.

**P.O. Box:** Example: 12345.

**Additional code:** Example: 1320300003.

***Emergency Call Service***

**Emergency Call Service:** Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

***Policies***

**Policy ID:** Specify the ID for this policy.

**Application Type:** The application types include “Voice”, “Voice Signalling”, “Guest Voice”, “Guest Voice Signalling”, “Softphone Voice”, “Video Conferencing”, “Streaming”, “Video Signalling”.

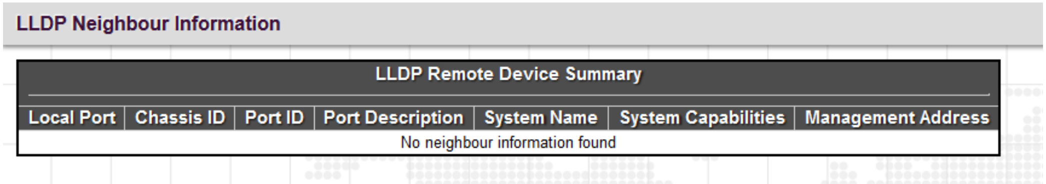
**Tag:** Tag indicating whether the specified application type is using a “tagged” or an “untagged” VLAN.

**VLAN ID:** Specify the VLAN ID for the port.

**L2 Priority:** Specify one of eight priority levels (0-7) as defined by 802.1D-2004.

**DSCP:** Specify one of 64 code point values (0-63) as defined in IETF RFC 2474.

### 4.11.3 Neighbours




**Local Port:** The local port that a remote LLDP-capable device is attached.

**Chassis ID:** An ID indicating the particular chassis in this system.

**Port ID:** A remote port ID that LDPDUs were transmitted.

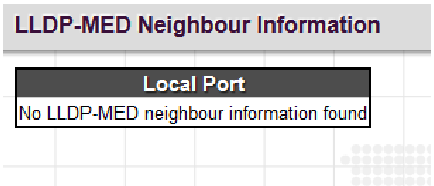
**Port Description:** A remote port's description.

**System Name:** The system name assigned to the remote system.

**System Capabilities:** This shows the neighbour unit's capabilities. When a capability is enabled, the capability is followed by (+). If disabled, the capability is followed by (-).

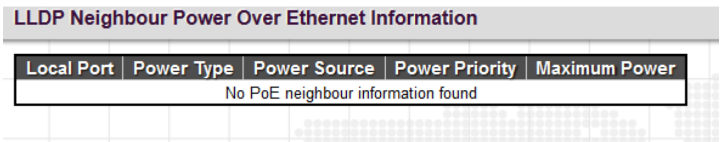
**Management Address:** The IPv4 address of the remote device. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. If the neighbor device allows management access, clicking on an entry in this field will re-direct the web browser to the neighbor's management interface.

### 4.11.4 LLDP-MED Neighbours




This page displays information about LLDP-MED neighbours detected on the network.

### 4.11.5 LLDP PoE




This pages displays information about LLDP PoE neighbours detected.

**Local Port:** The port for this switch on which the LLDP frame was received.

**Power Type:** This displays whether the device is Power Sourcing Entity (PSE) or Powered Device (PD). If the power type is unknown, it shows "Reserved".

**Power Source:** This indicates the power source utilized by PSE or PD device.

**Power Priority:** Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's port that is sourcing the power. There are three levels of power priority (Critical, High and Low). If the power priority is unknown, this is indicated as “Unknown.”

**Maximum Power:** This indicates the maximum power in watt required by a PD device from a PSE device or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.

### *4.11.6 LLDP EEE*

**LLDP Neighbors EEE Information**

| Local Port | Tx Tw | Rx Tw | Fallback Receive Tw | Echo Tx Tw | Echo Rx Tw | Resolved Tx Tw | Resolved Rx Tw | EEE in Sync |
|---|---|---|---|---|---|---|---|---|
| No LLDP EEE information found | | | | | | | | |

**Local Port:** The port for this switch on which the LLDP frame was received.

**Tx Tw:** The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.

**Rx Tw:** The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.

**Fallback Receive Tw:** The link partner's fallback receive Tw.

**Echo Tx Tw:** The link partner's Echo Tx Tw value. The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

**Echo Rx Tw:** The link partner's Echo Rx Tw value.

**Resolved Tx Tw:** The resolved Tx Tw for this link.

**Resolved Rx Tw:** The resolved Rx Tw for this link.

**EEE in Sync:** This shows whether the switch and the link partner have agreed on wake times.

**Red**: Switch and link partner have not agreed on wakeup times.

**Green:** Switch and link partner have agreed on wakeup times.

## 4.11.7 LLDP Global Counters

**LLDP Global Counters**

| Global Counters | |
|---|---|
| Neighbour entries were last changed | 2012-12-31T23:59:54+00:00 (7734 secs. ago) |
| Total Neighbours Entries Added | 0 |
| Total Neighbours Entries Deleted | 0 |
| Total Neighbours Entries Dropped | 0 |
| Total Neighbours Entries Aged Out | 0 |

**LLDP Statistics Local Counters**

| Local Port | Tx Frames | Rx Frames | Rx Errors | Frames Discarded | TLVs Discarded | TLVs Unrecognized | Org. Discarded | Age-Outs |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 (Fiber1) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 (Fiber2) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 (Fiber3) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

***Global Counters***

**Total Neighbours Entries Added:** Shows the number of new entries added since the switch was rebooted, and for which the remote TTL has not yet expired.

**Total Neighbors Entries Deleted:** The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.

**Total Neighbors Entries Dropped:** The number of times which the remote database on this switch dropped an LLDPDU because the entry table was full.

**Total Neighbors Entries Aged Out:** The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

***LLDP Statistics Local Counters***

**Local Port:** The port number.

**Tx Frames:** The number of LLDP PDUs transmitted.

**Rx Frames:** The number of LLDP PDUs received.

**Rx Errors:** The number of received LLDP frames with some kind of error.

**Frames Discarded:** The number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular Type Length Value (TLV).

**TLVs Discarded:** Each LLDP frame can contain multiple pieces of information, known as TLVs. If a TLV is malformed, it is counted and discarded.

**TLVs Unrecognized:** The number of well-formed TLVs, but with an unknown type value.

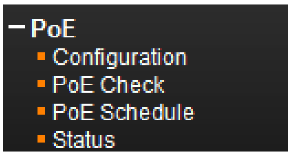
**Org. Discarded:** The number of organizational TLVs discarded.

**Age-Outs:** Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received within the age-out time, the LLDP information is removed, and the Age-Out counter is incremented.

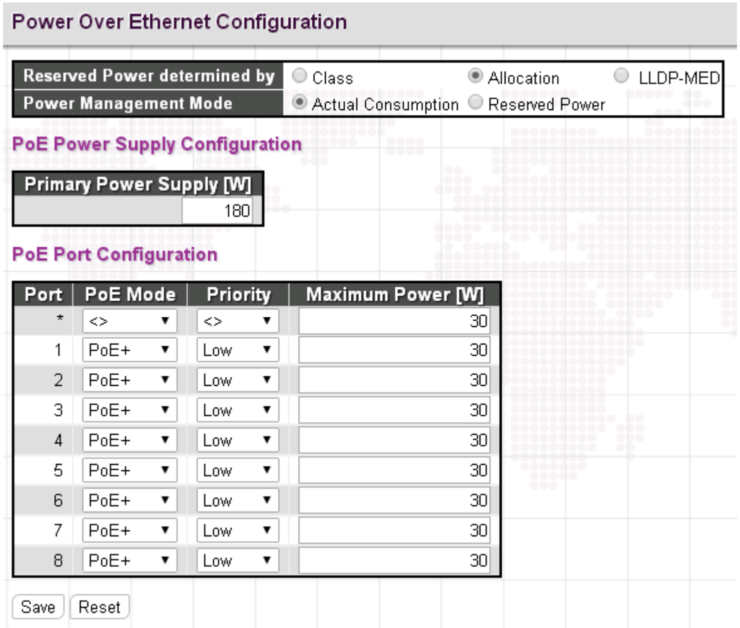
## 4.12 PoE (for PoE models only)

Power over Ethernet (PoE) configuration page is used to set the maximum PoE power provided to a port, the maximum power budget for the switch (power available to all RJ-45 ports), the port PoE operating mode, power allocation priority, and the maximum power allocated to each port. If the power demand from devices connected to the switch exceeds the power budget, the switch uses port power priority settings to limit the supplied power.

The “PoE” menu contains the following sub menus. Select the appropriate menu to configure the detailed settings.




### 4.12.1 PoE Configuration




***<u>Power Over Ethernet Configuration</u>***

**Reserved Power determined by:** There are three modes available for setting up how attached PD may reserve power:

**Class:** Each port automatically determines how much power to reserve according to the class which the connected PD belongs. Four different port classes are used, these are 4, 7, 15.4 and 30 Watts.

**Allocation:** The amount of power reserved for each is specified in “Maximum Power [W]” field.

**LLDP-MED:** This mode is similar to Class mode except that each port determines the amount power it reserves by exchanging PoE information using LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the Class mode.

***NOTE:*** *If ports use more power than the power reserved for them, they will be shut down.*

**Power Management Mode:** There are two modes to define how ports are shut down.

**Actual Consumption:** When this mode is selected, ports are shut down in the event of the following situations.

1. When the actual power consumption for all ports exceeds the amount of power supply can deliver.

2. When the actual power consumption for a given port exceeds the reserved power for that port.

Ports are shut down according to their port priority. If two ports have the same priority, the port with the higher port number is shut down.

**Reserved Power:** When this mode is selected, ports are shut down when total reserved power exceeds the amount of power that the power supply can deliver. In this mode, if the PD (Powered Device) keeps requesting more power than available from the power supply, then the port power is not turned on.

***PoE Power Supply Configuration***

**Primary Power Supply [W]:** The power budget for the switch. If PDs require more power than the switch's budge, the port priority settings are used to control the supplied.

***PoE Port Configuration***

**Port:** The port number. “Port *” rule applies to all ports.

**PoE Mode:** PoE operating modes include the following options:

**Disabled:** Disable PoE function on a per port basis.

**PoE:** Enable IEEE 802.3af (Class 4 PDs limited to 15.4W).

**PoE+:** Enable IEEE 802.3at (Class 4 PDs limited to 30W).

**Priority:** When ports or attached PDs requested more power than the power supply can provide, ports are shut down based on their priority level. The switch will start from shutting down ports that have the low priority and the highest port number.

**Maximum Power [W]:** Allocate the maximum power delivered to ports.

## *4.12.2 PoE Check (PoE PD Auto Test/Auto Reset)*

**Power Over Ethernet Device Failure Check**

| Port | PoE Check | Ping IP Address | No Response Timeout(Cycles 1 ~ 10) | Check Interval (10 ~ 300 Seconds) | No Response Action | Reboot Time (60 ~ 120) |
|---|---|---|---|---|---|---|
| * | <> | | 3 | 10 | <> | 60 |
| 1 | Disabled | | 3 | 10 | No Action | 60 |
| 2 | Disabled | | 3 | 10 | No Action | 60 |
| 3 | Disabled | | 3 | 10 | No Action | 60 |
| 4 | Disabled | | 3 | 10 | No Action | 60 |
| 5 | Disabled | | 3 | 10 | No Action | 60 |
| 6 | Disabled | | 3 | 10 | No Action | 60 |
| 7 | Disabled | | 3 | 10 | No Action | 60 |
| 8 | Disabled | | 3 | 10 | No Action | 60 |

Save Reset

**Port:** The port number. “Port *” rule applies to all ports.

**PoE Check:** Enable or disable PoE failure check function. This switch can monitor PD working status by pinging its IP address. If the switch does not receive a response from PD within the specified response time, the PD status is regarded as failed. Once the PD fails, the switch (PSE) can take an appropriate action selected in "No Response Action" field.

**Ping IP Address:** Specify the PD's IP address for ping purposes. Both IPv4 and IPv6 IP addresses are supported.

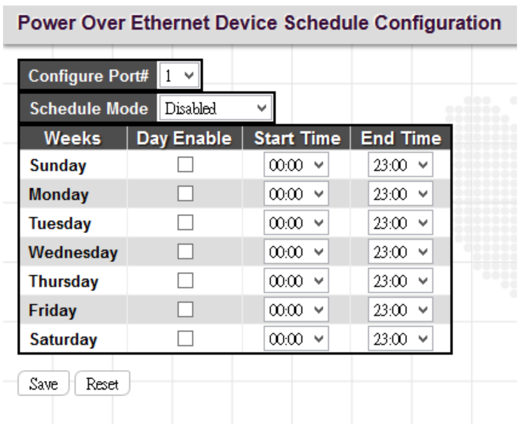
**No Response Timeout (Cycles 1~10):** Specify the total cycles of IP checking.

**Check Interval (10~300 Seconds):** Specify the interval between each ping checking.

**No Response Action:** If PDs fails to respond ping requests sent by the switch (PSE), then the switch (PSE) can take an appropriate action selected here.

> **No Action:** The switch (PSE) will not take any actions on the PD.
>
> **Reboot PD:** The switch (PSE) reboots the PD after the PD failure check.
>
> **Power Off PD:** The switch (PSE) turns off the PD after the PD failure check.

### *4.12.3 PoE Schedule*




In some working environments, PDs only work for a limited of time. Therefore, PoE schedule mechanism can be used to plan PoE schedule on a per port basis so as to ease the PSE's power burden.

**Configure Port#:** Select a port to configure its associated PoE schedule settings.

**Schedule Mode:** Enable or disable PoE schedule mode.

**Weeks:** List of weekdays.

**Day Enable:** Tick on days that you would like the PD to receive power from the PSE.

**Start Time:** Select the starting time for the PSE to provide power to the PD.

**End Time:** Select the end time for the PSE to stop providing power to the PD.

### *4.12.4 Status*

**Power Over Ethernet Status**

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

**Local Port:** The port number on this switch that provides PoE function.

**PD class:** Each PD is classified according to the maximum power it will use. The PD classes include:

Class 0: Max. power 15.4 W
Class 1: Max. power 4.0 W
Class 2: Max. power 7.0 W
Class 3: Max. power 15.4 W
Class 4: Max. power 30.0 W

**Power Requested:** The amount of power that the PDs wants to be reserved.

**Power Allocated:** The amount of power the switch has allocated for the PD.

**Power Used:** How much power the PD is currently using.

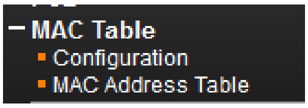
**Current Used:** How much current the PD is currently using.

**Priority:** The port's configured priority level.

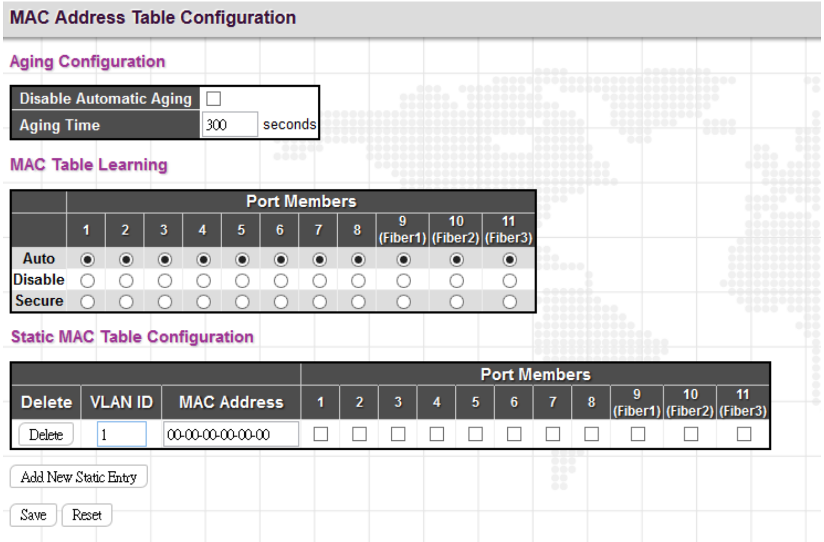
**Port Status:** PoE service status for the attached device.

## 4.13 MAC Table

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



### 4.13.1 MAC Address Table 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.

**Delete:** Delete this MAC address entry.

**VLAN ID:** Specify the VLAN ID 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.

### *4.13.2 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** Auto-refresh Refresh Clear |<< >>

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

| | | | Port Members | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Type | VLAN | MAC Address | CPU | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 (Fiber1) | 10 (Fiber2) | 11 (Fiber3) |
| Dynamic | 1 | 00-02-AB-0D-85-17 | | | | | | | | | ✓ | | | |
| Dynamic | 1 | 00-02-AB-0E-3E-70 | | | | | | | | | ✓ | | | |
| Static | 1 | 00-02-AB-D6-62-90 | ✓ | | | | | | | | | | | |
| Dynamic | 1 | 00-02-AB-D6-64-47 | | | | | | | | | ✓ | | | |
| Dynamic | 1 | 00-02-AB-D6-68-D0 | | | | | | | | | ✓ | | | |
| Dynamic | 1 | 00-1B-FE-00-38-C9 | | ✓ | | | | | | | | | | |
| Dynamic | 1 | 00-1E-8C-9D-1D-52 | | | | | | | | | ✓ | | | |
| Dynamic | 1 | 30-85-A9-3B-B1-50 | | | | | | | | | ✓ | | | |
| Static | 1 | 33-33-00-00-00-01 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Static | 1 | 33-33-00-00-00-02 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Static | 1 | 33-33-FF-00-AB-CD | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Static | 1 | 33-33-FF-D6-62-90 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Dynamic | 1 | 90-E6-BA-17-54-0E | | | | | | | | | ✓ | | | |
| Static | 1 | FF-FF-FF-FF-FF-FF | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

**Type:** Display whether the learned MAC address is static or dynamic.

**VLAN ID:** The VLAN ID associated with this entry.

**MAC Address:** The MAC address learned on CPU or certain ports.

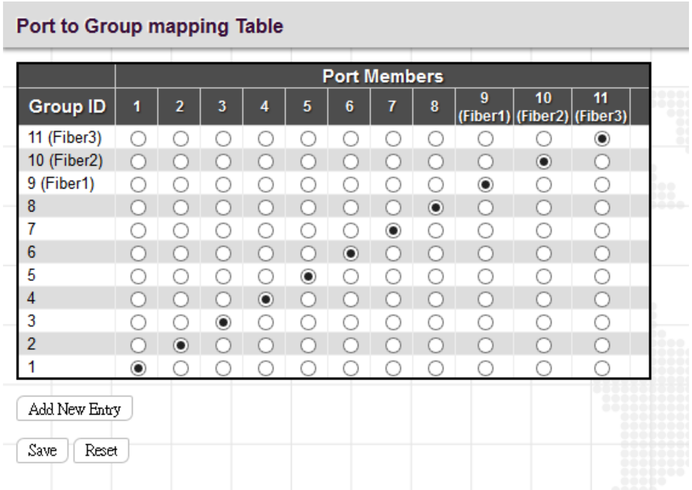
**Port Members:** Ports associated with this entry.

## 4.14 VLAN Translation

VLAN Translation is especially useful for users who want to translate the original VLAN ID to a new VLAN ID so as to exchange data across different VLANs and improve VLAN scaling. VLAN translation replaces an incoming C-VLAN tag with an S-VLAN tag instead of adding an additional tag. When configuring VLAN Translation, both ends of the link normally must be able to replace tags appropriately. In other words, both ends must be configured to translate the C-VLAN tag to S-VLAN tag and S-VLAN tag to C-VLAN tag appropriately in a network. Note that only access ports support VLAN translation.  It is not recommended to configure VLAN Translation on trunk ports.

The “VLAN Translation” menu contains the following sub menus. Select the appropriate one to configure settings or view its status.

### 4.14.1 Port to Group Mapping

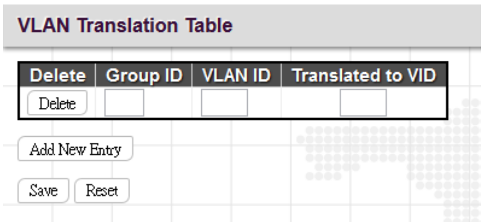



**Group ID:** The total VLAN Translation group can be used is 11 which is automatically created in Group Mapping Table when entering "Port to Group Mapping" page. A port can be mapped to any of the groups. Multiple ports can be mapped to a single group with the same Group ID.

***NOTE:*** *By default, each port is mapped to a group with a group ID equal to the port number. For example, port 2 is mapped to the group with ID is 2.*

**Port Number:** Click the appropriate radio button to include a port into a group.

### 4.14.2 VID Translation Mapping




**Group ID:** Indicate the Group ID that applies to this translation rule.

**VLAN ID:** Indicate the VLAN ID that will be mapped to a new VID.

**Translated to VID:** Indicate the new VID to which VID of ingress frames will be changed.

Click the "Add New Entry" button once to add a new VLAN Translation entry.

## 4.15 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:

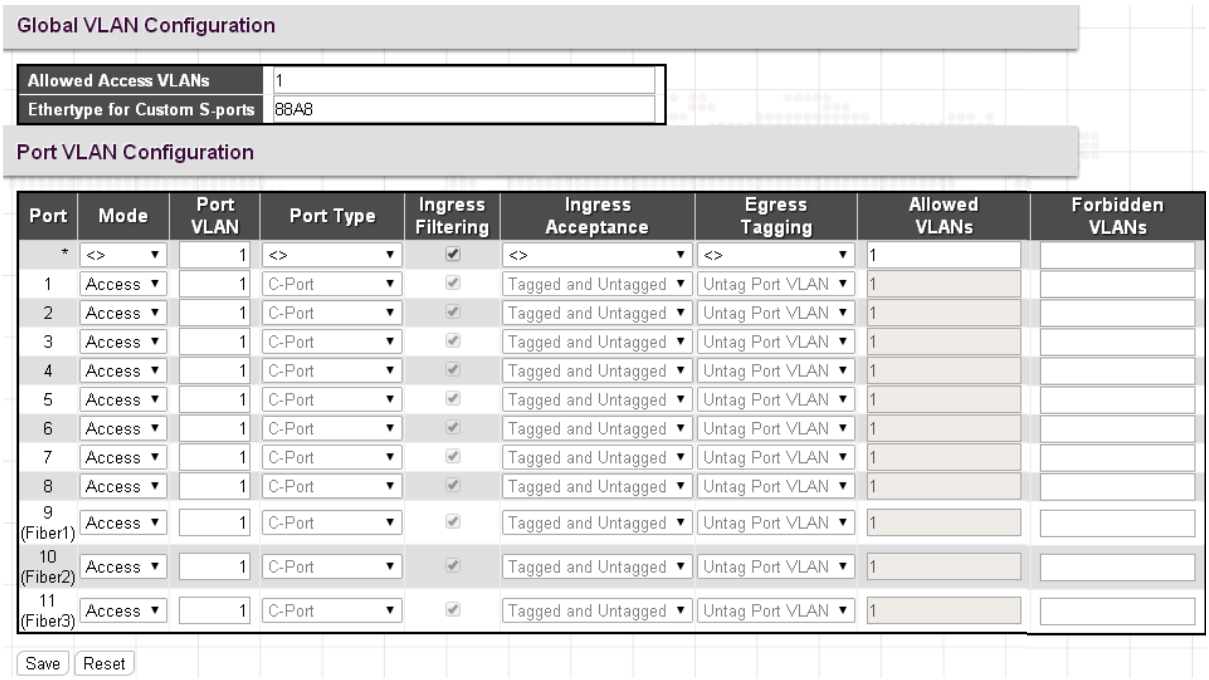
**VLANs provide extra security:** Devices that frequently communicate with each other are grouped into the same VLAN. If devices in a VLAN want to communicate with devices in a different VLAN, the traffic must go through a routing device or Layer 3 switching device.

**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 to set up the detailed configurations.


### 4.15.1 Configuration



Global VLAN Configuration

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

Port VLAN Configuration

| Port | Mode | Port VLAN | Port Type | Ingress Filtering | Ingress Acceptance | Egress Tagging | Allowed VLANs | Forbidden VLANs |
|---|---|---|---|---|---|---|---|---|
| * | <> | 1 | <> | ✔ | <> | <> | 1 | |
| 1 | Access | 1 | C-Port | ✔ | Tagged and Untagged | Untag Port VLAN | 1 | |
| 2 | Access | 1 | C-Port | ✔ | Tagged and Untagged | Untag Port VLAN | 1 | |
| 3 | Access | 1 | C-Port | ✔ | Tagged and Untagged | Untag Port VLAN | 1 | |
| 4 | Access | 1 | C-Port | ✔ | Tagged and Untagged | Untag Port VLAN | 1 | |
| 5 | Access | 1 | C-Port | ✔ | Tagged and Untagged | Untag Port VLAN | 1 | |
| 6 | Access | 1 | C-Port | ✔ | Tagged and Untagged | Untag Port VLAN | 1 | |
| 7 | Access | 1 | C-Port | ✔ | Tagged and Untagged | Untag Port VLAN | 1 | |
| 8 | Access | 1 | C-Port | ✔ | Tagged and Untagged | Untag Port VLAN | 1 | |
| 9 (Fiber1) | Access | 1 | C-Port | ✔ | Tagged and Untagged | Untag Port VLAN | 1 | |
| 10 (Fiber2) | Access | 1 | C-Port | ✔ | Tagged and Untagged | Untag Port VLAN | 1 | |
| 11 (Fiber3) | Access | 1 | C-Port | ✔ | Tagged and Untagged | Untag Port VLAN | 1 | |

Save Reset

***<u>Global VLAN Configuration</u>***

**Allowed Access VLANs:** This shows the allowed access VLANs. This setting only affects ports set in “Access” mode. Ports in other modes are members of all VLANs specified in “Allowed VLANs” field. By default, only VLAN 1 is specified. More allowed access VLANs can be entered by specifying the individual VLAN ID separated by comma. If you want to specify a range, separate it by a dash. For example, 1, 5, 10, 12-15, 100

**Ethertype for Custom S-ports:** Specify ether type used for customer s-ports.

***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,<br>3. If the tagged frame with TPID=0x8100, it becomes a double-tag frame and is forwarded.<br>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,<br>3. If a tagged frame with TIPID=0x8100, it is forwarded.<br>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,<br>3. If a tagged frame with TPID=0x88A8, it is forwarded.<br>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,<br>3. If a tagged frame with TPID=0x88A8, it is forwarded.<br>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:** When you select “Hybrid” mode, the Ingress Filtering field becomes selectable. 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. (Available when Hybrid mode is selected.)

**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. (Available when Hybrid or Trunk mode is selected.)

**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 a 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.

### 4.15.2 Membership

**VLAN Membership Status for Combined users**

Combined ▼ Auto-refresh ☐ Refresh

Start from VLAN 1 with 20 entries per page. |<< >>

| VLAN ID | Port Members | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 (Fiber1) | 10 (Fiber2) | 11 (Fiber3) |
| 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

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

**VLAN ID:** VLANs that are already created.

**Port members:** Display member ports on the configured VLANs.

### 4.15.3 Ports

**VLAN Port Status for Combined users**

Combined ▼ Auto-refresh ☐ Refresh

| Port | Port Type | Ingress Filtering | Frame Type | Port VLAN ID | Tx Tag | Untagged VLAN ID | Conflicts |
|---|---|---|---|---|---|---|---|
| 1 | C-Port | ✔ | All | 1 | Untag PVID | | No |
| 2 | C-Port | ✔ | All | 1 | Untag PVID | | No |
| 3 | C-Port | ✔ | All | 1 | Untag PVID | | No |
| 4 | C-Port | ✔ | All | 1 | Untag PVID | | No |
| 5 | C-Port | ✔ | All | 1 | Untag PVID | | No |
| 6 | C-Port | ✔ | All | 1 | Untag PVID | | No |
| 7 | C-Port | ✔ | All | 1 | Untag PVID | | No |
| 8 | C-Port | ✔ | All | 1 | Untag PVID | | No |
| 9 (Fiber1) | C-Port | ✔ | All | 1 | Untag PVID | | No |
| 10 (Fiber2) | C-Port | ✔ | All | 1 | Untag PVID | | No |
| 11 (Fiber3) | C-Port | ✔ | All | 1 | Untag PVID | | No |

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

**Port:** The port number.

**Port Type:** Display the selected port type on a port.

**Ingress Filtering:** Display whether Ingress Filtering is enabled or disabled.

**Frame Type:** Display the accepted frame type on a port.

**Port VLAN ID:** The port VLAN ID assigned to a port.

**Tx Tag:** Display 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.

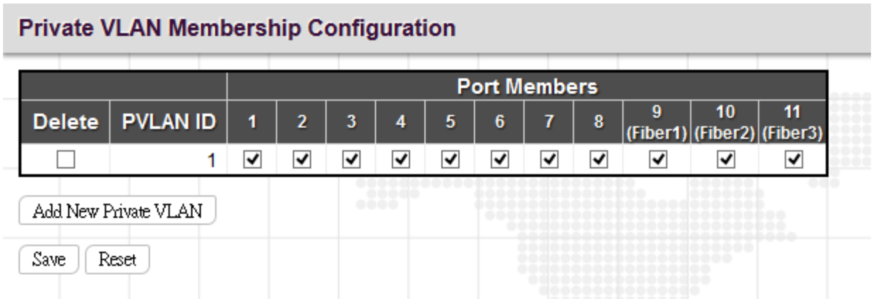
**Conflicts**: Display whether conflicts exist or not. When a software module requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

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

## 4.16 Private VLANs

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


### *4.16.1 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.

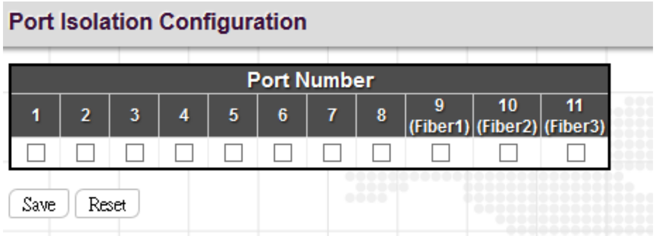
**Delete:** Delete this VLAN membership entry.

**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.

### *4.16.2 Port Isolation*



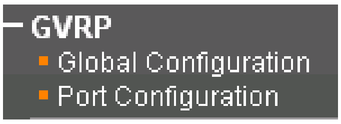

Private VLAN is used to group ports together so as to prevent communications within PVLAN. Port Isolation is used to prevent communications between customer ports in a same Private VLAN. The port that is isolated from others cannot forward any unicast, multicast or broadcast traffic to any other ports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

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

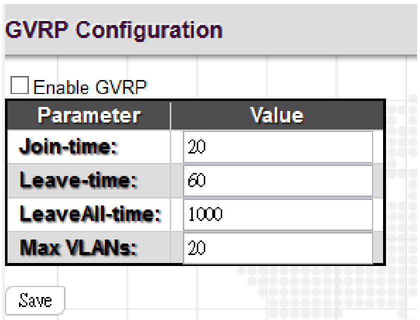
## 4.17 GVRP

GVRP (GVRP VLAN Registration Protocol) is defined in the IEEE 802.1Q standard and enables the switch to dynamically create IEEE 802.1Q compliant VLANs between GVRP-enabled devices. With GVRP, VLAN information can be automatically propagated from device to device so as to reduce errors when creating VLANs manually and provide VIDs consistency across network.

This section provides configuration pages for users to set up GVRP timers and enable GVRP on a per-port basis.




### *4.17.1 Global Configuration*




**Enable GVRP:** Select the checkbox to globally enable GVRP function.

**Join-time:** Specify the amount of time in units of centi-seconds that PDUs are transmitted. The default value is 20 centi-seconds. The valid value is 1~20.

***Note:*** *The "Leave-time" parameter must be three times greater than or equal to Join time.*

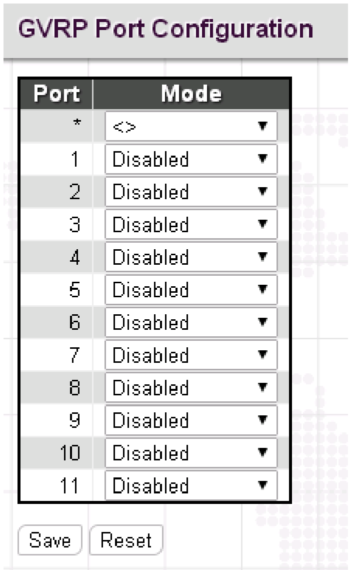
**Leave-time:** Specify the amount of time in units of centi-seconds that the device waits before deleting the associated etry. The leave time is activated by a "Leave All-time" message sent/received and cancelled by the Join message. The default value is 60 centi-seconds.

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

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

**Max VLANs:** The maximum number of VLANs can be learned via GVRP.

### *4.17.2 Port Configuration*

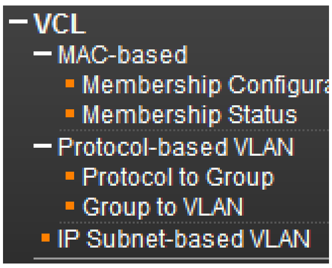



**Port:** The port number.

**Mode:** Enable GVRP on a per port basis.

## 4.18 VCL

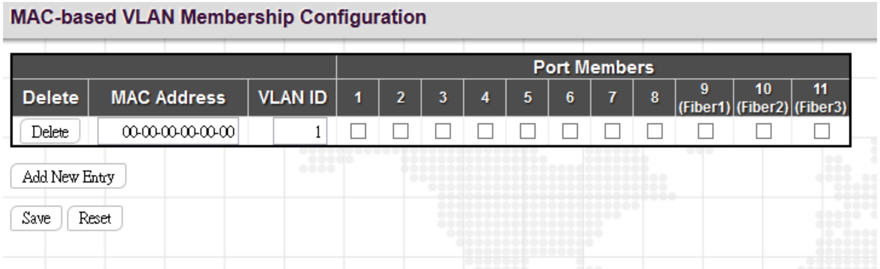
The "VCL" menu contains the following sub menus.




### *4.18.1 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).

#### 4.18.1.1 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.

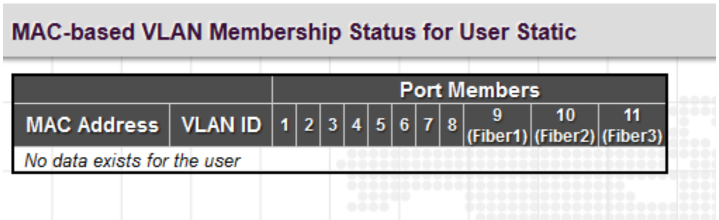
**Port Members:** Ports that belong to this VLAN.

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.

#### 4.18.1.2 Membership Status




This page shows the status of current VCL rules.

**MAC Address:** Display the configured MAC addresses.

**VLAN ID:** Display the VLAN ID of this membership entry.

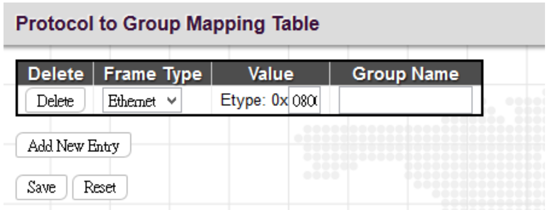
**Port Members:** Display ports that accept the configured MAC address.

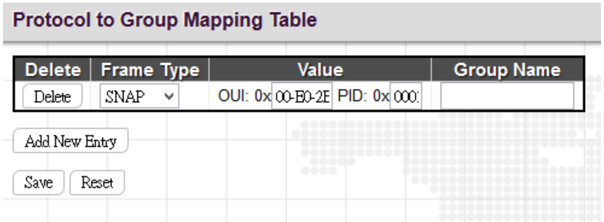
### 4.18.2 Protocol-based VLAN

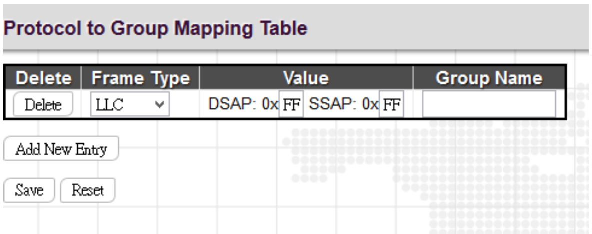
The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of 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.

### 4.18.2.1 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.

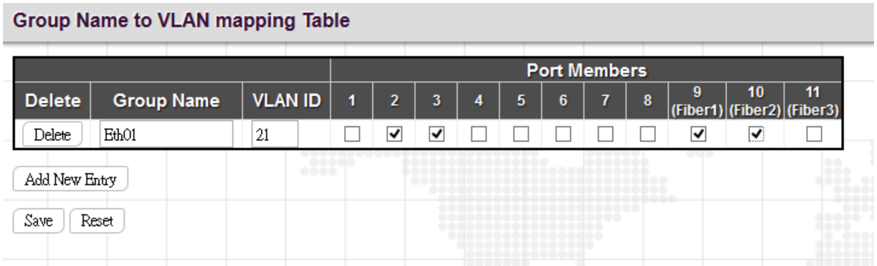
**OUI:** A value in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value in the ranges of 0x00-0xff.

**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).

### *4.18.2.2 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.

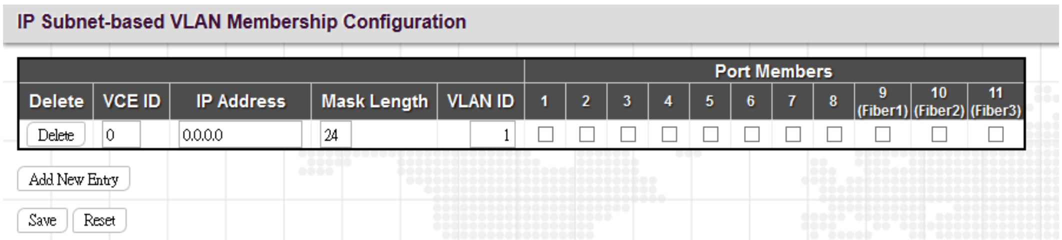
**Port Members:** Assign ports to this rule.

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.

## *4.18.3 IP Subnet-based VLAN*

IP Subnet-based VLAN configuration is to map untagged ingress frames to a specific VLAN if the source address is found in the IP subnet-to-VLAN mapping table. When IP subnet-based VLAN classification is enabled, the source address of untagged ingress 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).




**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.

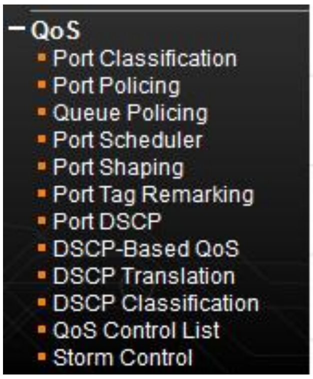
Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

## 4.19 QoS

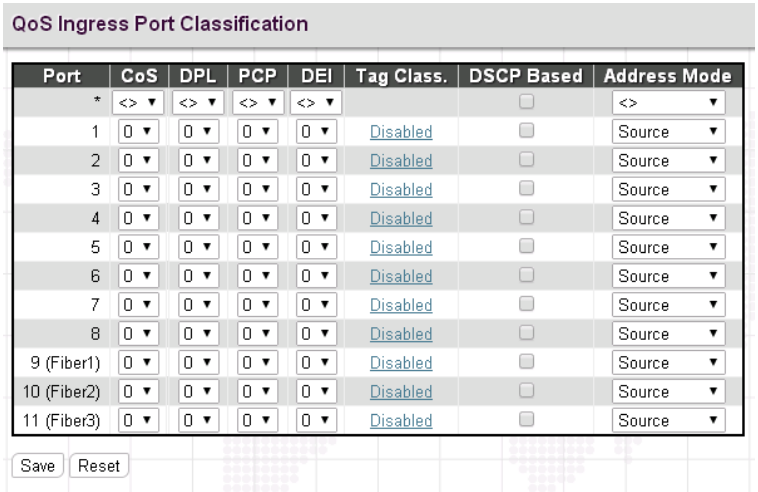
Network traffic is always unpredictable and the only basic assurance that can be offered is the best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria and receives 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.




### 4.19.1 Port Classification



QoS Ingress Port Classification

| Port | CoS | DPL | PCP | DEI | Tag Class. | DSCP Based | Address Mode |
|---|---|---|---|---|---|---|---|
| * | <> | <> | <> | <> | | | <> |
| 1 | 0 | 0 | 0 | 0 | Disabled | | Source |
| 2 | 0 | 0 | 0 | 0 | Disabled | | Source |
| 3 | 0 | 0 | 0 | 0 | Disabled | | Source |
| 4 | 0 | 0 | 0 | 0 | Disabled | | Source |
| 5 | 0 | 0 | 0 | 0 | Disabled | | Source |
| 6 | 0 | 0 | 0 | 0 | Disabled | | Source |
| 7 | 0 | 0 | 0 | 0 | Disabled | | Source |
| 8 | 0 | 0 | 0 | 0 | Disabled | | Source |
| 9 (Fiber1) | 0 | 0 | 0 | 0 | Disabled | | Source |
| 10 (Fiber2) | 0 | 0 | 0 | 0 | Disabled | | Source |
| 11 (Fiber3) | 0 | 0 | 0 | 0 | Disabled | | Source |

Save Reset

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

**QoS class:** Indicate the default QoS class. A QoS class of 0 has the lowest priority. By Default, 0 is used.

**DP Level:** Select the default Drop Precedence Level.

**PCP:** Select the appropriate value for the default Priority Code Point (or User Priority) for untagged frames.

**DEI:** Select the appropriate value for the default Drop Eligible Indicator for untagged frames.

**Tag Class:** This field displays classification mode for tagged frames on this port:

**Disabled:** Use the default QoS class and DP level for tagged frames.

**Enabled:** Use the mapped versions of PCP and DEI for tagged frames.

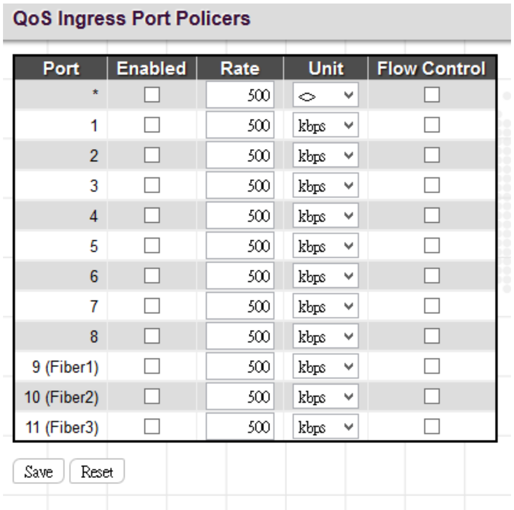
**DSCP Based:** Select the checkbox to enable DSCP based QoS (Ingress Port).

**Address Mode:** The Address Mode specifying whether the QCL classification must be based on source MAC/IP (SMAC/SIP) or destination Mac/IP (DMAC/DIP) addresses on this port.

**Source:** Enable SMAC/SIP matching.

**Destination:** Enable DMAC/DIP matching

### *4.19.2 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.

### 4.19.3 Queue Policing

**QoS Ingress Queue Policers**

| Port | Queue 0 Enable | Queue 1 Enable | Queue 2 Enable | Queue 3 Enable | Queue 4 Enable | Queue 5 Enable | Queue 6 Enable | Queue 7 Enable |
|---|---|---|---|---|---|---|---|---|
| * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 2 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9 (Fiber1) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 10 (Fiber2) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 11 (Fiber3) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Save Reset

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

**Queue 0~7 Enable:** Select the appropriate checkboxes to enable queue policing function on switch ports.

When enabled, the following image will appear:

**QoS Ingress Queue Policers**

| Port | Queue 0 | | | Queue 1 | Queue 2 | Queue 3 | Queue 4 | Queue 5 | Queue 6 | Queue 7 |
|---|---|---|---|---|---|---|---|---|---|---|
| | E | Rate | Unit | Enable | Enable | Enable | Enable | Enable | Enable | Enable |
| * | ☑ | 500 | <> | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 2 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9 (Fiber1) | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 10 (Fiber2) | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 11 (Fiber3) | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Save Reset

**Rate:** Indicate the rate for the ingress queue policer. By default, 500kbps is used. Allowed range for kbps is 100 to 1000000. Allowed range for Mbps is 1 to 3300Mbps.

**Unit:** Select he unit of measure for the ingress queue policer.

**Save:** Save the current running configurations to memory.

**Reset:** Clear all selected settings.

### 4.19.4 Port Scheduler

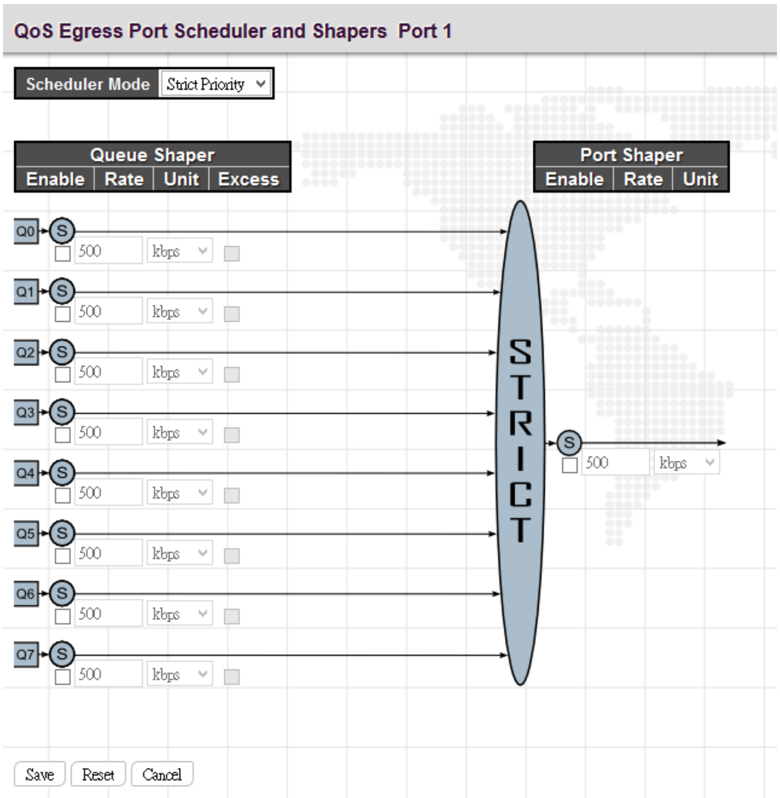
**QoS Egress Port Schedulers**

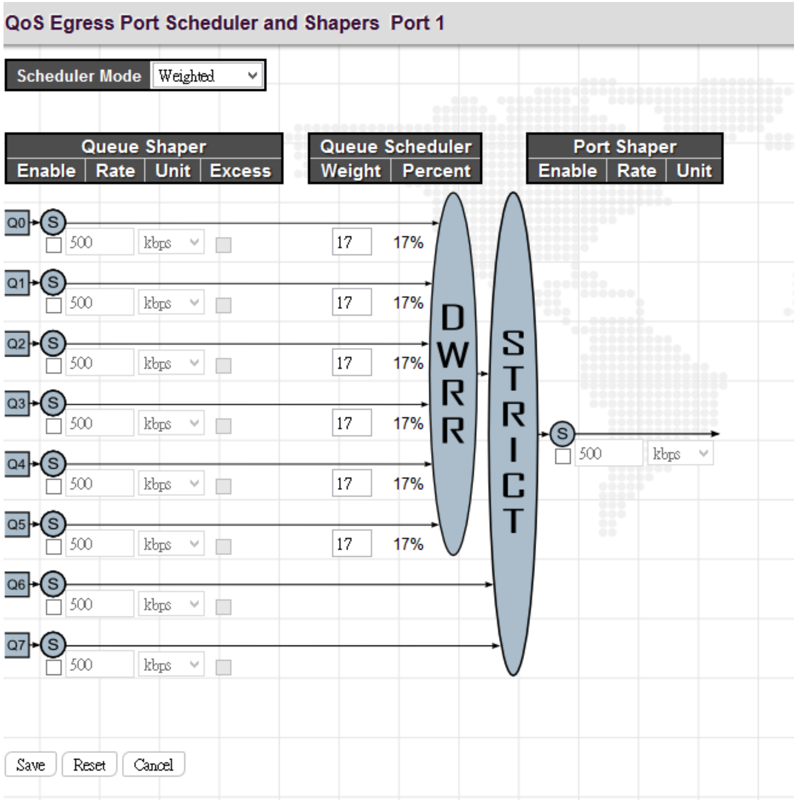
| Port | Mode | Weight | | | | | |
|---|---|---|---|---|---|---|---|
| | | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 |
| 1 | Strict Priority | - | - | - | - | - | - |
| 2 | Strict Priority | - | - | - | - | - | - |
| 3 | Strict Priority | - | - | - | - | - | - |
| 4 | Strict Priority | - | - | - | - | - | - |
| 5 | Strict Priority | - | - | - | - | - | - |
| 6 | Strict Priority | - | - | - | - | - | - |
| 7 | Strict Priority | - | - | - | - | - | - |
| 8 | Strict Priority | - | - | - | - | - | - |
| 9 (Fiber1) | Strict Priority | - | - | - | - | - | - |
| 10 (Fiber2) | Strict Priority | - | - | - | - | - | - |
| 11 (Fiber3) | Strict Priority | - | - | - | - | - | - |

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

**Mode:** Display scheduler mode selected.

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

***<u>Queue Shaper/Port Shaper/Queue Shaper</u>***

**Enable:** Select the checkbox to enable queue shaper on a certain queue for this selected port.

**Rate:** Indicate the rate for the queue shaper. By default, 500kbps is used. Allowed range for kbps is 100 to 1000000. Allowed range for Mbps is 1 to 3300Mbps.

**Unit:** Select he unit of measure for the queue shaper.

**Excess:** Select the checkbox to allow excess bandwidth.

***<u>Queue Schedule</u>***

**Queue Scheduler:** When Scheduler Mode is set to Weighted, the user needs to indicate a relative weight for each queue. DWRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

**Weight:** Assign a weight to each queue. This weight sets the frequency at which each queue is polled for service and subsequently affects the response time software applications assigned a specific priority value.

**Percent:** The weight as a percentage for this queue.

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

**Enable:** Select the checkbox to enable Port shaper.

**Rate:** Indicate the rate for Port Shaper. By default, 500kbps is used. Allowed range for kbps is 100 to 1000000. Allowed range for Mbps is 1 to 3300Mbps.

**Unit:** Select the rate of measure

### 4.19.5 Port Shaping

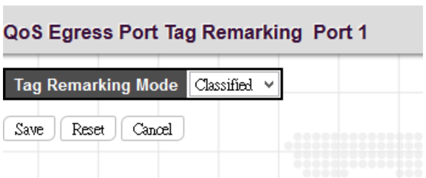
**QoS Egress Port Shapers**

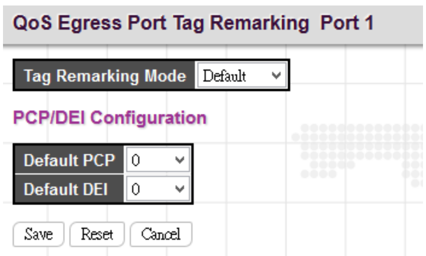
| Port | Shapers | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | Port |
| 1 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 2 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 3 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 4 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 5 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 6 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 7 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 8 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 9 (Fiber1) | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 10 (Fiber2) | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 11 (Fiber3) | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |

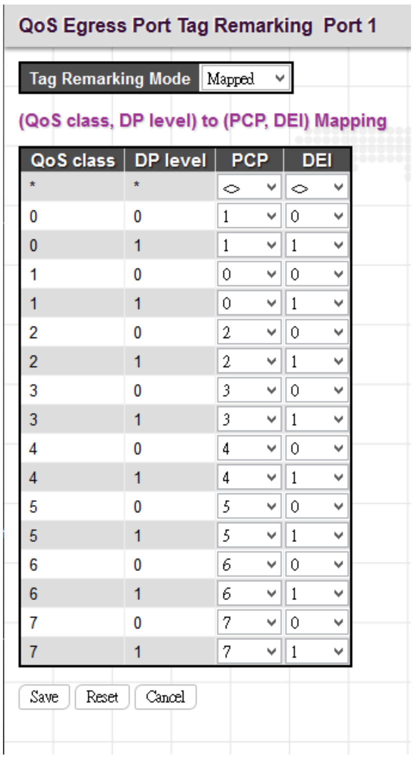
This displays each port’s queue shaper and port shaper’s rate.

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

### 4.19.6 Port Tag Remarking





QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode: Mapped

(QoS class, DP level) to (PCP, DEI) Mapping

| QoS class | DP level | PCP | DEI |
|---|---|---|---|
| * | * | <> | <> |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 |
| 2 | 0 | 2 | 0 |
| 2 | 1 | 2 | 1 |
| 3 | 0 | 3 | 0 |
| 3 | 1 | 3 | 1 |
| 4 | 0 | 4 | 0 |
| 4 | 1 | 4 | 1 |
| 5 | 0 | 5 | 0 |
| 5 | 1 | 5 | 1 |
| 6 | 0 | 6 | 0 |
| 6 | 1 | 6 | 1 |
| 7 | 0 | 7 | 0 |
| 7 | 1 | 7 | 1 |

Save Reset Cancel

**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).

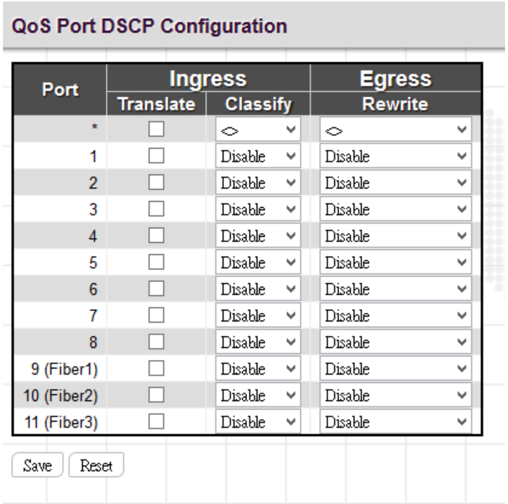
**Mapped:** Use the mapping of the classified QoS class values and DP levels to PCP/DEI values.

**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)

### 4.19.7 Port DSCP



QoS Port DSCP Configuration

| Port | Ingress | | Egress |
|---|---|---|---|
| | Translate | Classify | Rewrite |
| * | ☐ | <> | <> |
| 1 | ☐ | Disable | Disable |
| 2 | ☐ | Disable | Disable |
| 3 | ☐ | Disable | Disable |
| 4 | ☐ | Disable | Disable |
| 5 | ☐ | Disable | Disable |
| 6 | ☐ | Disable | Disable |
| 7 | ☐ | Disable | Disable |
| 8 | ☐ | Disable | Disable |
| 9 (Fiber1) | ☐ | Disable | Disable |
| 10 (Fiber2) | ☐ | Disable | Disable |
| 11 (Fiber3) | ☐ | Disable | Disable |

Save Reset

**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.

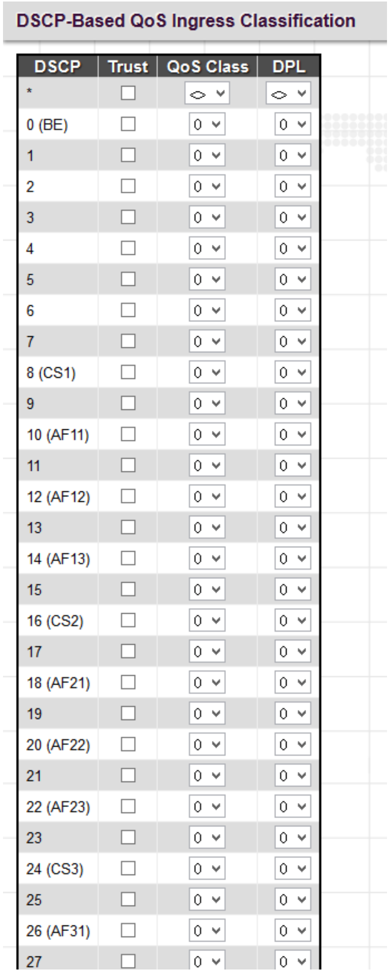
**Disable:** Egress rewriting is disabled.

**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.

### *4.19.8 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.

### 4.19.9 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.

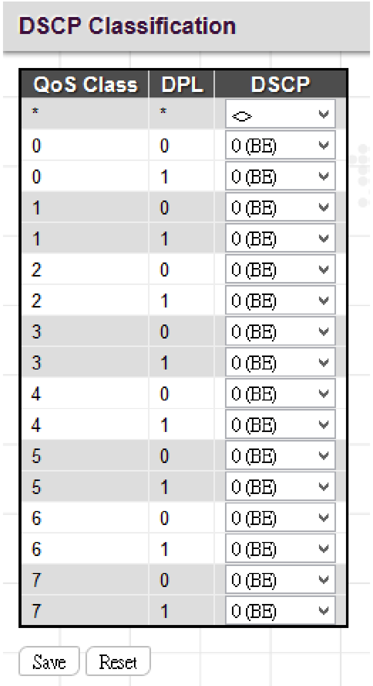
**Ingress Translate:** Enable Ingress Translation of DSCP values based on the specified classification method.

**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.

### 4.19.10 DSCP Classification


DSCP Classification

| QoS Class | DPL | DSCP |
|---|---|---|
| * | * | <> |
| 0 | 0 | 0 (BE) |
| 0 | 1 | 0 (BE) |
| 1 | 0 | 0 (BE) |
| 1 | 1 | 0 (BE) |
| 2 | 0 | 0 (BE) |
| 2 | 1 | 0 (BE) |
| 3 | 0 | 0 (BE) |
| 3 | 1 | 0 (BE) |
| 4 | 0 | 0 (BE) |
| 4 | 1 | 0 (BE) |
| 5 | 0 | 0 (BE) |
| 5 | 1 | 0 (BE) |
| 6 | 0 | 0 (BE) |
| 6 | 1 | 0 (BE) |
| 7 | 0 | 0 (BE) |
| 7 | 1 | 0 (BE) |

Save Reset

Map DSCP values to QoS class and DPL value.

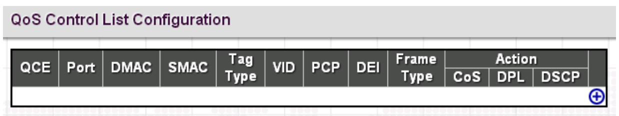
**QoS Class:** List of actual QoS class values.

**DPL:** List of actual DPL values

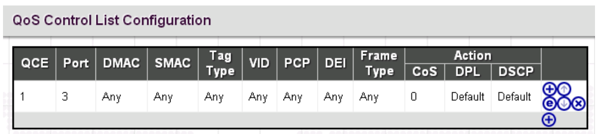
**DSCP:** Select the DSCP value to map QoS class and DPL value. DSCP value selected for "*" will map to all QoS class and DPL value.

### 4.19.11 QoS Control List

Quality of Service control list is used to establish policies for handling ingress packets based on frame type, MAC address, VID, PCP, DEI values. Once a QCE is mapped to a port, traffic matching the first entry in the QoS Control List is assigned to the QoS class, drop precedence level, and DSCP value defined by that entry. Traffic not matching any of the QCEs are classified to the default QoS Class for the port.


QoS Control List Configuration

| QCE | Port | DMAC | SMAC | Tag Type | VID | PCP | DEI | Frame Type | Action CoS | Action DPL | Action DSCP |
|---|---|---|---|---|---|---|---|---|---|---|---|


QoS Control List Configuration

| QCE | Port | DMAC | SMAC | Tag Type | VID | PCP | DEI | Frame Type | Action CoS | Action DPL | Action DSCP |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 3 | Any | Any | Any | Any | Any | Any | Any | 0 | Default | Default |

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:** Indicates tag type. Possible values are: Any, Untagged, Tagged, C-Tagged, S-Tagged.

**VID:** Display VLAN ID (1-4095)

**PCP:** Display PCP value.

**DEI:** Display DEI value.

**Action:** Display the classification action taken on ingress frames when the configured parameters are matched in the frame's content. If a frame matches the QCL, the following actions will be taken.

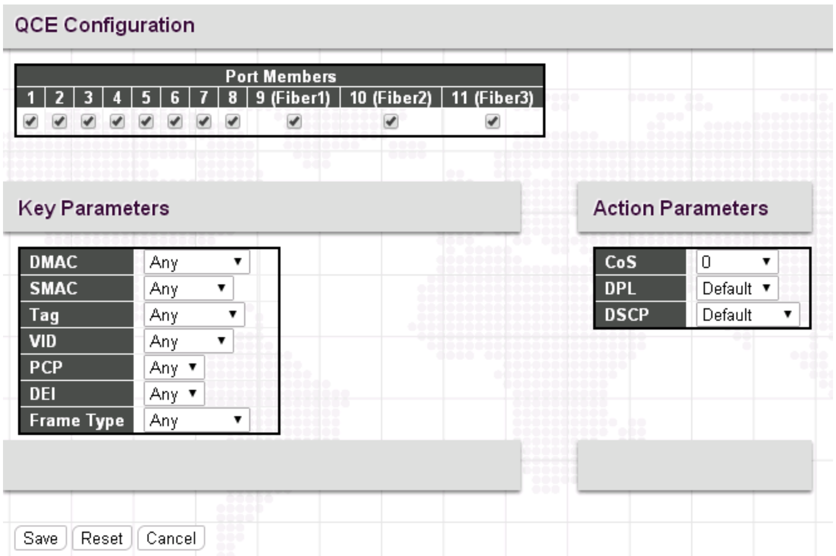
**CoS:** If a frame matches the QCL, it will be put in the queue corresponding to the specified QoS class.

**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***

**SMAC:** Select source MAC address type. By default, any is used. Select "Specific" to specify a source MAC (first three bytes of the MAC address or OUI).

**DMAC Type:** Select destination MAC address type. By default, any is used. Other options available are "UC" for unicast, "MC" for multicast, and "BC" for broadcast.

**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.

**Ethernet:** This option can only be used to filter Ethernet II formatted packets (Options: Any, Specific – 600-ffff hex; Default: ffff). Note that 800 (IPv4) and 86DD (IPv6) are excluded. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

**LLC:** LLC refers to Link Logical Control and further provides three options.

**SSAP:** SSAP stands for Source Service Access Point address. By default, any is used. Select specific to indicate a value (0x00 - 0xFF).

**DSAP:** DSAP stands for Destination Service Access Point address. By default, any is used. Select specific to indicate a value (0x00 to 0xFF).

**Control:** Control field may contain command, response, or sequence information depending on whether the LLC frame type is Unnumbered, Supervisory, or Information. By default, any is used. Select specific to indicate a value (0x00 to 0xFF).

**SNAP:** SubNetwork Access Protocol can be distinguished by an OUI and a Protocol ID. (Options for PID: Any, Specific (0x00-0xffff); Default: Any) If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI isother than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

**IPv4:**

**Protocol:** IPv4 frame type includes Any, TCP, UDP, Other. If "TCP" or "UDP" is selected, you might further define Sport (Source port number) and Dport (Destination port number).

**Source IP:** Select source IP type. By default, any is used. Select "Specific" to indicate self-defined source IP and submask format. The address and mask must be in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero

**IP Fragment:** By default, any is used. Datagrams sometimes may be fragmented to ensure they can pass through a network device that uses a maximum transfer unit smaller than the original packet's size.

**DSCP:** By default, any is used. Select "Specific" to indicate a DSCP value. Select "Range" to indicate a range of DSCP value.

**IPv6:**

**Protocol:** IPv6 protocol includes Any, TCP, UDP, Other. If "TCP" or "UDP" is selected, you may need to further define Sport (Source port number) and Dport (Destination port number).

**Source IP:** Select source IP type. By default, any is used. Select "Specific" to indicate self-defined source IP and submask format.

**DSCP:** By default, any is used. Select "Specific" to indicate a DSCP value. Select "Range" to indicate a range of DSCP value.

***Action Parameters***

Specify the classification action taken on ingress frame if the parameters match the frame's content. The actions taken include the following:

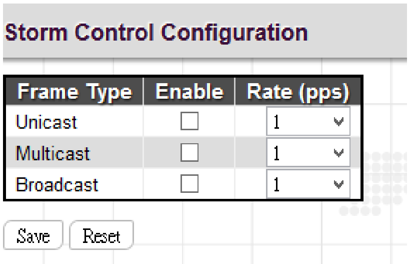
**CoS:** If a frame matches the QCE, it will be put in the queue corresponding to the specified QoS class or placed in a queue based on basic classification rules.

**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.

### *4.19.12 Storm Control*

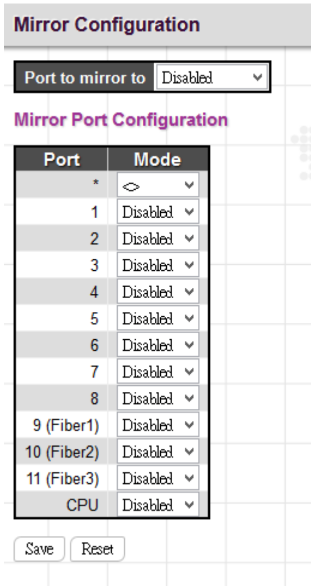
Storm Control is used to keep a network from downgraded performance or a complete halt by setting up a threshold for traffic like broadcast, unicast and multicast. When a device on the network is malfunctioning or application programs are not well designed or properly configured, storms may occur and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

## 4.20 Mirroring




**Port to mirror:** Select the mirror port to which rx or tx traffic will be mirrored. Or disable port mirroring function.

***Mirror Port Configuration***

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

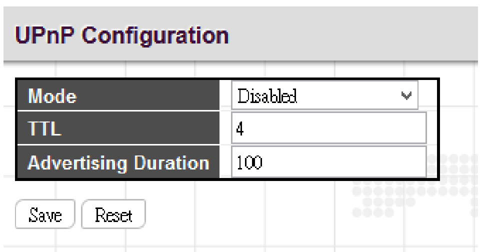
**Disabled:** Disable the port mirroring function on a given port.

**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.

## 4.21 UPnP



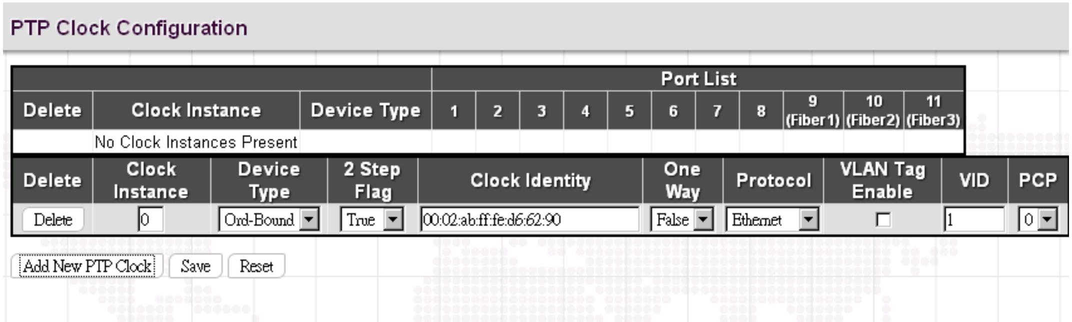

**Mode:** Enable or disable UPnP operation.

**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.

## 4.22 PTP (IEEE1588)

### *4.22.1 Configuration*




Click on “Add New PTP Clock” button to create a new entry.

**Clock Instance:** Indicate the Instance of a particular Clock Instance. The valid instance number is from 0 to 3.

**Device Type:** Indicate the Type of the Clock Instance. There are five Device Types.

**Ord-Bound:** Clock's Device Type is Ordinary-Boundary Clock.

**P2p Transp:** Clock's Device Type is Peer to Peer Transparent Clock.

**E2e Transp:** Clock's Device Type is End to End Transparent Clock.

**Master Only:** Clock's Device Type is Master Only.

**Slave Only:** Clock's Device Type is Slave Only.

**2 Step Flag:** True if two-step Sync events and Pdelay_Resp events are used

**Clock Identity:** This shows unique clock identifier.

**One Way:** If true, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

**Protocol:** Select transport protocol used by the PTP protocol engine.

**Ethernet:** PTP over Ethernet multicast.

**ip4multi:** PTP over IPv4 multicast.

**ip4uni:** PTP over IPv4 unicast.

Note: IPv4 unicast protocol only works in Master only and Slave only clocks. In a unicast Slave only clock you also need to configure which master clocks to request Announce and Sync messages from.

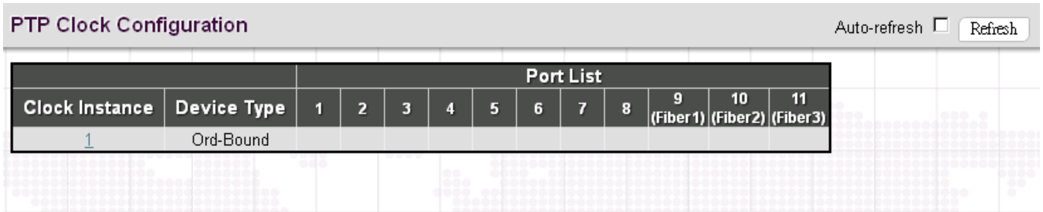
**VLAN Tag Enable:** Enables the VLAN tagging for the PTP frames.

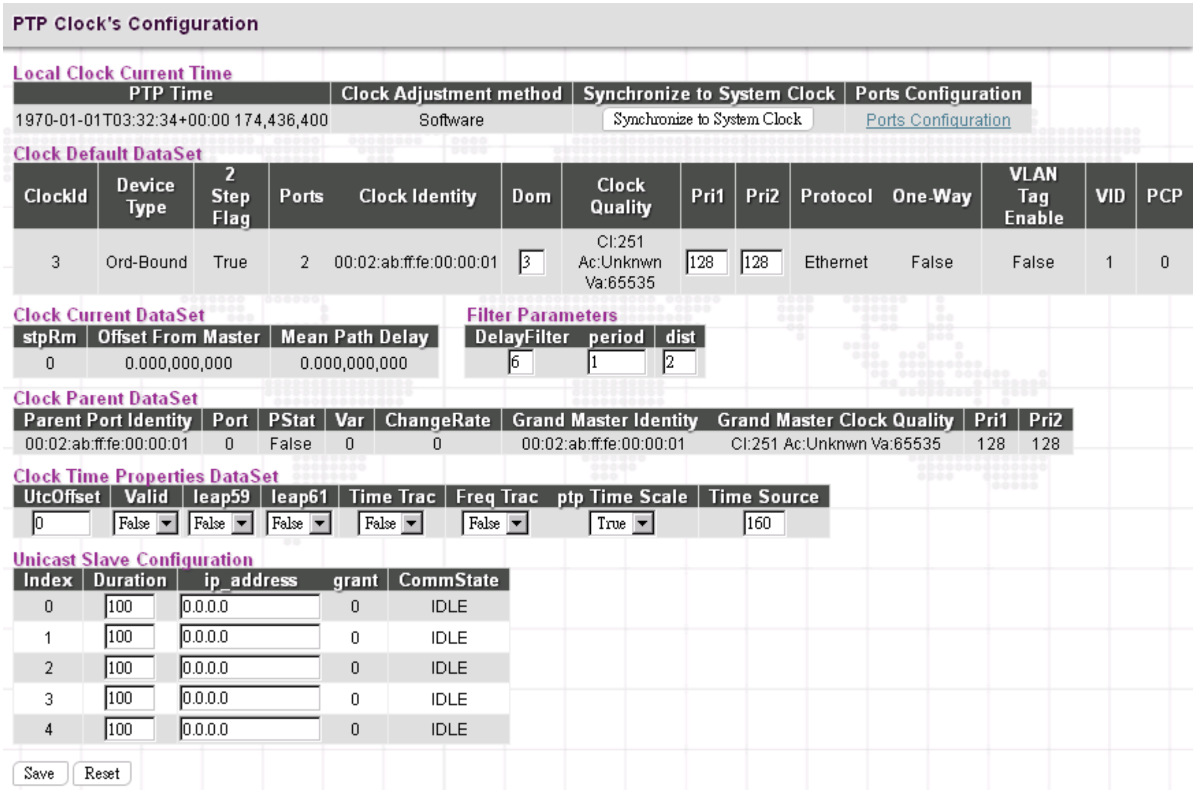
Note: Packets are only tagged if the port is configured for vlan tagging. i.e: Port Type != Unaware and PortVLAN mode == None, and the port is member of the VLAN.

**VID:** VLAN Identifier used for tagging the PTP frames.

**PCP:** Priority Code Point value used for PTP frames.

Click on the Clock Instance number to edit the Clock details.




***Local Clock Current time:*** This shows and updates local clock data.

**PTP Time:** Shows the actual PTP time with nanosecond resolution.

**Clock Adjustment Method:** Shows the actual clock adjustment method. The method depends on the available hardware.

**Synchronize to System Clock:** Click this button to synchronize the System Clock to PTP Time.

**Ports Configuration:** Click to edit the port data set for the ports assigned to this clock instance.

***Clock Default Dataset:*** The clock default data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members defined at clock creation time, the Dynamic members defined by the system, and the configurable members which can be set here.

**ClockId:** This shows the instance id number (0~3).

**Device Type:** This shows the Type of the Clock Instance.

**2 Step Flag:** This shows True or False.

**Ports:** This shows the total number of physical ports in the node.

**Clock Identity:** This shows unique clock identifier.

**Dom:** Configure clock domain (0~127).

**Clock Quality:** The clock quality is determined by the system, and holds 3 parts: Clock Class, Clock Accuracy and OffsetScaledLog Variance as defined in IEEE1588. The Clock Accuracy values are defined in IEEE1588 table 6 (Currently the clock Accuracy is set to 'Unknown' as default).

**Pri1:** Configure Clock priority 1 used by the BMC master select algorithm. The valid value is from 0 to 255.

**Pri2:** Configure Clock priority 2 used by the BMC master select algorithm. The valid value is from 0 to 255.

**Protocol:** This shows transport protocol used by the PTP protocol engine.

**One-Way:** If true, one way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

**VLAN Tag Enable:** This shows whether VLAN tagging for the PTP frames is enabled (True) or not (False).

**VID:** This shows VLAN Identifier used for tagging the VLAN packets.

**PCP:** This shows Priority Code Point value used for PTP frames.

***Clock current Data Set:*** The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic

**stpRm:** This stands for "Steps Removed" and is the number of PTP clocks traversed from the grandmaster to the local slave clock.

**Offset from master:** This shows time difference between the master clock and the local slave clock, measured in ns.

**Mean Path Delay:** This shows the mean propagation time for the link between the master and the local slave.

***Filter Parameters***

**DelayFilter, Period, Dist:** The default delay filter is a low pass filter, with a time constant of 2**DelayFilter*DelayRequestRate. The default offset filter uses a minimum delay filter method i.e. The minimum measured offset during Period samples is used in the calculation. The distance between two calculations is Dist periods.

***Clock Parent Data Set:*** The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

**Parent Port Identity:** This shows Clock identity for the parent clock, if the local clock is not a slave, the value is the clocks own id.

**Port:** This shows port ID for the parent master port.

**PStat:** Parents Stats (always false).

**Var:** It is observed parent offset scaled log variance.

**Change Rate:** Observed Parent Clock Phase Change Rate. i.e. the slave clocks rate offset compared to the master. (unit = ns per s).

**Grand Master Identity:** Clock identity for the grand master clock, if the local clock is not a slave, the value is the clocks own id.

**Grand Master Clock Quality:** The clock quality (Clock Class, Clock Accuracy and OffsetScaledLog Variance) announced by the grand master.

**Pri1:** Clock priority 1 announced by the grand master.

**Pri2:** Clock priority 2 announced by the grand master.

***Clock Time Properties Data Set:*** The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, i.e. the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation.

***Unicast Slave Configuration:*** When operating in IPv4 Unicast mode, the slave is configured up to 5 master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then request Sync messages from the selected master.

**Duration:** Configure the number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds.

**ip_address:** Configure IPv4 Address of the Master clock.

**grant:** The granted repetition period for the sync message.

**CommState:** The state of the communication with the master, possible values are:

**IDLE:** The entry is not in use.

**INIT:** Announce is sent to the master (Waiting for a response).

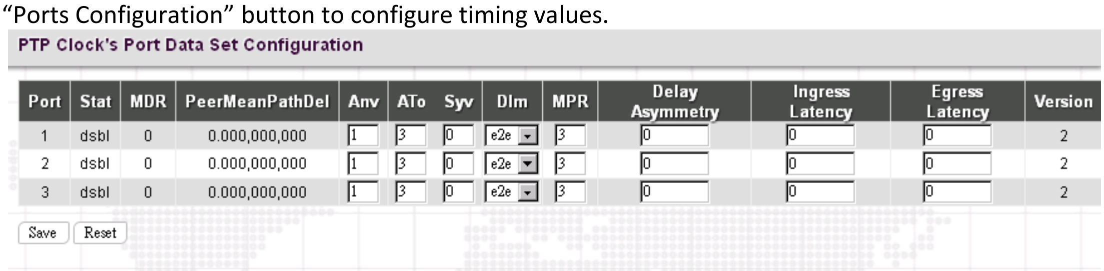
**CONN:** The master has responded.

**SELL:** The assigned master is selected as current master.

**SYNC:** The master is sending Sync messages.

***Ports Configuration***

Click on "Ports Configuration" button to configure timing values.



PTP Clock's Port Data Set Configuration

| Port | Stat | MDR | PeerMeanPathDel | Anv | ATo | Syv | Dlm | MPR | Delay Asymmetry | Ingress Latency | Egress Latency | Version |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0 | 0 | 0 | 2 |
| 2 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0 | 0 | 0 | 2 |
| 3 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0 | 0 | 0 | 2 |

Save Reset

**Anv:** The interval for issuing announce messages in master state.

**ATo:** The timeout for receiving announce messages on the port.

**Syv:** The interval for issuing sync messages in master.

**Dlm:** Configure member delay Mechanism used for the port. This can be defined per port in an Ordinary/Boundary clock. In a transparent clock all ports use the same delay mechanism, determined by the clock type.

> **e2e:** End to end delay measurement.
>
> **p2p:** Peer to peer delay measurement.

**MPR:** The interval for issuing Delay_Req messages for the port in E2Emode. This value is announced from the master to the slave in an announce message. The value is reflected in the MDR field in the Slave.

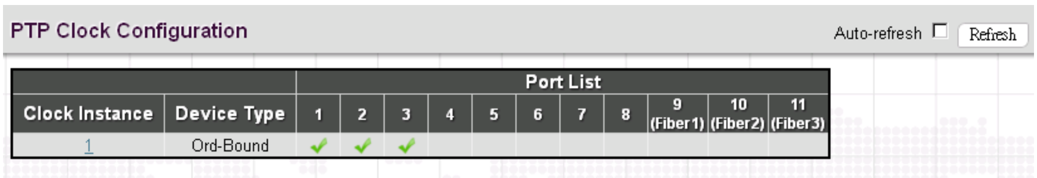
**Delay Asymmetry:** If the transmission delay for a link in not symmetric, the asymmetry can be configured here, see IEEE 1588 Section 7.4.2 Communication path asymmetry

**Ingress latency:** Ingress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.

**Egress Latency:** Egress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.

**Version:** The current implementation only supports PTP version 2.

### *4.22.2 Status*


PTP Clock Configuration   Auto-refresh ☐ Refresh

| Clock Instance | Device Type | Port List | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 (Fiber1) | 10 (Fiber2) | 11 (Fiber3) |
| 1 | Ord-Bound | ✓ | ✓ | ✓ | | | | | | | | |

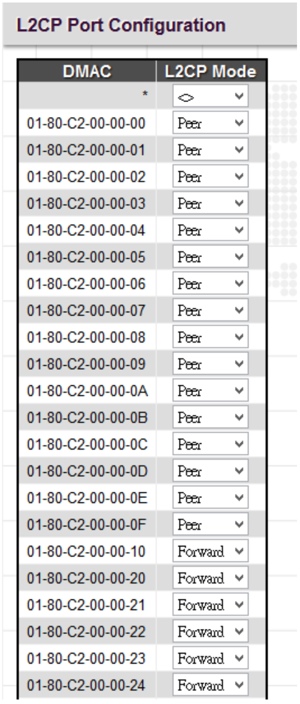
**Clock Instance:** This indicates the Instance of a particular Clock Instance 0 to 3.

**Device Type:** This indicates the Type of the Clock Instance. There are five Device Types.

**Port List:** This shows the ports configured for that Clock Instance.

## 4.23 L2CP

L2CP stands for Layer 2 Control Protocol and contains Ethernet control protocols such as Spanning Tree BPDUs, LACP, Pause frames, etc. A L2CP frame has a specific destination address (DA) belonging to reserved multicast MAC address ranges. MEF defines L2CP processing rules for Ethernet Frames carrying a MAC destination address (DA) within the range of 01-80-C2-00-00-00 through 01-80-C2-00-00-0F and 01-80-C2-00-00-20 through 01-80-C2-00-00-2F. Therefore, if a vendor defines L2CP frames outside the specified MAC DA ranges, the L2CP handling rules do not apply to these frames.


L2CP Port Configuration

| DMAC | L2CP Mode |
|---|---|
| * | <> |
| 01-80-C2-00-00-00 | Peer |
| 01-80-C2-00-00-01 | Peer |
| 01-80-C2-00-00-02 | Peer |
| 01-80-C2-00-00-03 | Peer |
| 01-80-C2-00-00-04 | Peer |
| 01-80-C2-00-00-05 | Peer |
| 01-80-C2-00-00-06 | Peer |
| 01-80-C2-00-00-07 | Peer |
| 01-80-C2-00-00-08 | Peer |
| 01-80-C2-00-00-09 | Peer |
| 01-80-C2-00-00-0A | Peer |
| 01-80-C2-00-00-0B | Peer |
| 01-80-C2-00-00-0C | Peer |
| 01-80-C2-00-00-0D | Peer |
| 01-80-C2-00-00-0E | Peer |
| 01-80-C2-00-00-0F | Peer |
| 01-80-C2-00-00-10 | Forward |
| 01-80-C2-00-00-20 | Forward |
| 01-80-C2-00-00-21 | Forward |
| 01-80-C2-00-00-22 | Forward |
| 01-80-C2-00-00-23 | Forward |
| 01-80-C2-00-00-24 | Forward |

**DMAC:** The destination MAC address. The MAC DA range for Bridge block of protocol is 01-80-C2-00-00-00 through 01-80-C2-00-00-0F and for GARP block of protocol is 01-80-C2-00-00-20 through 01-80-C2-00-00-2F.

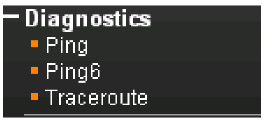
**L2CP Mode:** Select the L2CP frame handling mode for the corresponding destination MAC address (DMAC).

**Peer:** Redirect to CPU to allow peering/tunneling/discard depending on ECE and protocol configuration.

**Forward:** Allow peering/forwarding/tunneling/discarding depending on ECE and protocol configuration.

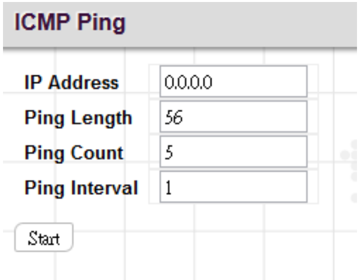
## 4.24 Diagnostics

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




### *4.24.1 Ping*

This Ping function is for ICMPv4 packets.




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

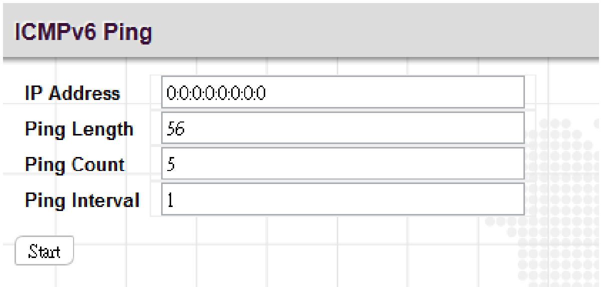
**Ping Length:** The size or length of echo packets.

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

**Ping Interval:** The time interval between each ping request.

### *4.24.2 Ping6*

This Ping function is for ICMPv6 packets.



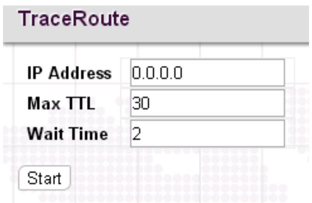

**IP Address:** Enter the IP address that you wish to ping.

**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.

### *4.24.3 Traceroute*



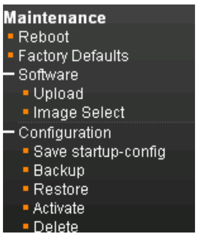

**IP Address:** Specify the destination IP address for traceroute.

**MAX TTL:** Specify the maximum number of hops (max time-to-live value) traceroute will probe. Values range from 1 to 255. The default is 30.

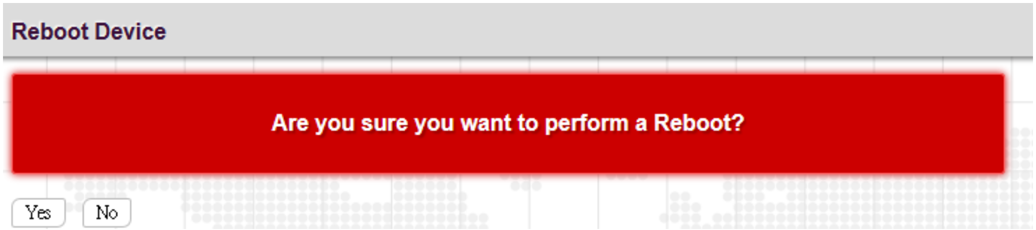
**Wait Time:** Set the time (in seconds) to wait for a response to a probe (default 2 seconds). Values range from 1 to 60.

## 4.25 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.

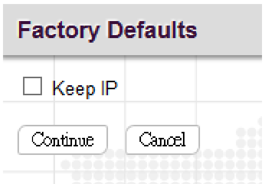



### 4.25.1 Reboot




Click "Yes" button to reboot the switch.

### 4.25.2 Factory Defaults

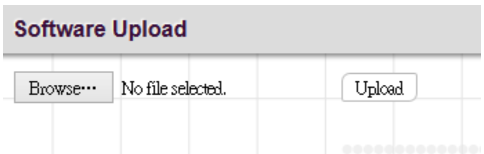



**Keep IP:** Check the "Keep IP" box if you want to use the current IP settings after restoring to factory default settings.

Click "Continue" 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.

### 4.25.3 Software

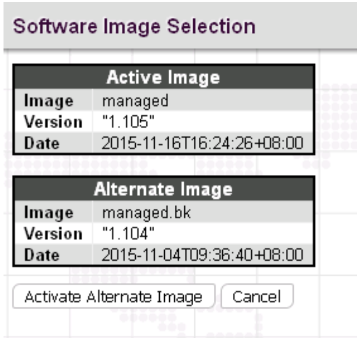
#### 4.25.3.1 Upload




Update the latest Firmware file.

Select a Firmware file (this file should have ".dat" extension name) from your local device and then click "Upload" to start updating. The upload process will take about 5 minutes. After the Firmware file has been successfully uploaded to the switch, the switch will use the new Firmware file and reboot the switch to activate settings.

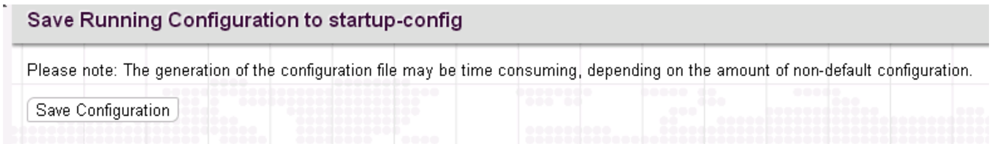
#### 4.25.3.2 Image Select




Select the image file to be used in this device.

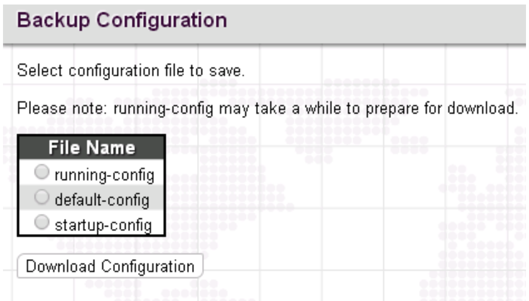
### 4.25.4 Configuration

#### 4.25.4.1 Save startup-config




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

#### 4.25.4.2 Backup

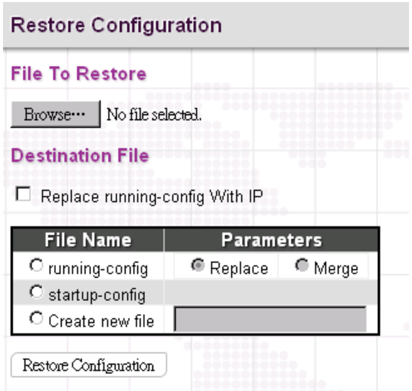



**running-config:** Download a copy of the current running configurations to your local device.

**default-config:** Download a copy of the factory default configurations to your local device.

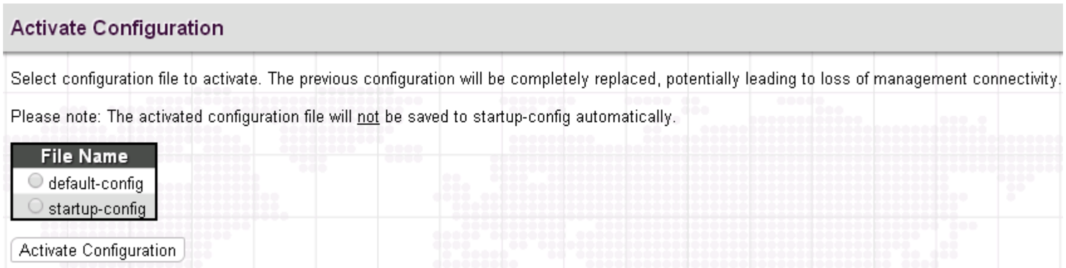
**startup-config**: Download a copy of startup configurations to your local device.

### 4.25.4.3 Restore



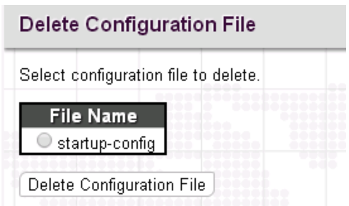

Select a file and then click “Upload Configuration” to start uploading the file.

### 4.25.4.4 Activate




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

### 4.25.4.5 Delete




Select the file that you would like to delete. Click on the “Delete Configuration File” to remove the file from the device.

# APPENDIX A. u-Ring CONFIGURATION PROCEDURE

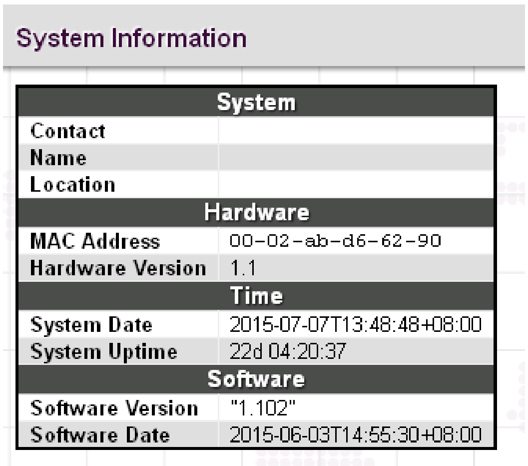
## Introduction

u-Ring is a proprietary redundancy protocol that supports 250 units in a ring topology and can bring redundant paths into service within 10 ms when link failures occur. Compared with spanning tree protocol, u-Ring achieves faster recovery time on the network and is more flexible and scalable in network architecture. u-Ring redundancy protocol can automatically self identifies the ring Master (the user-defined Master is also supported) and then block a port resided in Master device for backup purposes. Once the disconnection is detected on the network, u-Ring can bring backup ports back into “forwarding” mode so that the disconnected path can keep contact with the whole network.

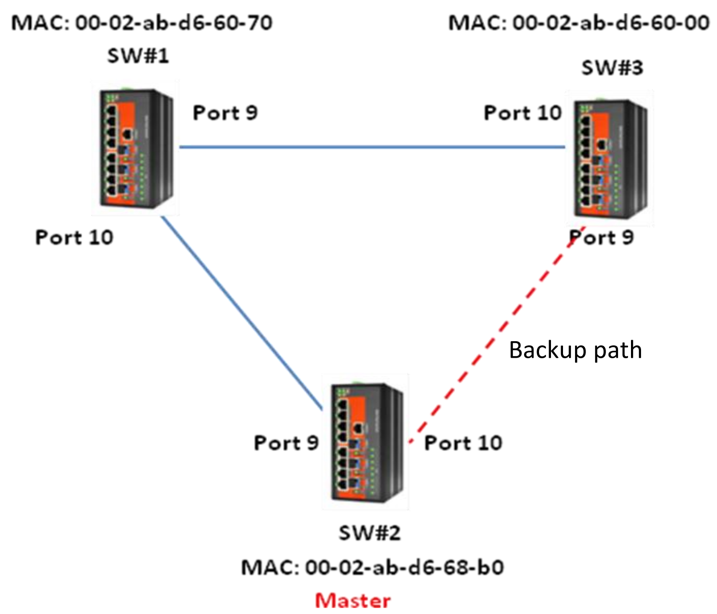
The purpose of this document is to give valuable aid to a network engineer in topology design, deployment and configuration of Industrial Grade Ethernet Switches for ring protection. The example uses a ring of three units and performs all configurations via the web GUI management interface.

## Equipment Used in this Example:

1. The Industrial Grade Ethernet Switches with u-Ring redundancy protocol * 3
2. Laptop * 1



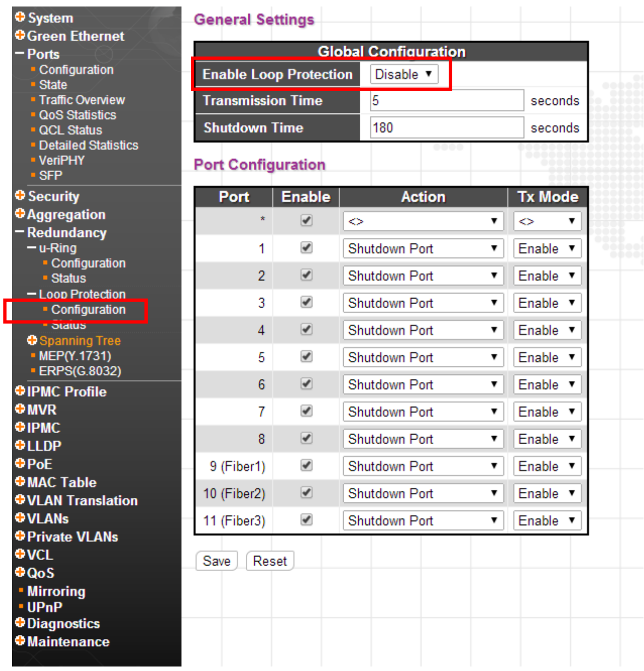
## Testing Topology:

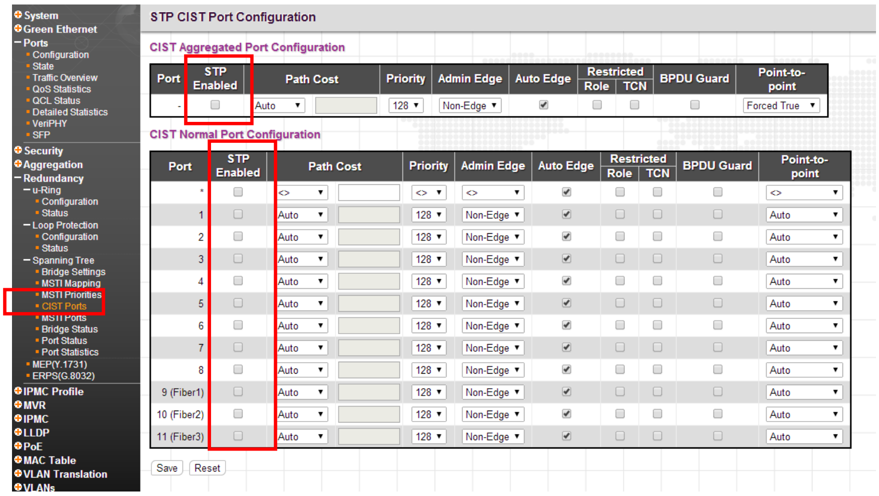


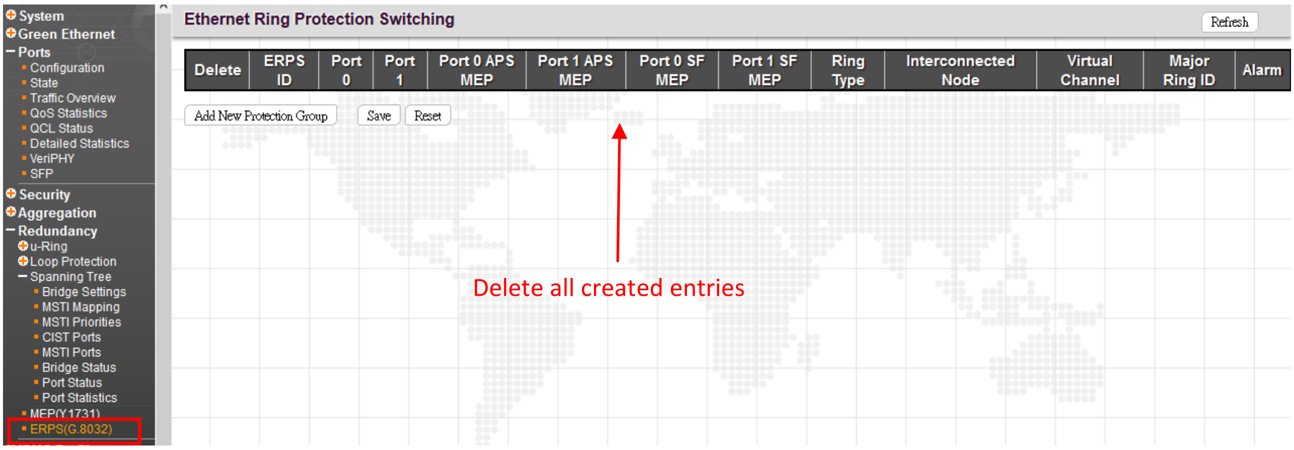

***Warning: During initial configuration and in order to avoid an Ethernet "Loop" condition, please do not connect the physical Ring prior to completion of the u-Ring configuration.***

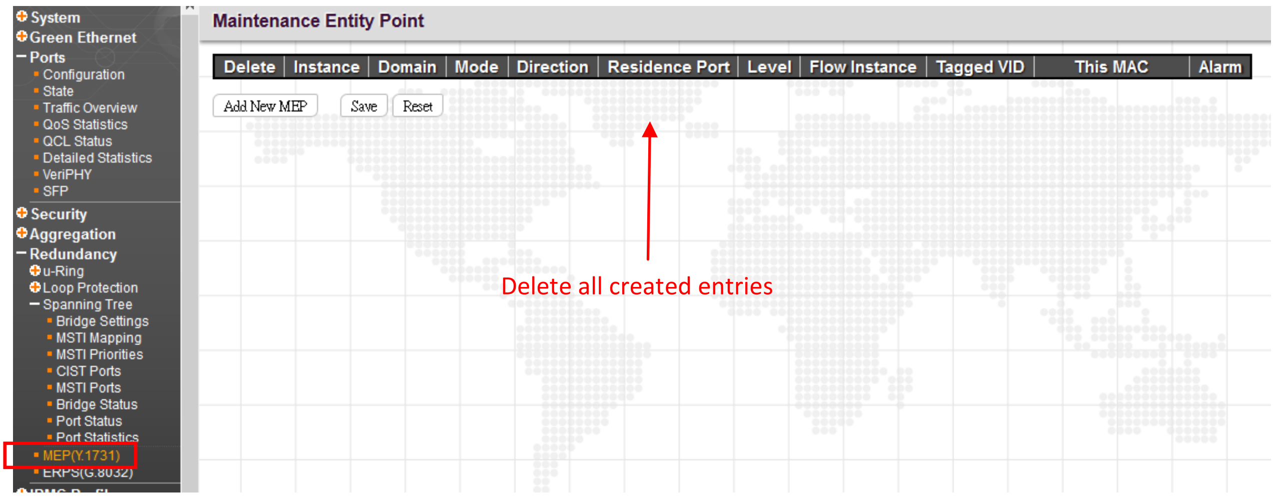
## <u>Configuration:</u>

**A. Make sure SW#1, SW#2, SW#3's Loop Protection, STP, ERPS and MEP configurations are all disabled.**



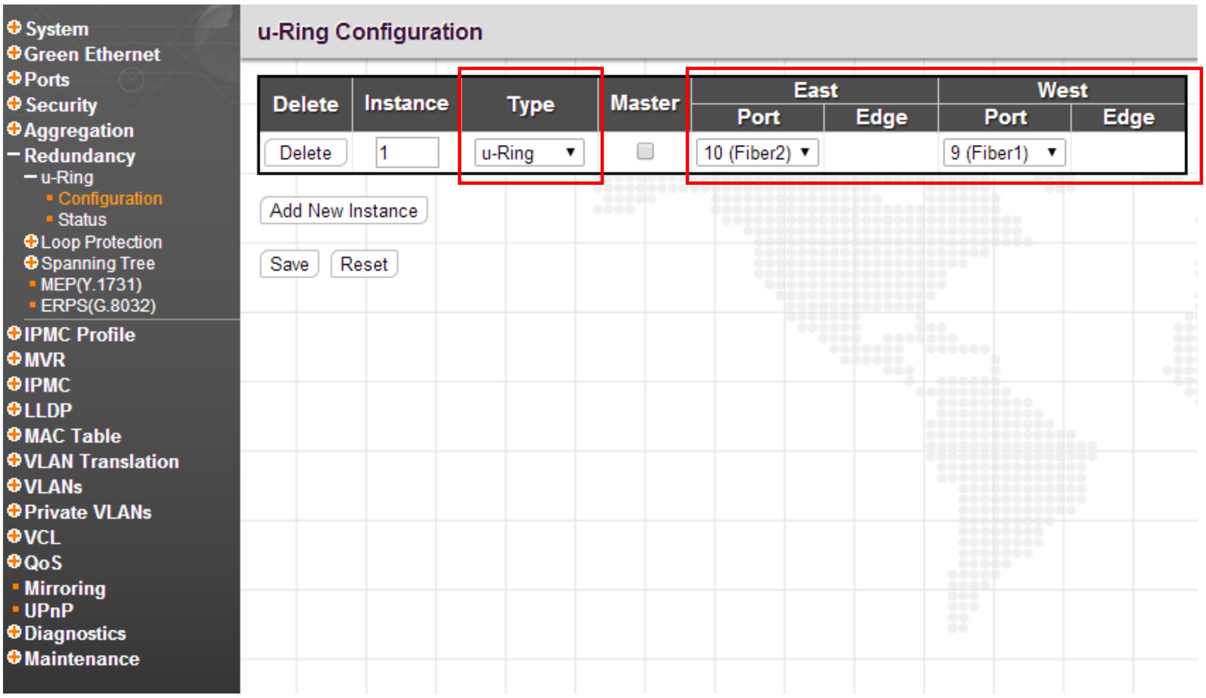


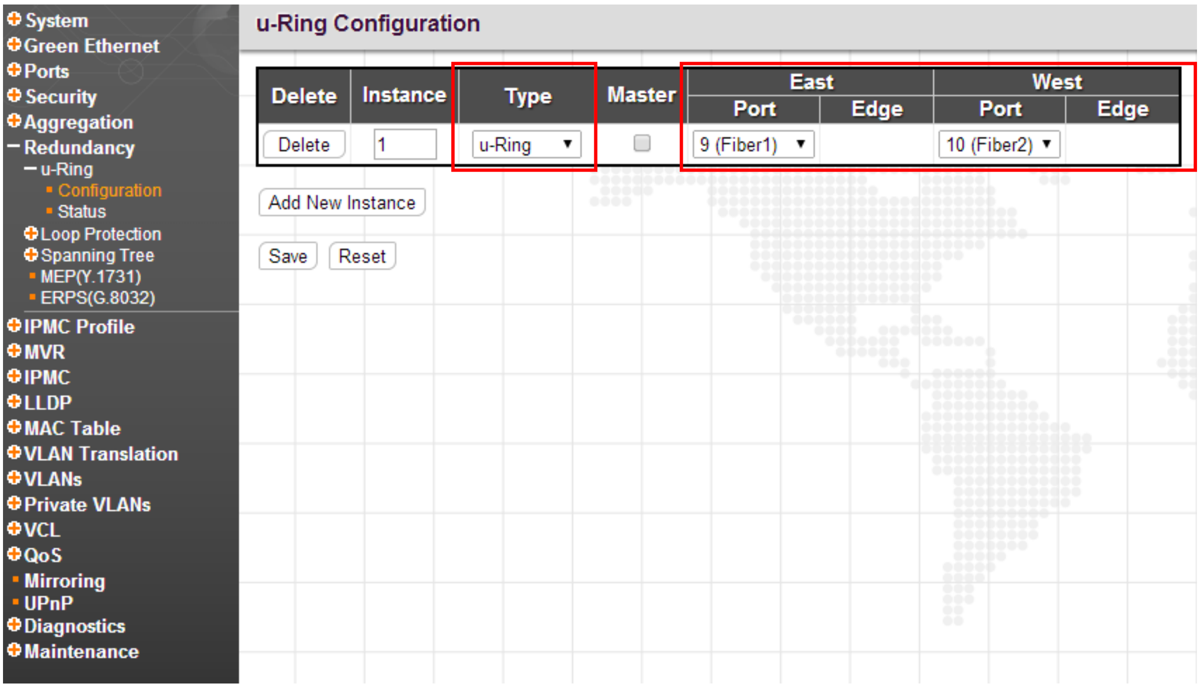




## B. Add a new Instance in Redundancy>u-Ring>Configuration page

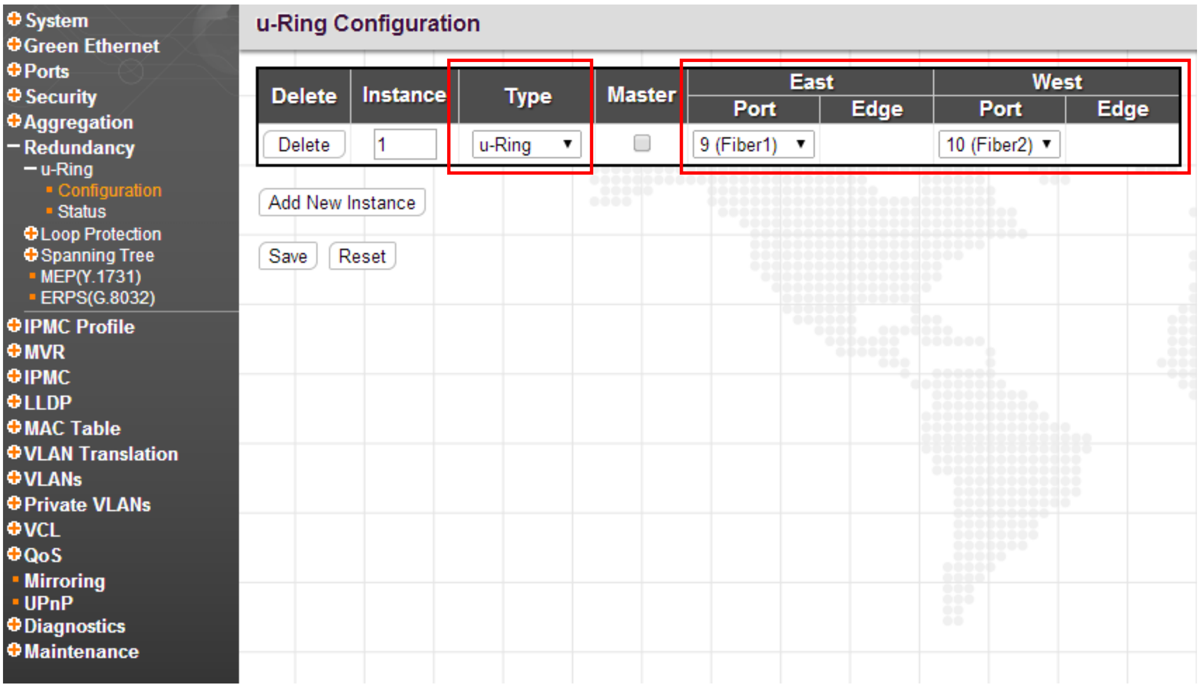
SW#1: Select “u-Ring” type and select East port (10 Fiber 2) and West port (9 Fiber1) from the pull-down menu. Then click “Save” button.




SW#2: Select “u-Ring” type and select East port (9 Fiber1) and West port (10 Fiber2) from the pull-down menu. Then click “Save” button.




SW#3: Select “u-Ring” type and select East port (9 Fiber1) and West port (10 Fiber2) from the pull-down menu. Then click “Save” button.



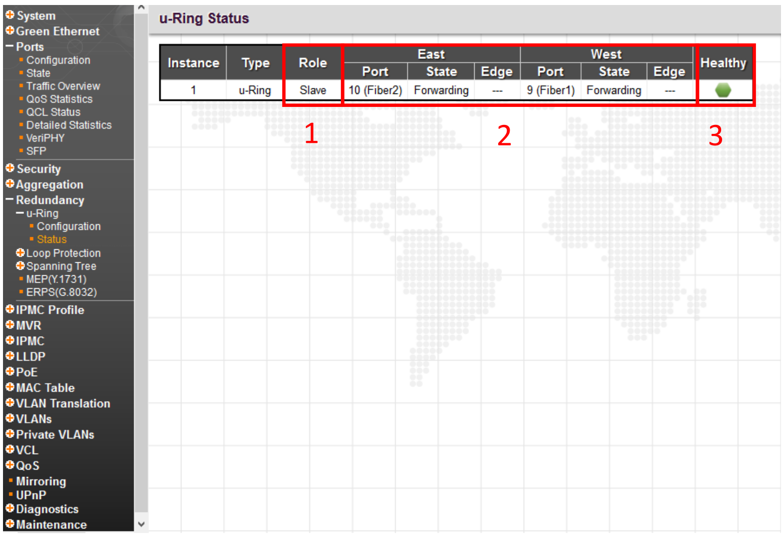

**C. Connect the physical ring. Once cabling is connected correctly, u-Ring starts working.**

## Verification:

There are three ways to verify the configured settings. The first one is to check link status via Satus page. Second, using ping to test the connectivity between switches. Finally, disconnect a port to see whether the blocked port is brought back to “Forwarding” mode or not.

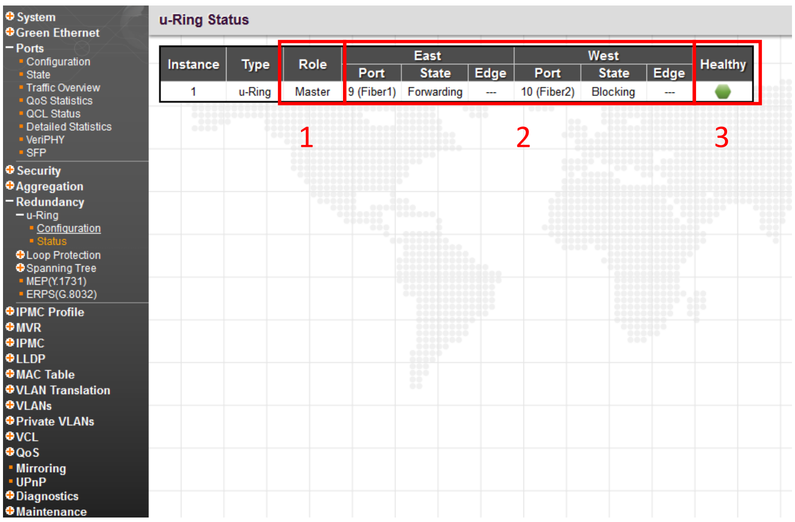
**A. Check the Redundancy>u-Ring>status page of each device.**

SW#1



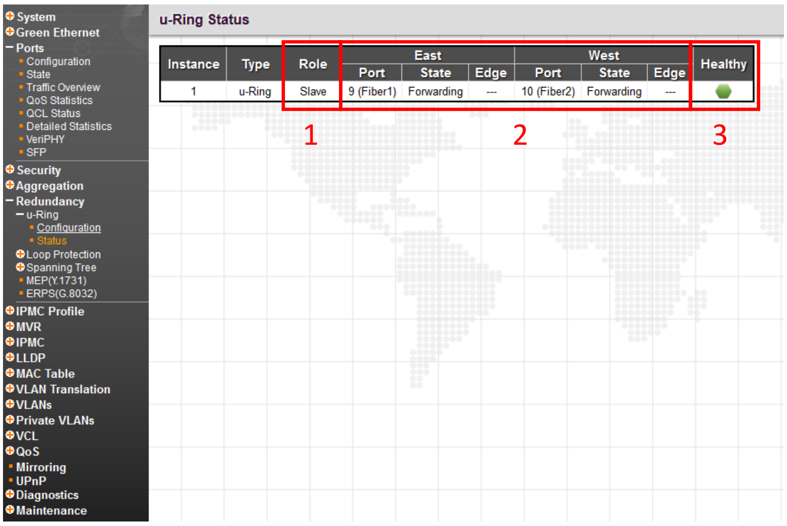

1. The role of SW#1 is “Slave” which means that East and West port will not be blocked (forward data).
2. East and West port are “Forwarding” data.
3. The “Green” color means that the ring connection is good.

SW#2



1. SW#2 has the biggest MAC address among switches in the ring. Therefore, it is elected as the “Master” which means that one of the connected ports will be blocked.
2. East port (9 Fiber1) forwards data. West port (10 Fiber2) is blocked because it has higher port number than East port.
3. The “Green” color means that the ring connection is good.

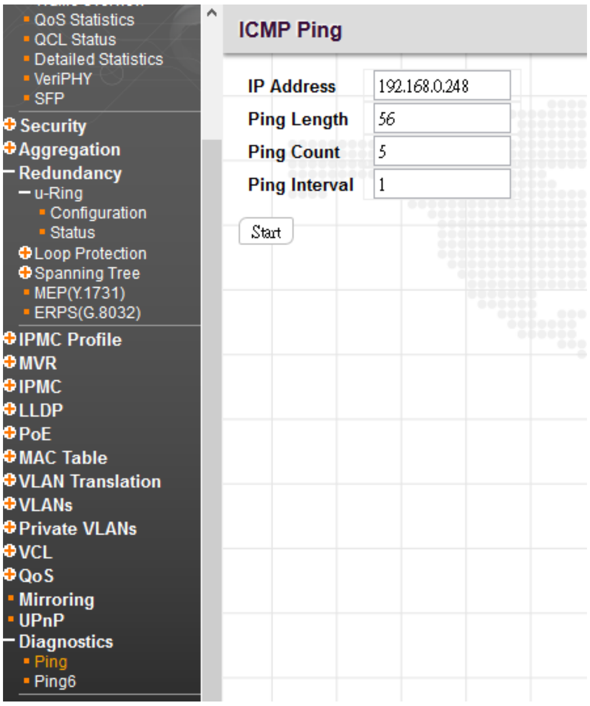
SW#3

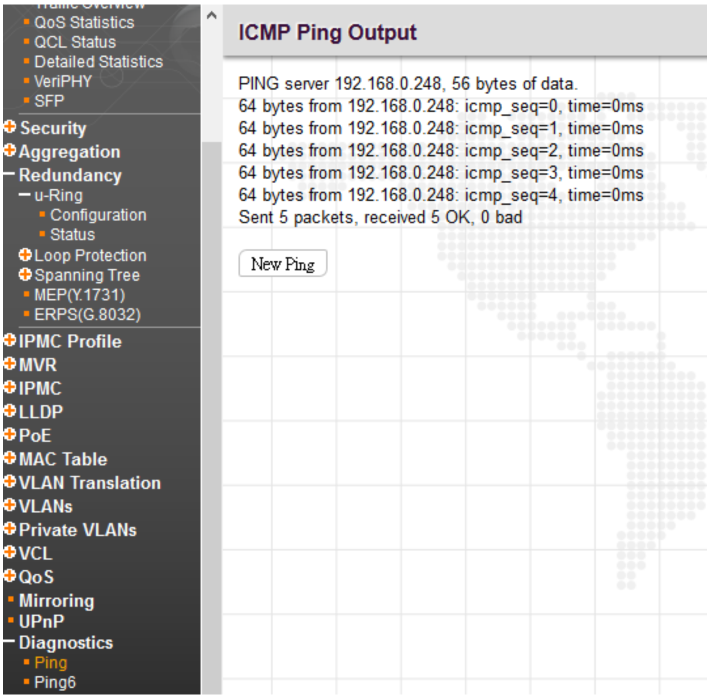



1. The role of SW#3 is “Slave” which means that East and West port will not be blocked (forward data).
2. East and West port are “Forwarding” data.
3. The “Green” color means that the ring connection is good.

**B. Using Ping to test the connectivity between Switches.**

Go to Diagnostics>Ping page.



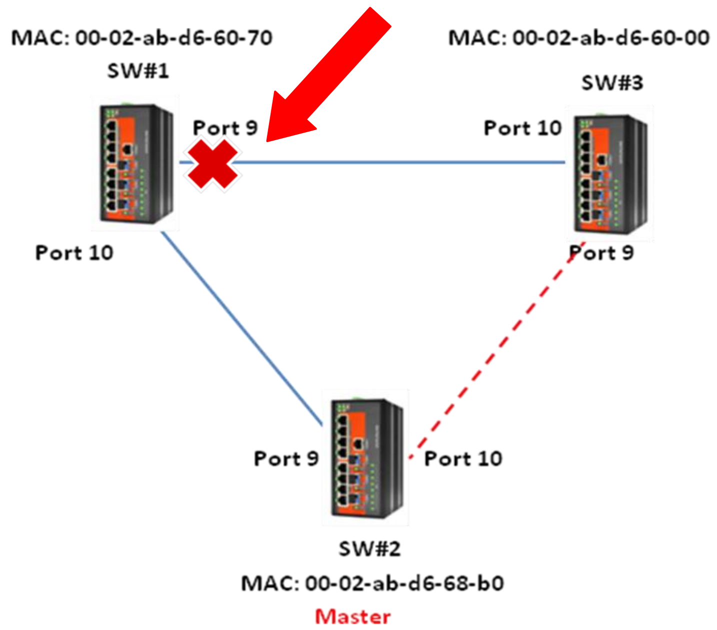




If one of the switches cannot ping the other switch, please check that you have correct cabling and configurations including IP assignment, u-Ring configuration.

**C. Disconnect a port to see whether the status of blocked port in SW#2 (Port 10) changes to "Forwarding" or not.**

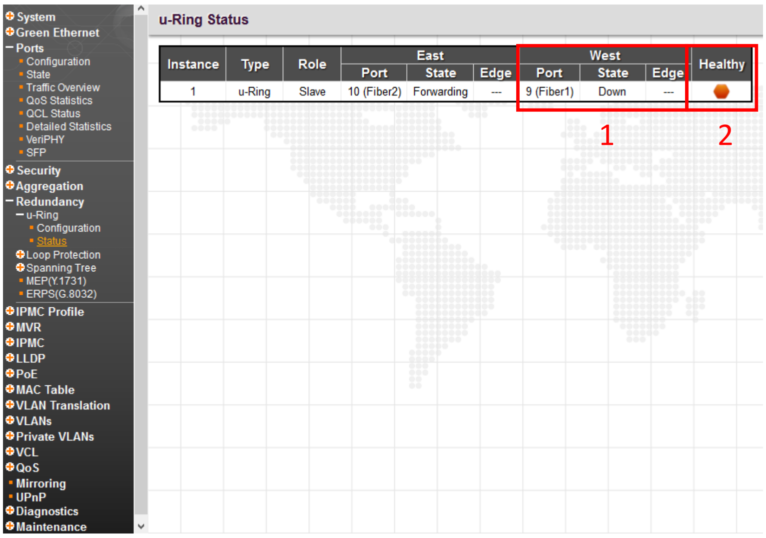
1. Manually disconnect Port 9 in SW#1.

Manually disconnect Port 9 in SW#1.



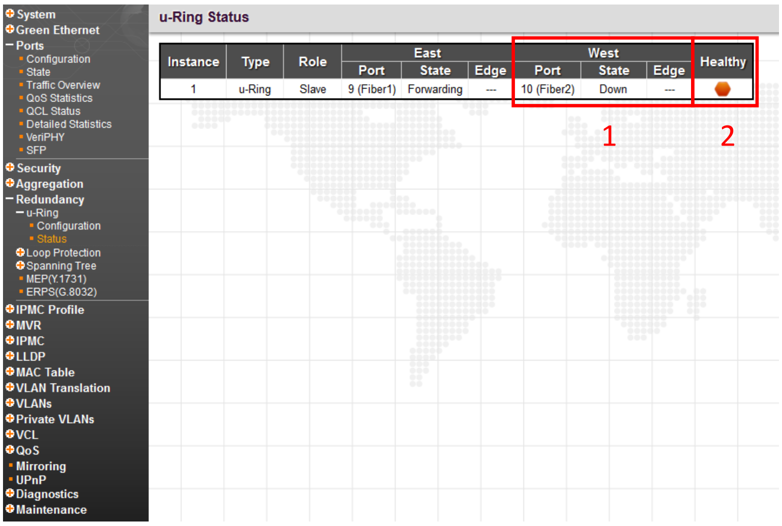

2. The status of SW#1 Port 9 and SW#3 Port 10 is down.

SW#1



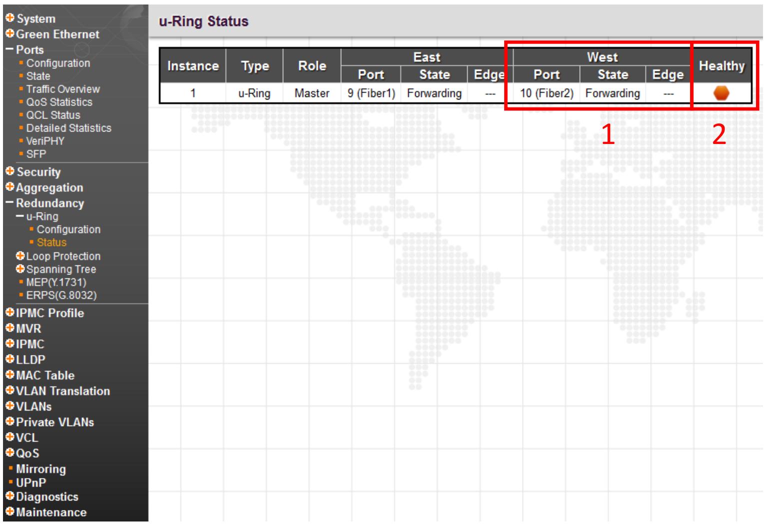

1. The status of port 9 is down.
2. The “Red” alarm color means that there is something wrong with the ring (This may result from physical disconnection).

SW#3




1. The status of port 10 is down.
2. The “Red” alarm color means that there is something wrong with the ring (This may result from physical disconnection).

SW#2




1. The status of Port 10 changes from “Blocking” to “Forwarding”.
2. The “Red” alarm color means that there is something wrong with the ring (This may result from physical disconnection).

# APPENDIX B. G.8032 CONFIGURATION PROCEDURE

## Abstract:

ERPS (Ethernet Ring Protection Switching), is an effort at ITU-T under G.8032 Recommendation to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer.

In ERPS there is a central node called RPL (Ring Protection Link) Owner Node which blocks one of the ports to ensure that there is no loop formed for the Ethernet traffic. The link blocked by the RPL owner node is called the Ring Protection Link or RPL. The node at the other end of the RPL is known as RPL Neighbor Node. ERPS uses R-APS (Automatic Protection Switching) control messages to coordinate the activities of switching on/off the RPL link.

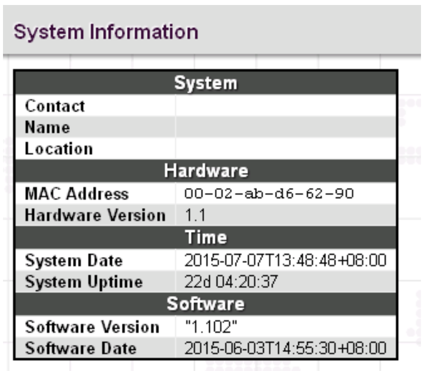
Any failure along the ring triggers a R-APS(SF) (R-APS signal fail) message along both directions from the nodes adjacent to the failed link after these nodes have blocked the port facing the failed link. On obtaining this message, RPL owner unblocks the RPL port.

## Introduction:

The purpose of this document is to give valuable aid to a network engineer in topology design, deployment and configuration of Industrial Grade Ethernet Switches for ring protection with sub-50ms recovery time. The example uses a ring of three units and performs all configurations via the web GUI management interface.

## Equipment Used in this Example:

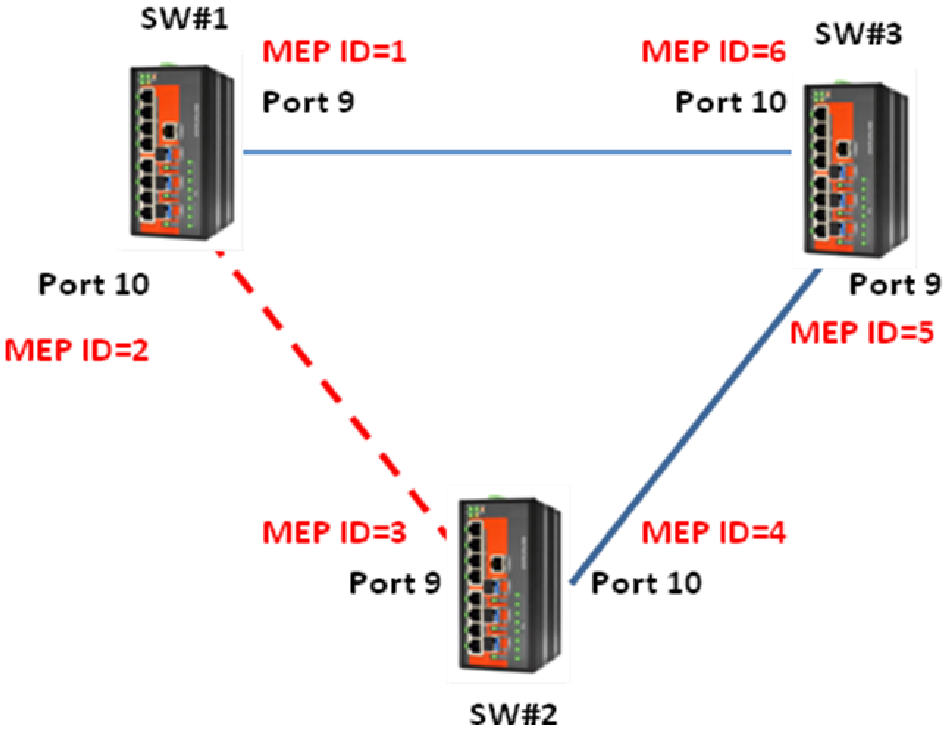
1. The Industrial Grade Ethernet Switches with G.8032 function * 3
2. Software Version 1.1 or above
3. Laptop * 1



System Information

| System | |
|---|---|
| Contact | |
| Name | |
| Location | |
| **Hardware** | |
| MAC Address | 00-02-ab-d6-62-90 |
| Hardware Version | 1.1 |
| **Time** | |
| System Date | 2015-07-07T13:48:48+08:00 |
| System Uptime | 22d 04:20:37 |
| **Software** | |
| Software Version | "1.102" |
| Software Date | 2015-06-03T14:55:30+08:00 |

## Testing Topology:




<Figure 1>

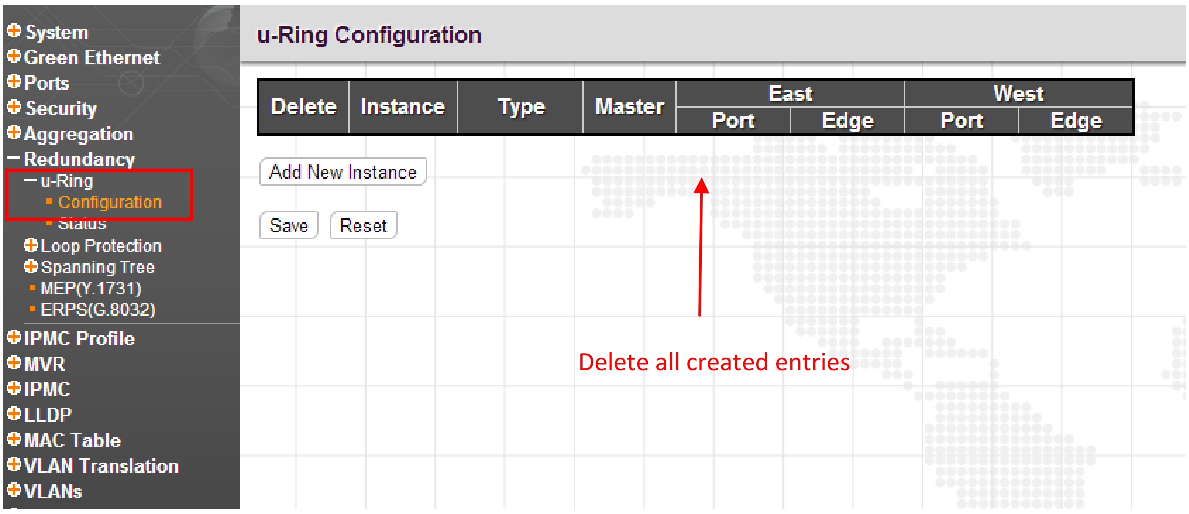
***Warning:***

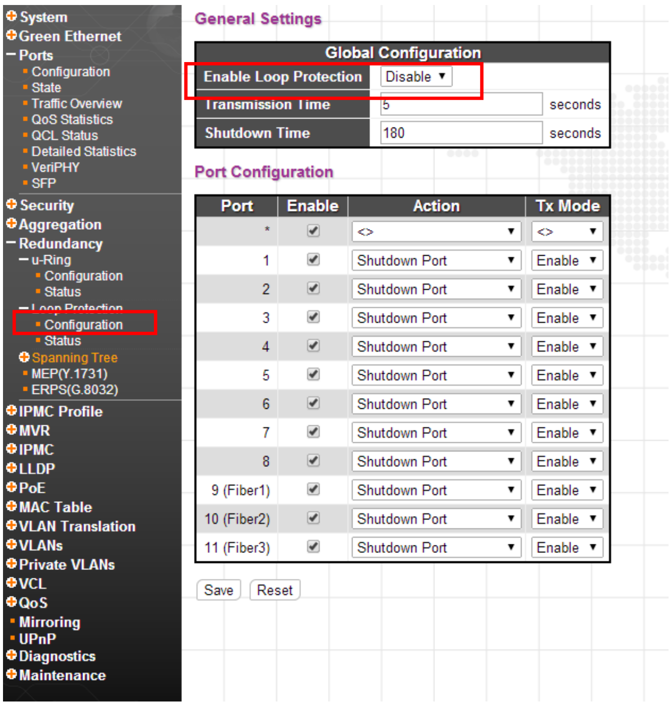
1. ***Please design your network topology and physical links first. Since G.8032 syncs with neighbor switch's MAC address (Peer to peer), it is important to make sure your physical connections are in correct locations and that they are not arbitrarily changed.***
2. ***During initial configuration and in order to avoid an Ethernet "Loop" condition, please do not connect the physical Ring prior to completion of the G.8032 configuration.***

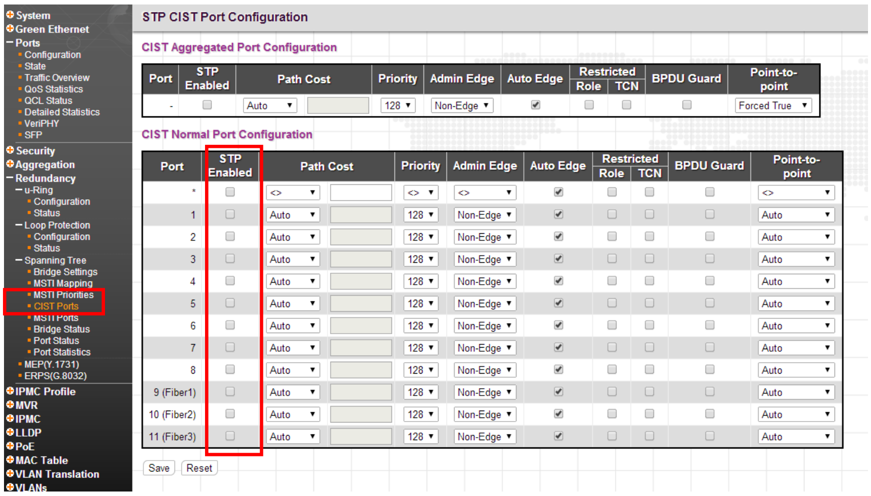
# MEP & VLAN configuration

## Configuration of SW#1:

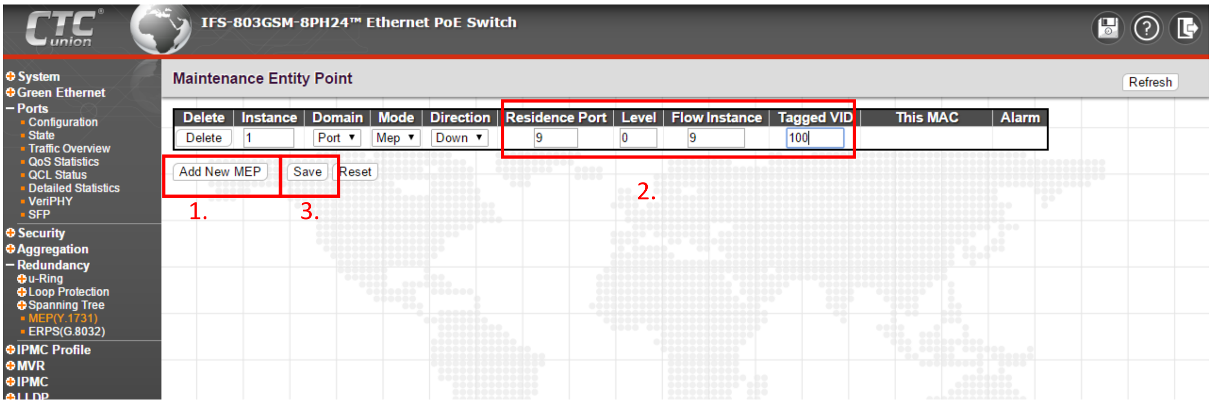
**A. Make sure SW#1's u-Ring, Loop Protection and STP configurations are all disabled.**



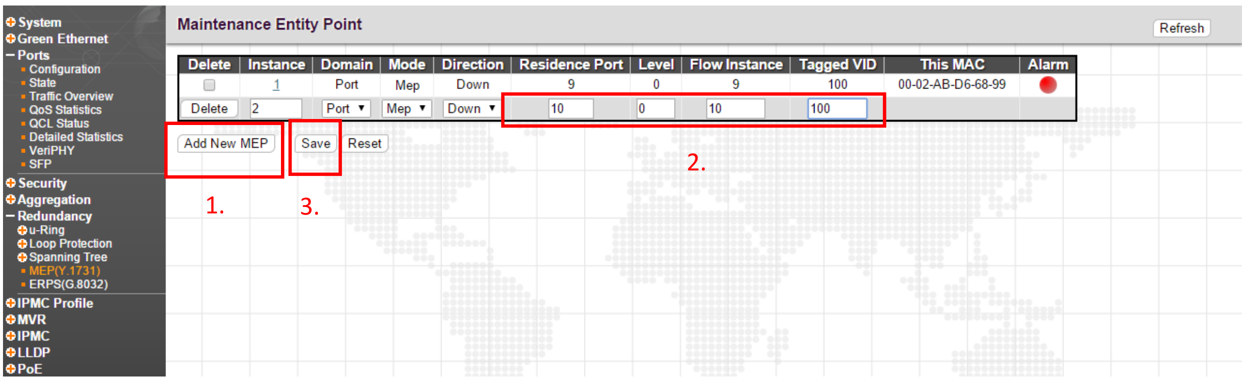





**B. Configure MEP (Maintenance associated End Point) on SW#1**



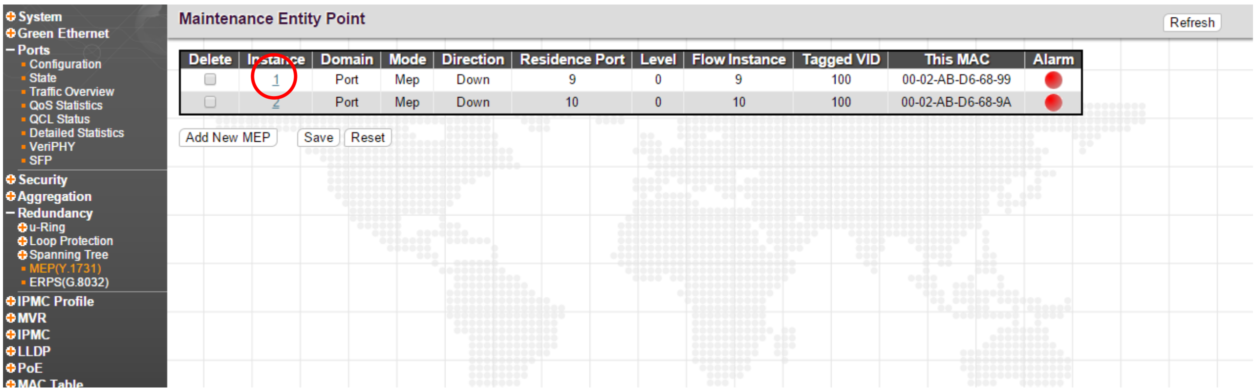
1. Click "Add New MEP"
2. Enter port 9 (Fiber 1) into "Residence Port" and "Flow Instance" and set VID to 100 (user defined, we will use 100 here and throughout)
3. Click "Save"

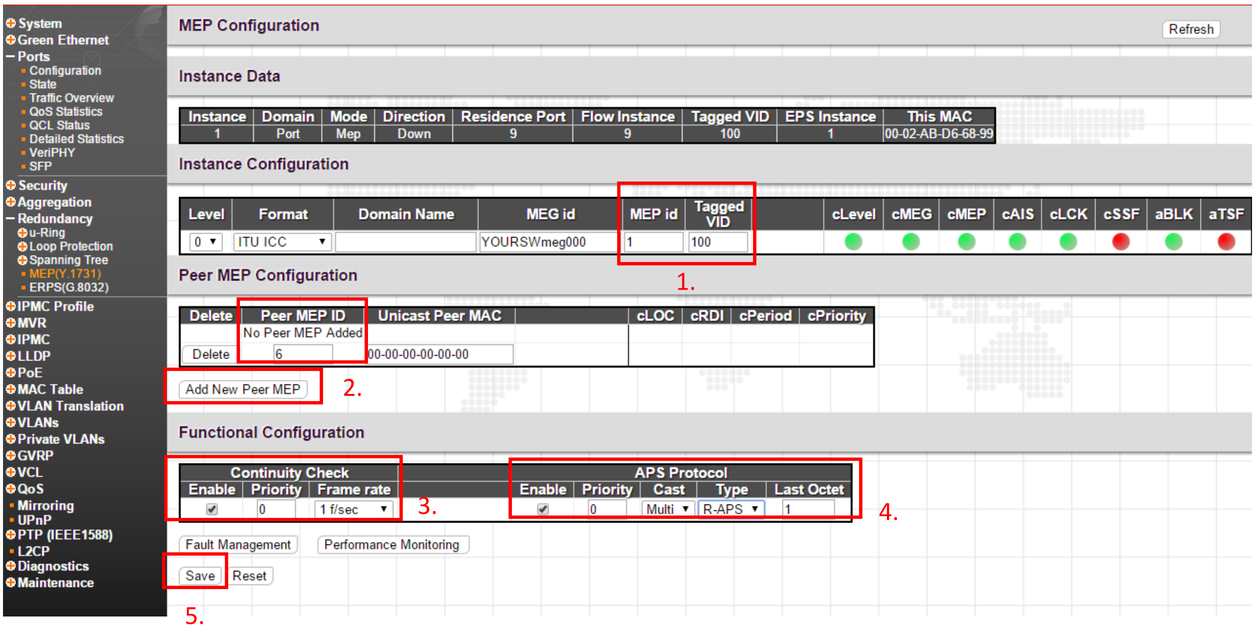


1. Click "Add New MEP"
2. Enter port 10 (Fiber 2) into "Residence Port" and "Flow Instance" and set VID to 100 (user defined, we will use 100 here and throughout)
3. Click "Save"

***NOTE:*** *All switches must use the same VID.*

## C. Click "Instance 1 " to configure detailed setting of MEP



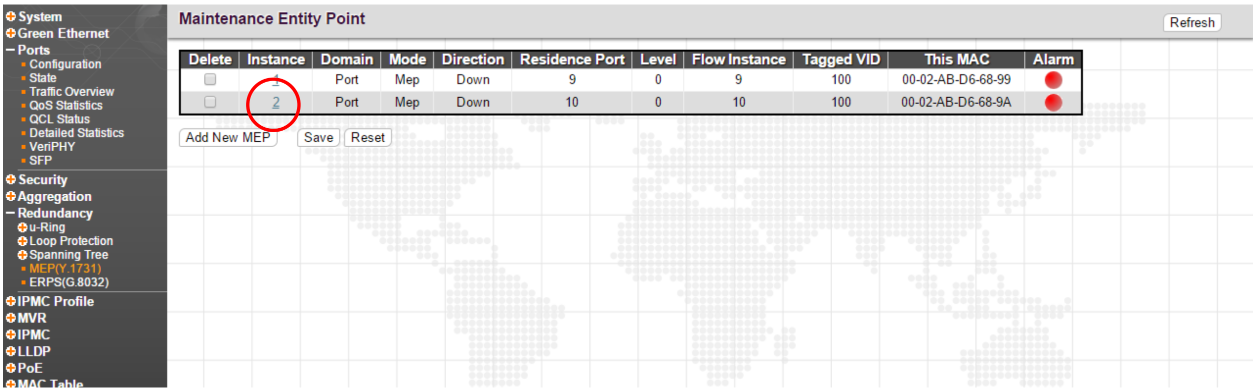



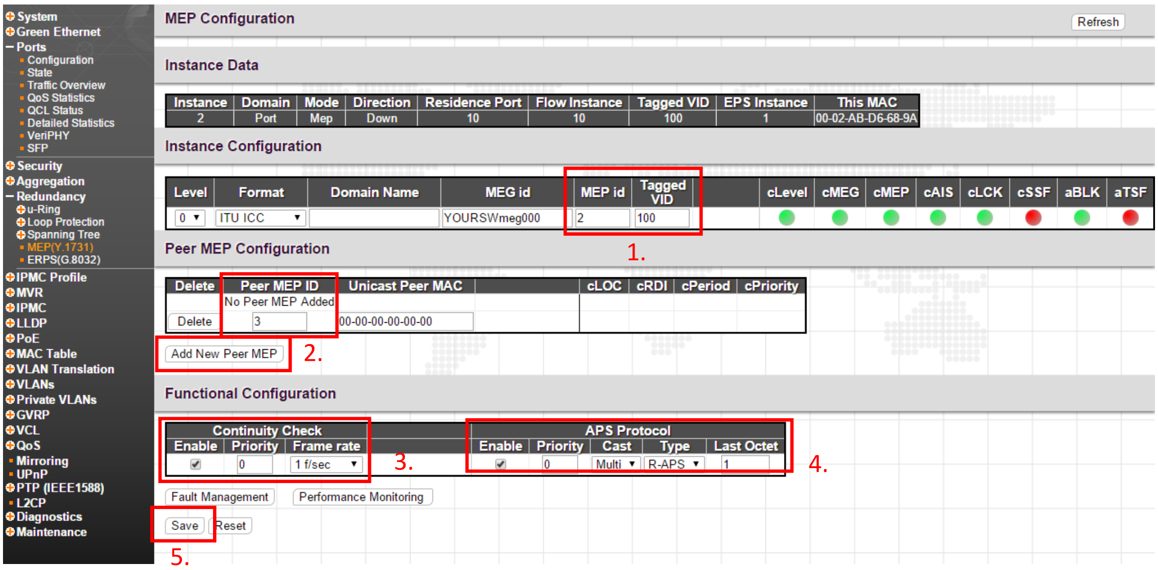

1. Set the first MEP ID to "1" and make sure Tagged VID matches our set VID (100 here)
2. Click "Add New Peer MEP" and enter the peer's ID which is "6" in our topology example
3. Enable Continuity Check and leave "Frame rate" at 1 f/sec
4. Enable the APS Protocol, with "Multicasting" and type "R-APS"
5. Click "Save"

***NOTE:***

*The MEP ID (1) here is for Port 9 of SW#1.*
*And Peer MEP ID (6) is the neighbor port 10 of SW#3.*
*Always refer back to your design topology as in < Figure 1>.*

## D. Click "Instance 2 " to configure further setting of MEP for port 10



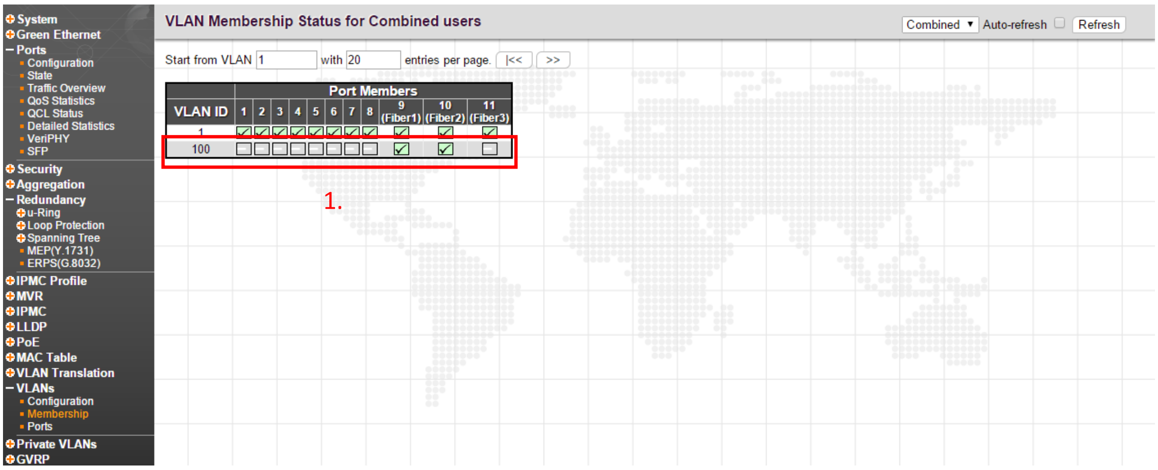




1. Set the second port MEP ID to "2" and make sure Tagged VID matches our set VID (100 here)
2. Click "Add New Peer MEP" and enter the peer's ID which is "3" in our topology example
3. Enable Continuity Check and leave "Frame rate" at 1 f/sec
4. Enable the APS Protocol, with "Multicasting" and type "R-APS"
5. Click "Save"

***NOTE:***

*The MEP ID (2) here is for Port 10 of SW#1*
*And Peer MEP ID (3) is the neighbor port 9 of SW#2.*
*Always refer back to your design topology as in < Figure 1>.*

### E. Check VLAN Membership Table

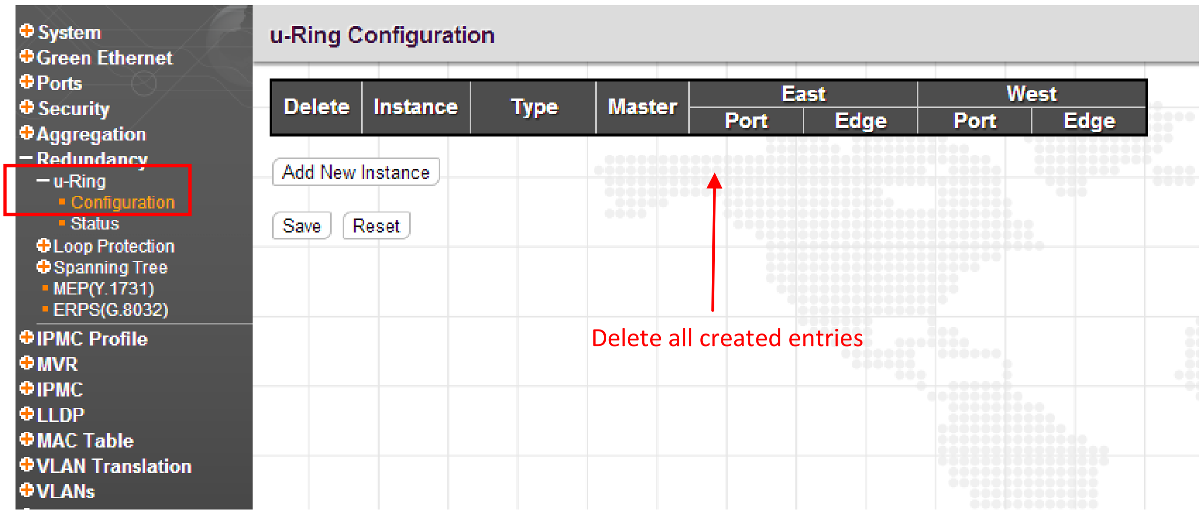


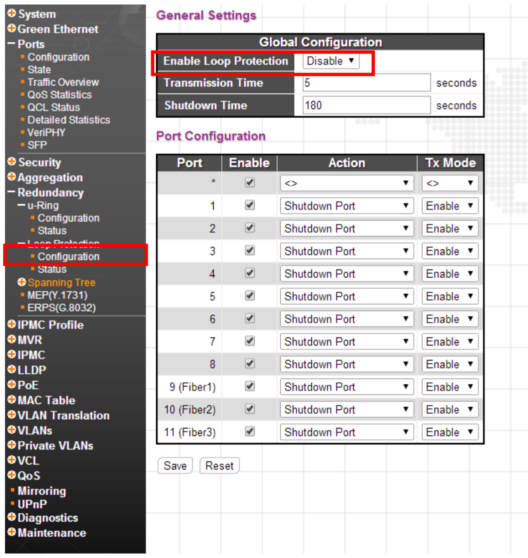

1. When MEP instances are created, an entry of VLAN membership associated with MEP configuration will be established automatically in VLAN Membership Table. Hence, you do not manually create this VLAN entry. In this example, VLAN ID 100 entry with port 9 & 10 as members is created dynamically.

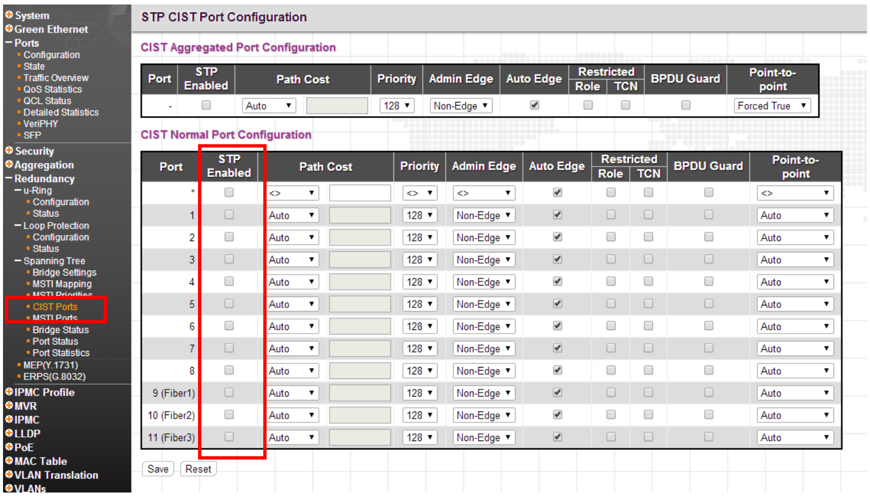
***NOTE:***
*When MEP instances are deleted, VLAN membership associated with MEP configuration will also be deleted automatically.*

## <u>Configuration of SW#2</u>

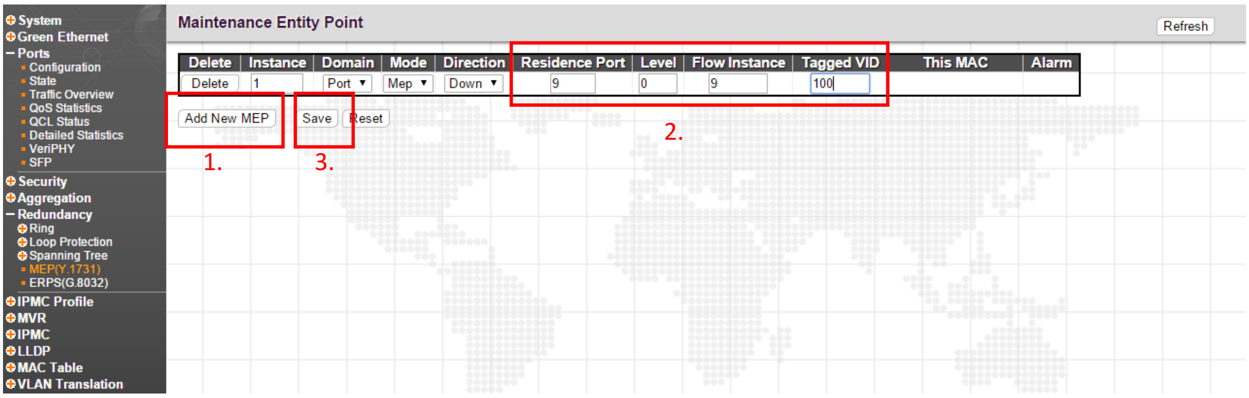
**A. Use the same configuration process as SW#1, make sure SW#2's u-Ring, Loop Protection and STP configurations are all disabled.**

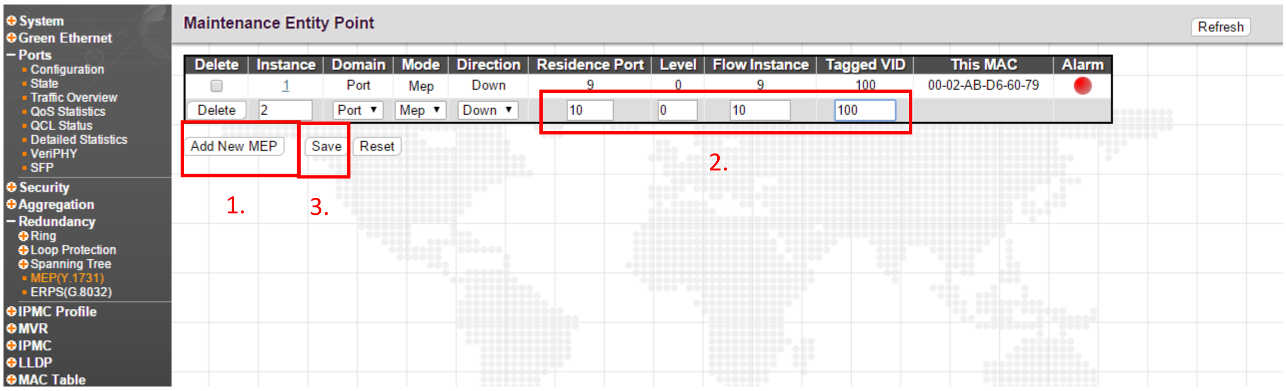




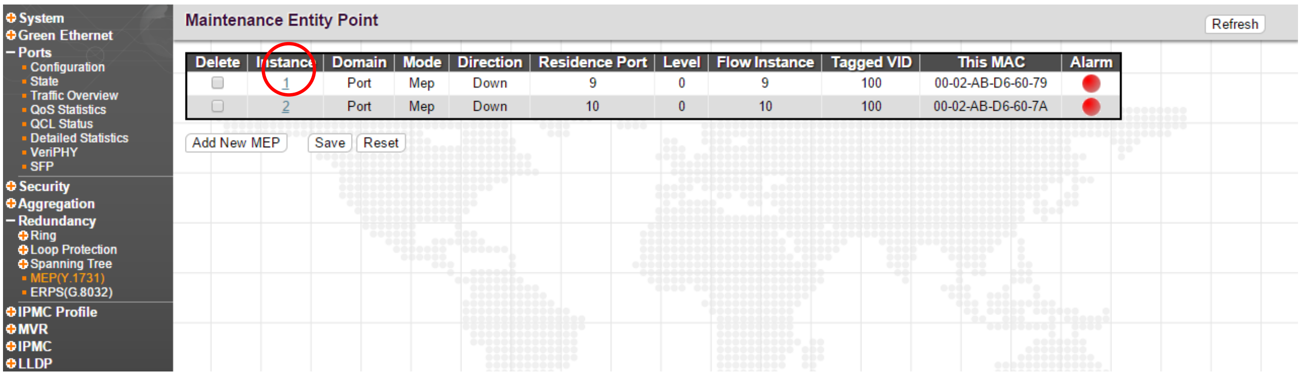



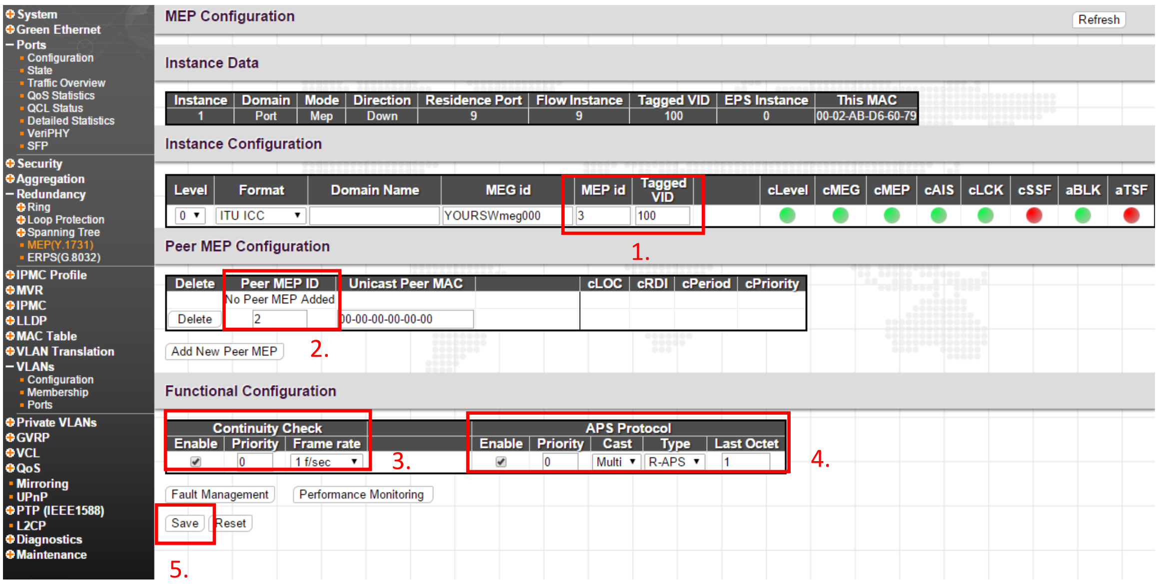

## B. Configure MEP on SW#2






## C. Click "Instance 1 " to configure further setting of MEP

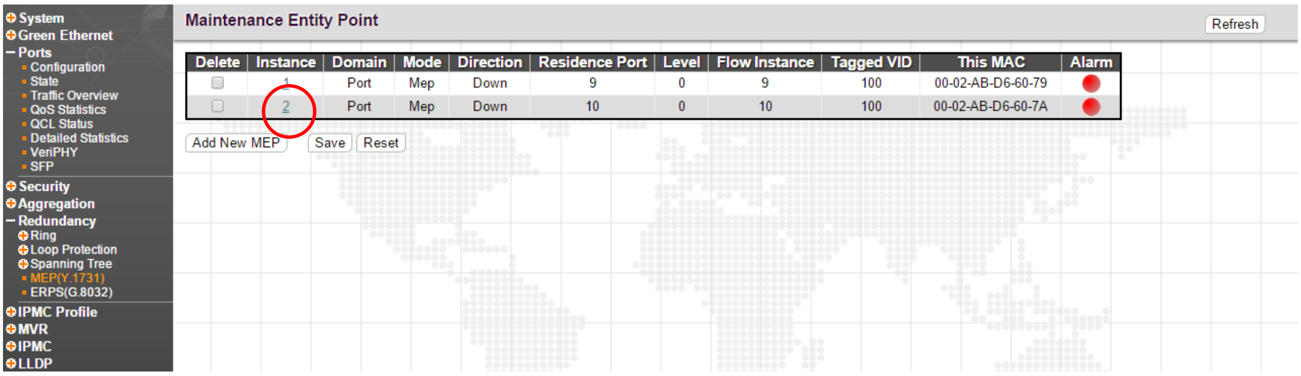


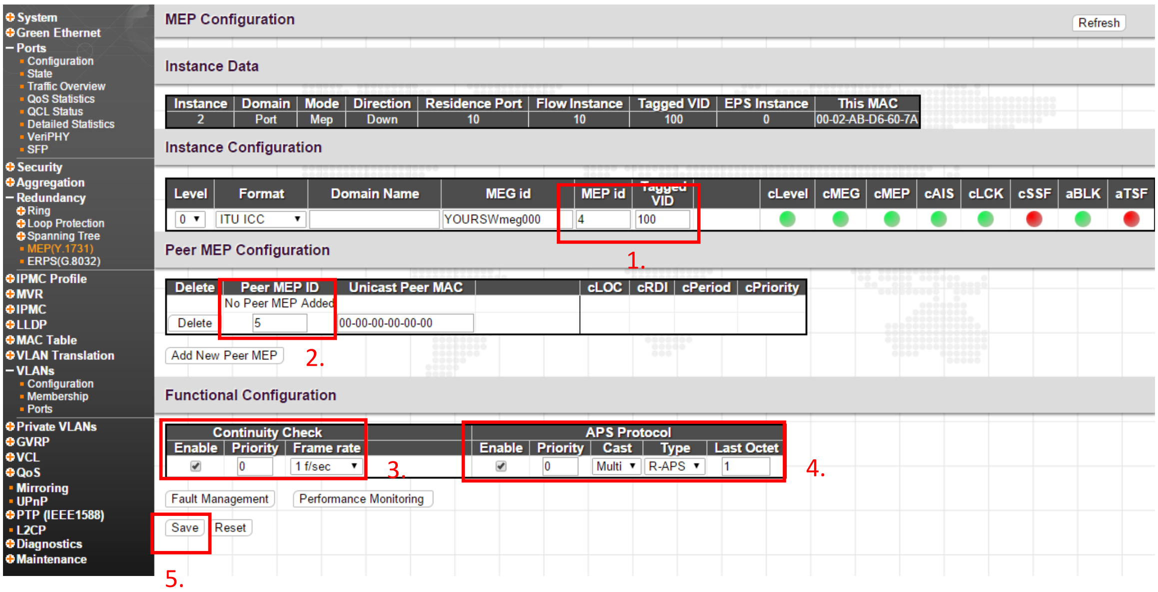




**NOTE:**

*The MEP ID (3) here is for Port 9 of SW#2*
*And Peer MEP ID (2) is the neighbor port 10 of SW#1.*
*Always refer back to your design topology as in < Figure 1>.*

**D. Click "Instance 2 " to configure further setting of MEP**



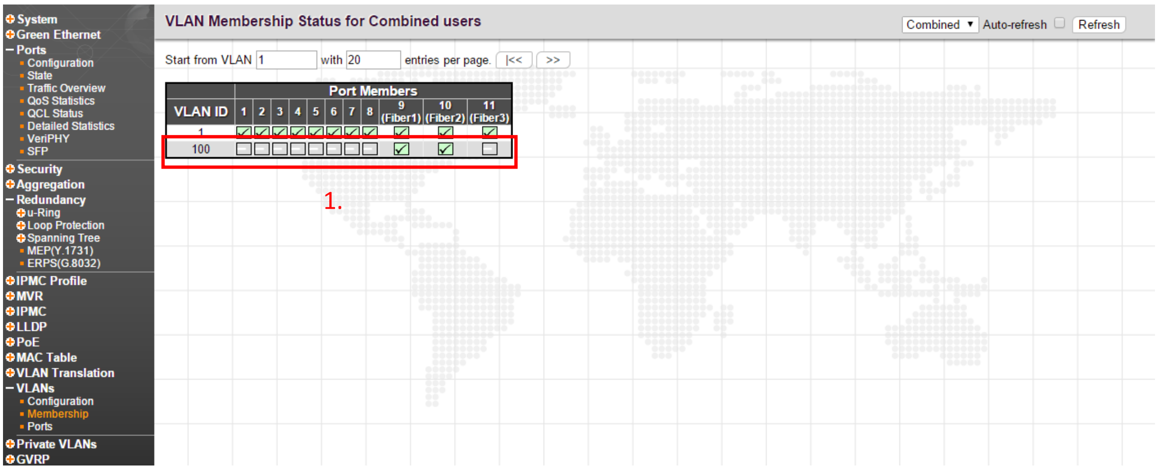

***NOTE:***

*The MEP ID (4) here is for Port 10 of SW#2*

*And Peer MEP ID (5) is the neighbor port 9 of SW#3.*

*Always refer back to your design topology as in < Figure 1>.*

## E. Check VLAN Membership Table

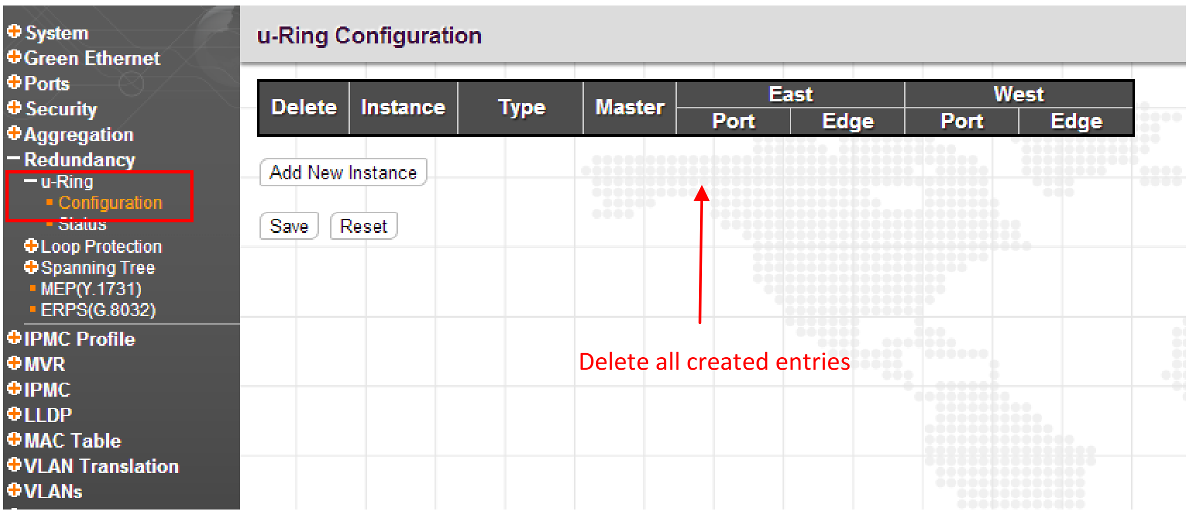


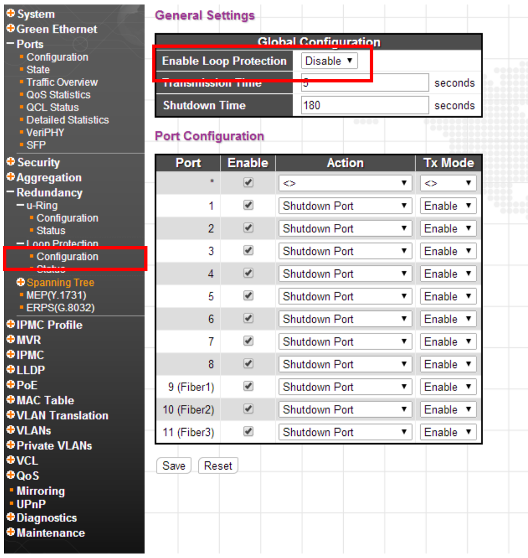

1. When MEP instances are created, an entry of VLAN membership associated with MEP configuration will be established automatically in VLAN Membership Table. Hence, you do not manually create this VLAN entry. In this example, VLAN ID 100 entry with port 9 & 10 as members is created dynamically.

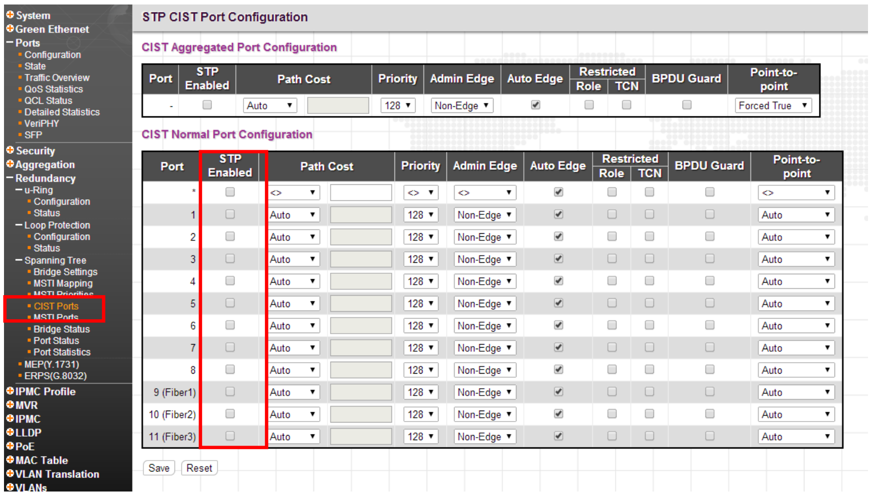
***NOTE:***
*When MEP instances are deleted, VLAN membership associated with MEP configuration will also be deleted automatically.*

## Configuration of SW#3

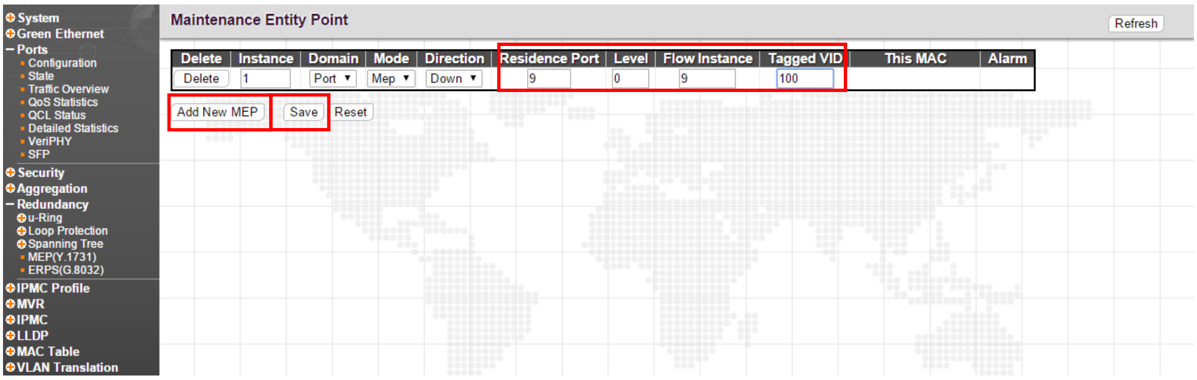
**A. Same configuration process as SW#1 & SW#2, make sure SW#3's u-Ring, Loop Protection and STP configurations are all disabled.**

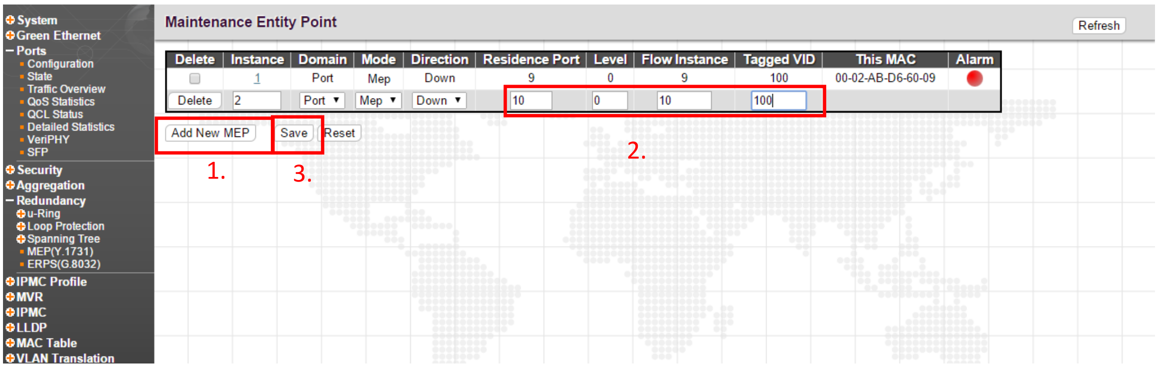




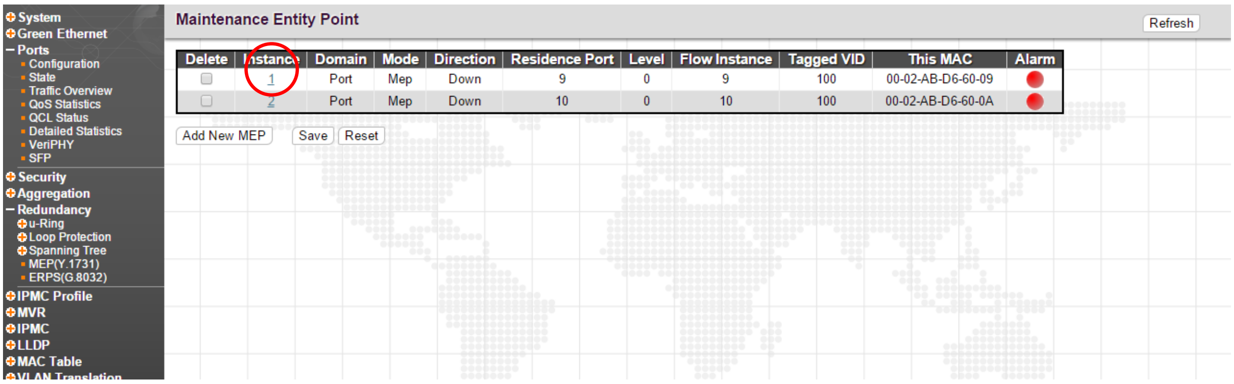


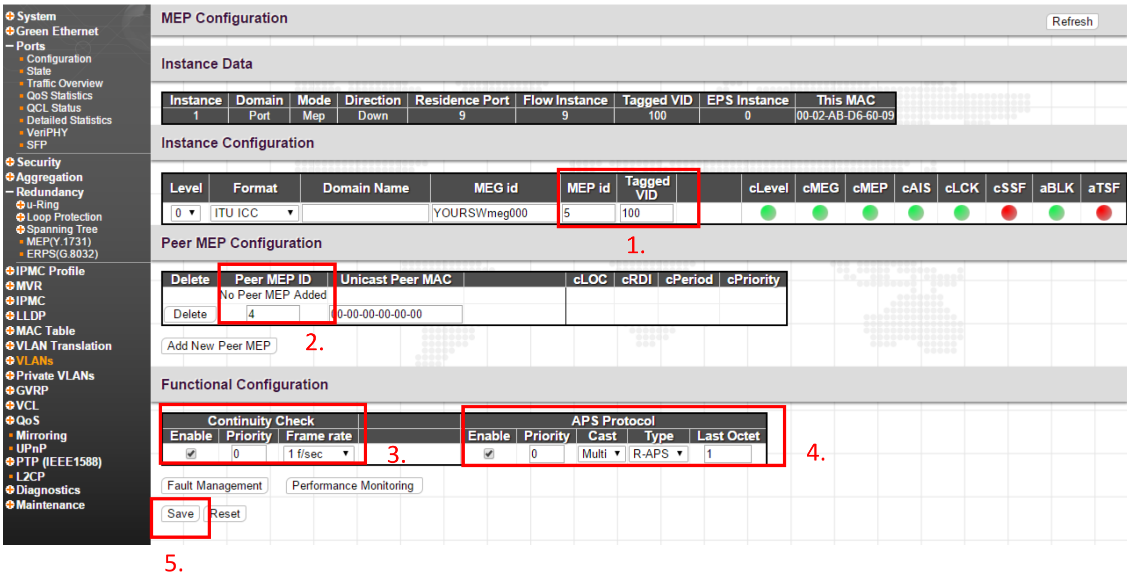
## B. Configure MEP on SW#3





## C. Click "Instance 1 " to configure further setting of MEP

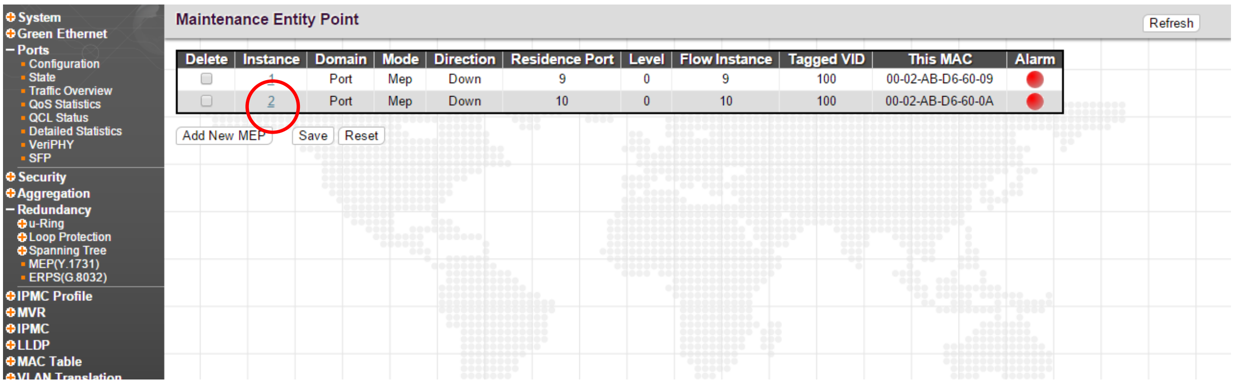


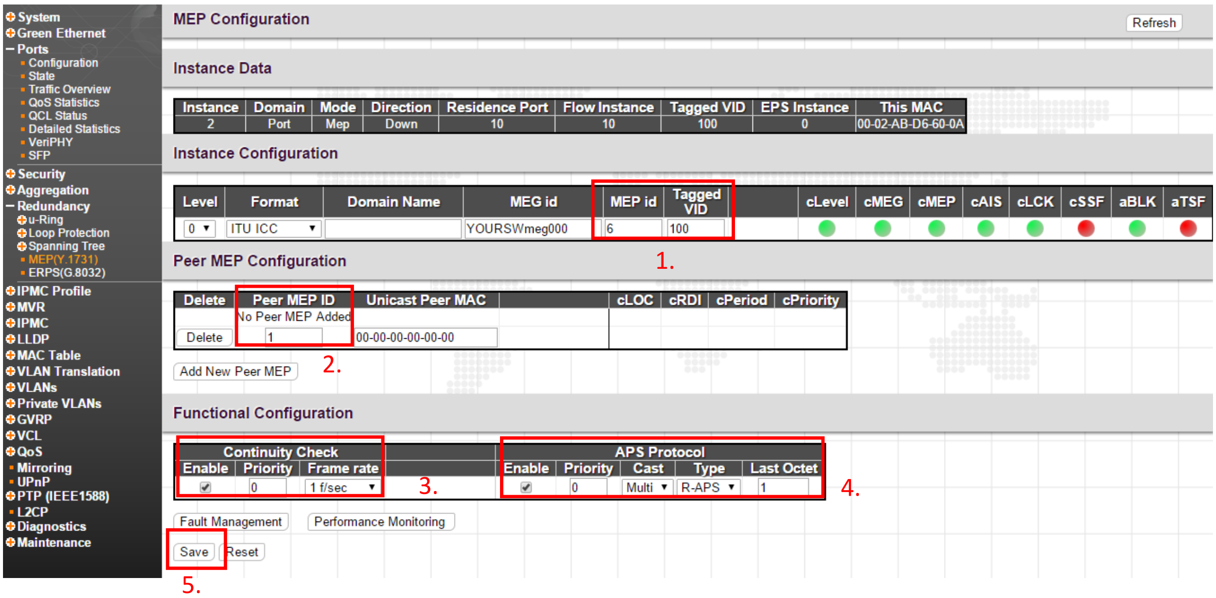


***NOTE:***

*The MEP ID (5) here is for Port 9 of SW#3*
*And Peer MEP ID (4) is the neighbor port 10 of SW#2.*
*Always refer back to your design topology as in < Figure 1>.*

## D. Click "Instance 2" to configure further setting of MEP

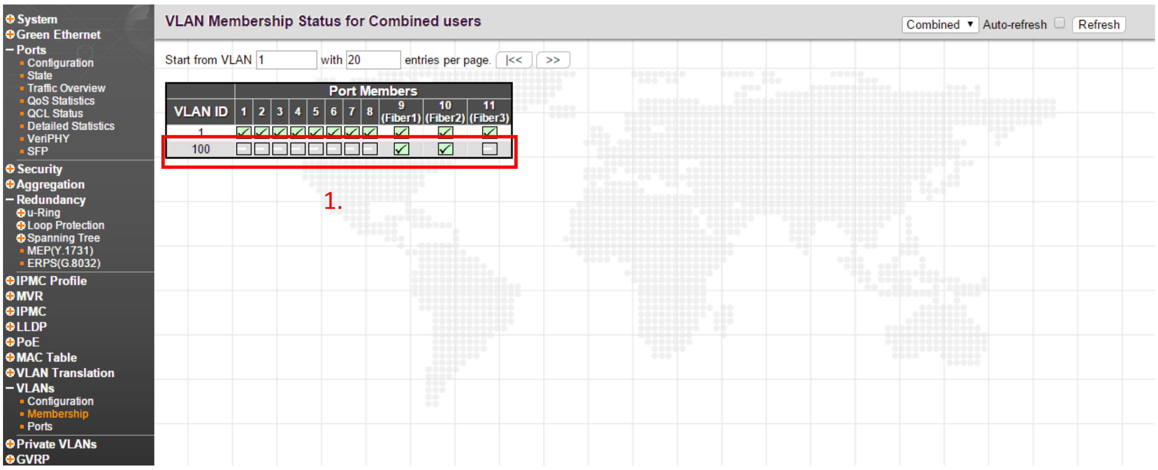




***NOTE:***

*The MEP ID (6) here is for Port 9 of SW#3*
*And Peer MEP ID (1) is the neighbor port 9 of SW#1. Always refer back to your design topology as in < Figure 1>.*

## E. Check VLAN Membership Table



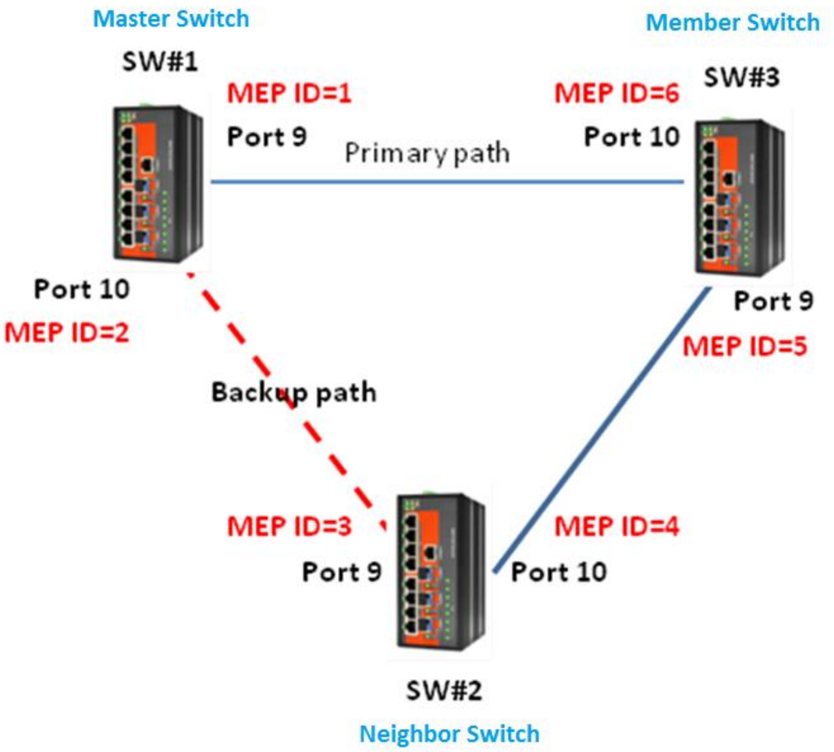

1. When MEP instances are created, an entry of VLAN membership associated with MEP configuration will be established automatically in VLAN Membership Table. Hence, you do not manually create this VLAN entry. In this example, VLAN ID 100 entry with port 9 & 10 as members is created dynamically.

---

***NOTE:***
*When MEP instances are deleted, VLAN membership associated with MEP configuration will also be deleted automatically.*

---

# ERPS Configuration

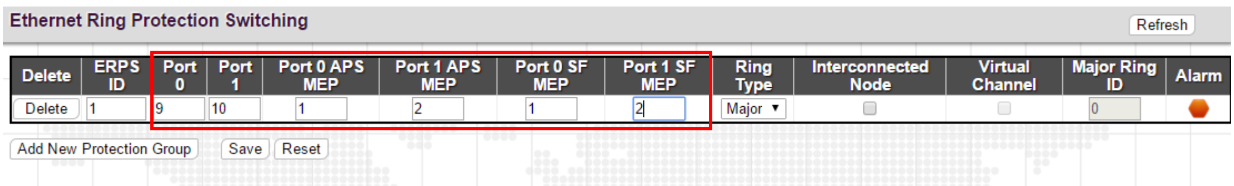



We need to assign one switch as Master, one as Neighbor, and all others as Member switches. The function of Master switch is to decide which path is active (unblocked) and which one is backup path (blocked). Neighbor switch is connecting to Master switch directly by backup path (or standby path).

In this topology, we assign SW#1 as Master switch, SW#2 as Neighbor switch and SW#3 as Member switch. The configuration example is below:

## ERPS configuration of SW#1 (Master switch)

### A. Create 1 ERPS protection Group

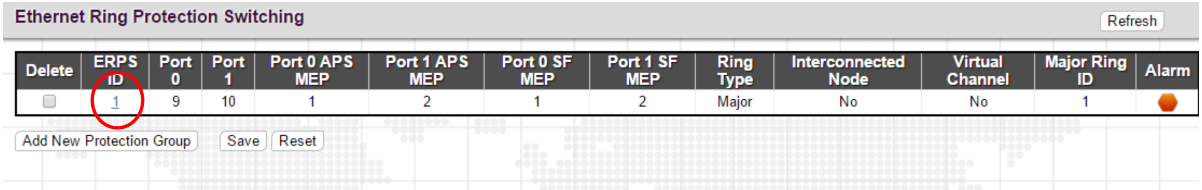


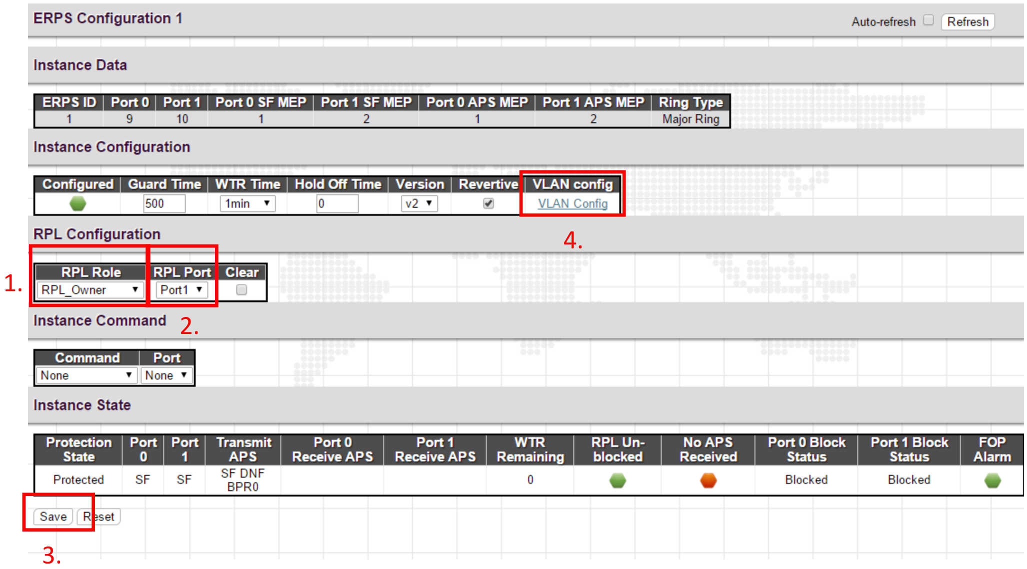

1. From ERPS Click "Add New Protection Group" and follow the setting logic described below
2. Click "Save"

***NOTE:***
*The Port 0 and 1 send the CCM (Continuity Check Message) packets of Y.1731 out from switch physical interfaces. We use Port 9 and 10 for the ERPS example here.*
*"Port 0 APS MEP" "Port 1 APS MEP" "Port 0 SF MEP" Port 1 SF MEP" columns will follow the MEP Instance ID we assigned for Port 9 & 10 earlier, so interface 9 = port 0 = Instance ID 1 ,*

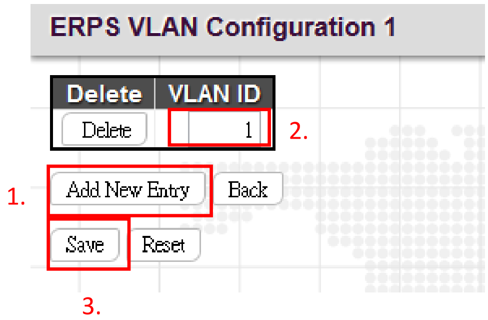
*interface 10 = port 1= Instance ID 2.*

**B. Click ERPS ID to configure advance setting of ERPS – (Master switch)**




1. For Master switch, please select RPL role "RPL_Owner"
2. Set the "RPL Port" to Port1
3. Click "Save"
4. Click "VLAN Config" and follow the settings below



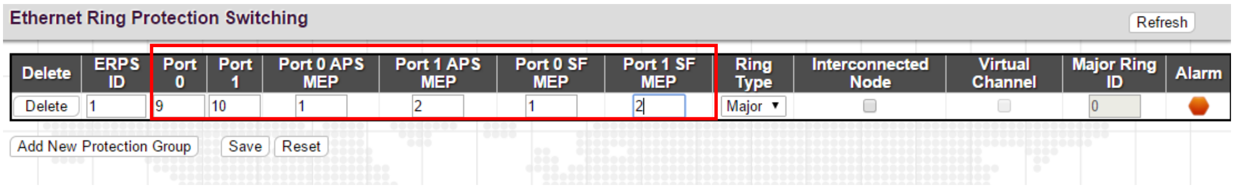

1. Click "Add New Entry"
2. Set VLAN ID to "1"
3. Click "Save"

***NOTE: RPL Role***
*RPL_Owner = Master switch*
*RPL_Neighbor = Neighbor switch*
*None = Member switch*

*RPL port : assign which port is standby path, we assign port 1 (Interface 10 of SW1) for example. Finally, we add VLAN ID 1 for management VLAN of ERPS*

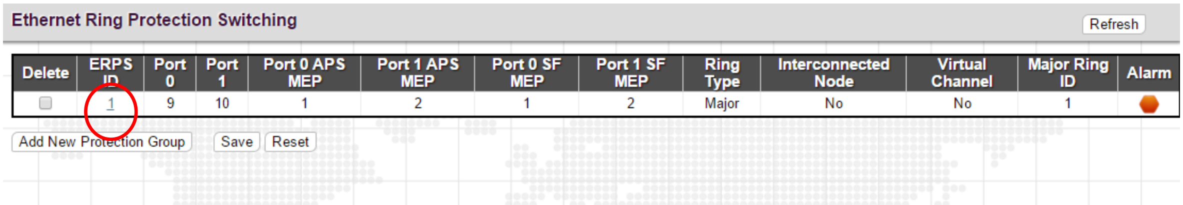
## ERPS configuration of SW#2 (Neighbor switch )

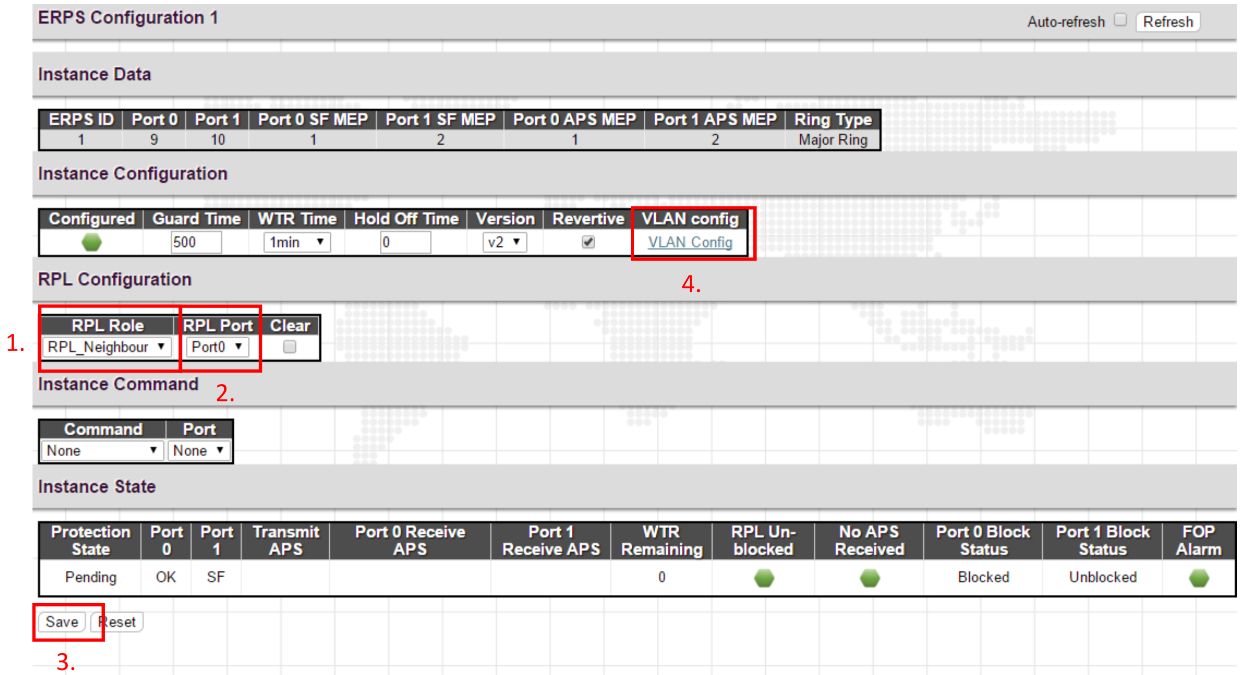
### A. Create 1 ERPS protection Group




1. Click "Add New Protection Group", configure Ports, APS and SF
2. Click "Save"

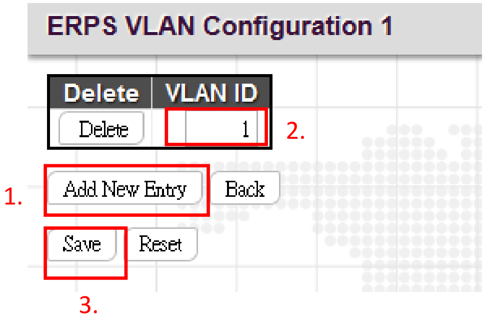
### B. Click ERPS ID to configure advance setting of ERPS – (Neighbor switch)




1. For Neighbor switch, please select "RPL_Neighbour" RPL Role
2. Set the "RPL Port" to Port0
3. Click "Save"

4. Click "VLAN Config" and follow the settings below




1. Click "Add New Entry"
2. Set VLAN ID to "1"
3. Click "Save"

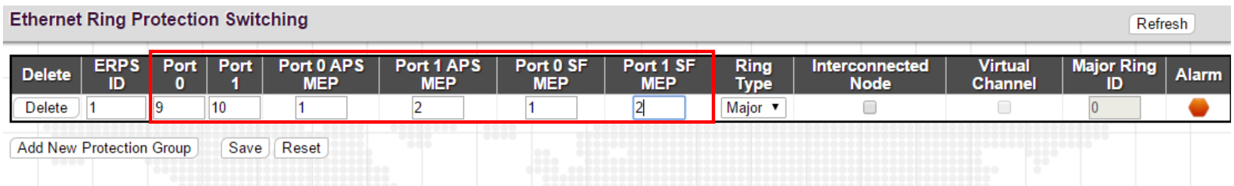
---

***NOTE:*** *RPL Port = Port 0 (Interface 9 of SW#2 )*

---

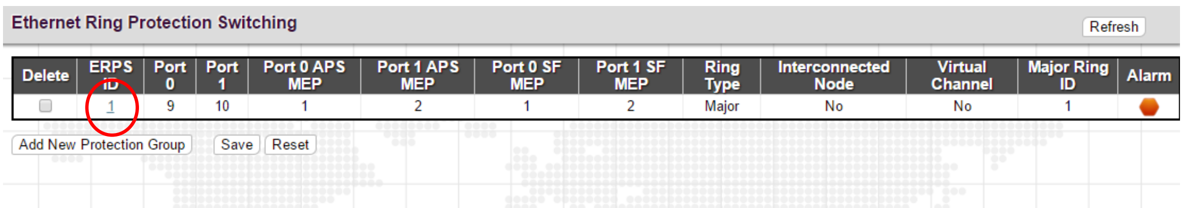
## ERPS configuration of SW#3 (Member switch )

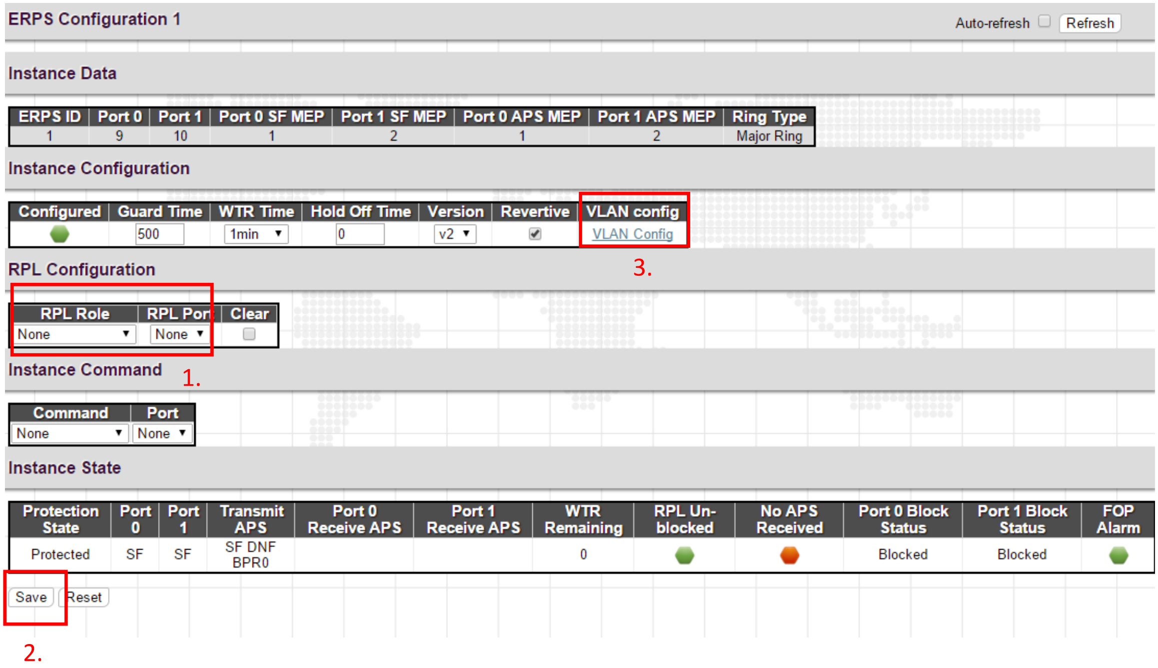
### A. Create 1 ERPS protection Group



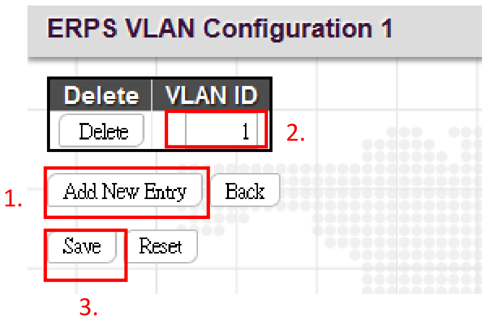

1. Click "Add New Protection Group", configure Ports, APS and SF
2. Click "Save"

### B. Click ERPS ID to configure advance setting of ERPS – (Member switch)






1. For Member switches, make sure that RPL role and port are set to "None"
2. Click "Save"
3. Click "VLAN Config"

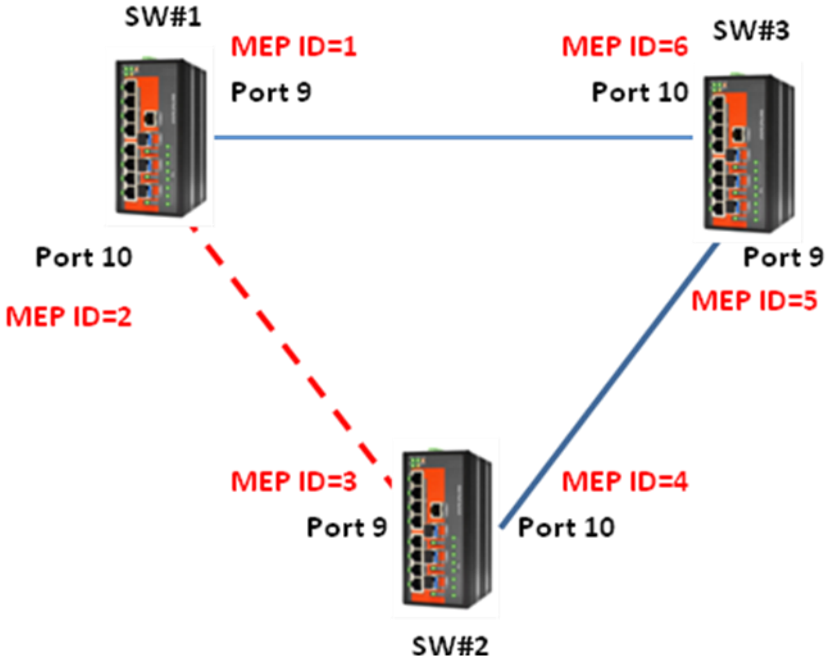



1. Click "Add New Entry"
2. Set VLAN ID to "1"
3. Click "Save"

***NOTE:*** *RPL Role => None = Member switch.*

# Verification and Testing I

**A. Put the connection back to form a Ring network.**




**B. Check MEP port status, the Alarm LED indicator should be shown in green.**

<SW#1 >

**Maintenance Entity Point**

| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | This MAC | Alarm |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1 | Port | Mep | Down | 9 | 0 | 9 | 100 | 00-02-AB-D6-68-99 | ● |
| ☐ | 2 | Port | Mep | Down | 10 | 0 | 10 | 100 | 00-02-AB-D6-68-9A | ● |

Add New MEP | Save | Reset

<SW#2>

**Maintenance Entity Point**

| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | This MAC | Alarm |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1 | Port | Mep | Down | 9 | 0 | 9 | 100 | 00-02-AB-D6-60-79 | ● |
| ☐ | 2 | Port | Mep | Down | 10 | 0 | 10 | 100 | 00-02-AB-D6-60-7A | ● |

Add New MEP | Save | Reset

<SW#3>

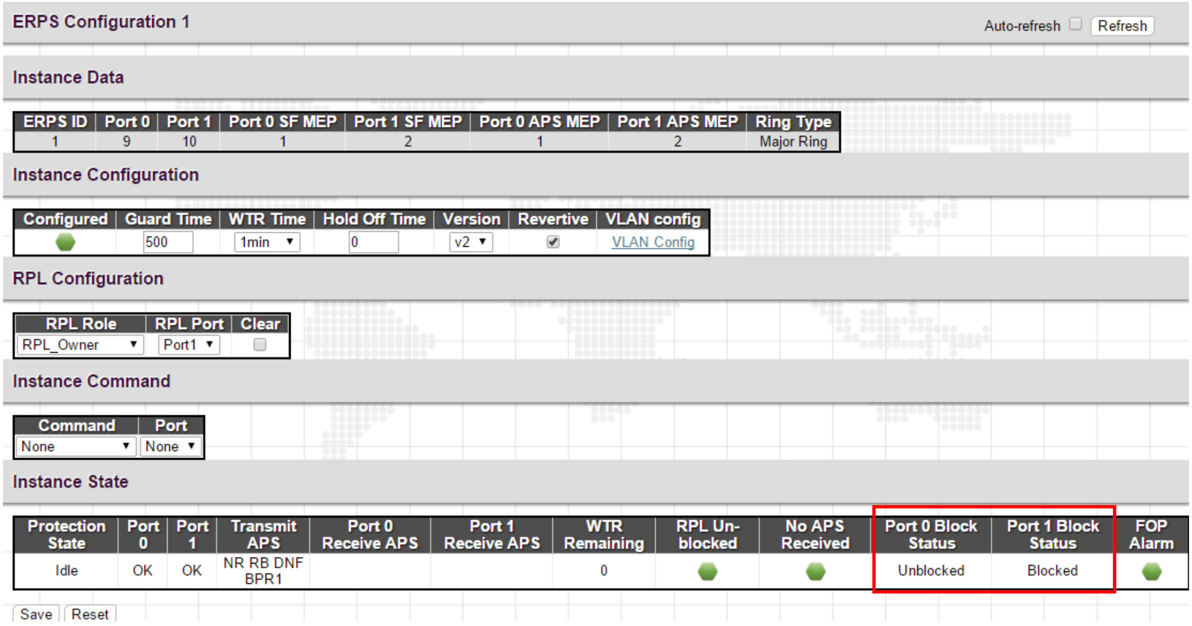
**Maintenance Entity Point**

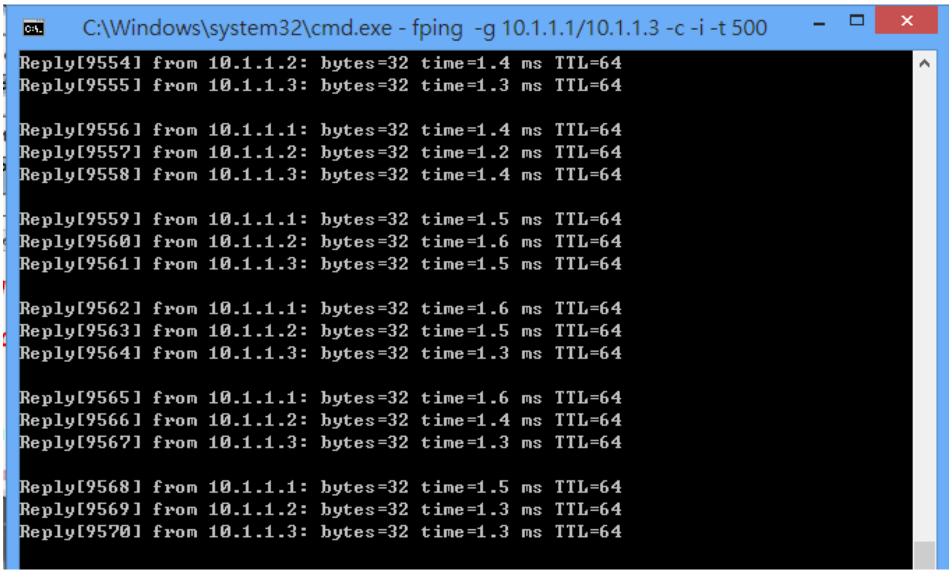
| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | This MAC | Alarm |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1 | Port | Mep | Down | 9 | 0 | 9 | 100 | 00-02-AB-D6-60-09 | ● |
| ☐ | 2 | Port | Mep | Down | 10 | 0 | 10 | 100 | 00-02-AB-D6-60-0A | ● |

Add New MEP | Save | Reset

***NOTE:*** *If the Alarm indication is shown in red, please recheck your configuration in MEP setting and make sure your physical connection is correct as described in topology <Figure 1>.*

**C. Check ERPS Primary and standby path can auto switch correctly while pinging all switches continuously.**



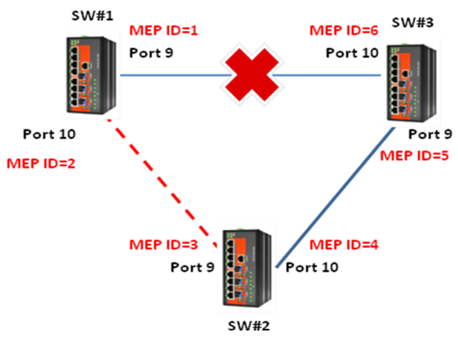



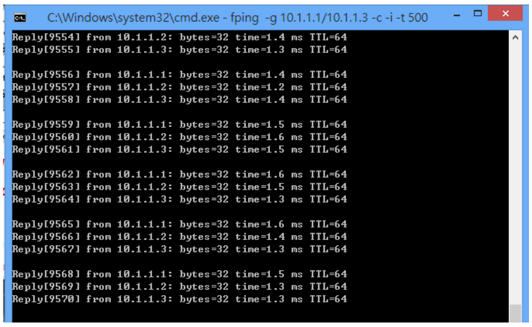

***NOTE:***

*In normal status, Port 0 (Interface 9) is primary path (Unblock)*
*Port 1 (Interface 10) is standby path, so it is blocked.*

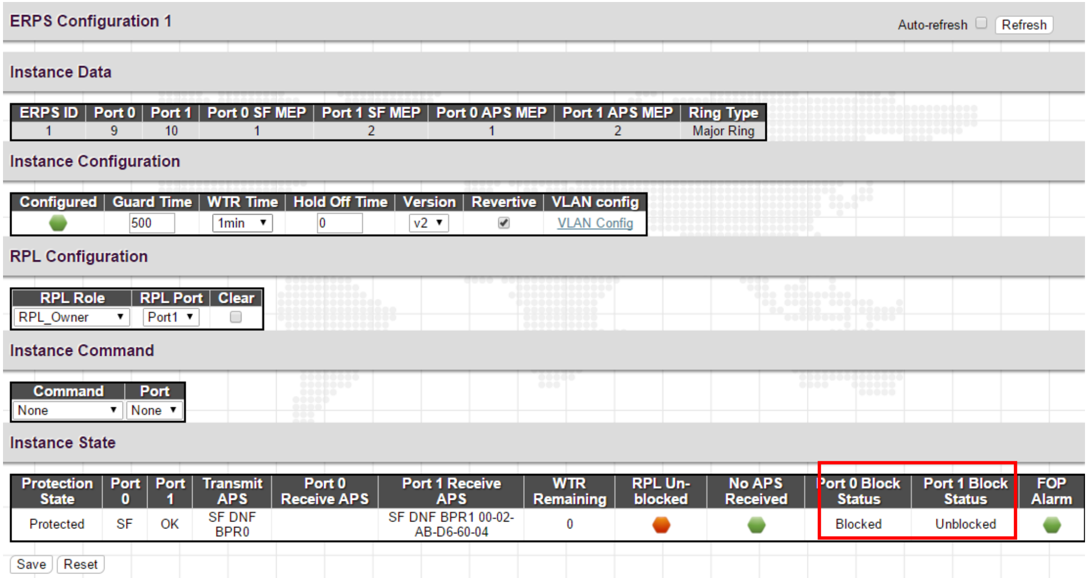
# Verification and Testing II

**A. Disconnect path between SW#1 and SW#3, like the figure below. The standby path should now be active and still can ping all switches.**



```
C:\Windows\system32\cmd.exe - fping -g 10.1.1.1/10.1.1.3 -c -i -t 500
Reply[9554] from 10.1.1.2: bytes=32 time=1.4 ms TTL=64
Reply[9555] from 10.1.1.3: bytes=32 time=1.3 ms TTL=64

Reply[9556] from 10.1.1.1: bytes=32 time=1.4 ms TTL=64
Reply[9557] from 10.1.1.2: bytes=32 time=1.2 ms TTL=64
Reply[9558] from 10.1.1.3: bytes=32 time=1.4 ms TTL=64

Reply[9559] from 10.1.1.1: bytes=32 time=1.5 ms TTL=64
Reply[9560] from 10.1.1.2: bytes=32 time=1.6 ms TTL=64
Reply[9561] from 10.1.1.3: bytes=32 time=1.5 ms TTL=64

Reply[9562] from 10.1.1.1: bytes=32 time=1.6 ms TTL=64
Reply[9563] from 10.1.1.2: bytes=32 time=1.5 ms TTL=64
Reply[9564] from 10.1.1.3: bytes=32 time=1.3 ms TTL=64

Reply[9565] from 10.1.1.1: bytes=32 time=1.6 ms TTL=64
Reply[9566] from 10.1.1.2: bytes=32 time=1.4 ms TTL=64
Reply[9567] from 10.1.1.3: bytes=32 time=1.3 ms TTL=64

Reply[9568] from 10.1.1.1: bytes=32 time=1.5 ms TTL=64
Reply[9569] from 10.1.1.2: bytes=32 time=1.3 ms TTL=64
Reply[9570] from 10.1.1.3: bytes=32 time=1.3 ms TTL=64
```



ERPS Configuration 1 — Auto-refresh ☐ Refresh

Instance Data

| ERPS ID | Port 0 | Port 1 | Port 0 SF MEP | Port 1 SF MEP | Port 0 APS MEP | Port 1 APS MEP | Ring Type |
|---|---|---|---|---|---|---|---|
| 1 | 9 | 10 | 1 | 2 | 1 | 2 | Major Ring |

Instance Configuration

| Configured | Guard Time | WTR Time | Hold Off Time | Version | Revertive | VLAN config |
|---|---|---|---|---|---|---|
| ● | 500 | 1min | 0 | v2 | ☑ | VLAN Config |

RPL Configuration

| RPL Role | RPL Port | Clear |
|---|---|---|
| RPL_Owner | Port1 | ☐ |

Instance Command

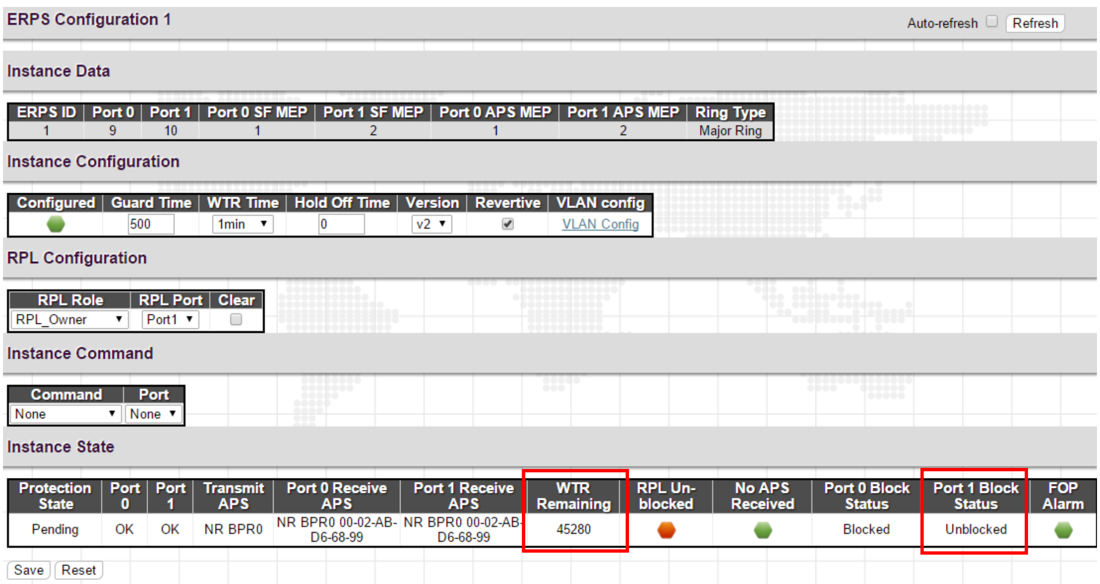
| Command | Port |
|---|---|
| None | None |

Instance State

| Protection State | Port 0 | Port 1 | Transmit APS | Port 0 Receive APS | Port 1 Receive APS | WTR Remaining | RPL Un-blocked | No APS Received | Port 0 Block Status | Port 1 Block Status | FOP Alarm |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Protected | SF | OK | SF DNF BPR0 | | SF DNF BPR1 00-02-AB-D6-60-04 | 0 | ● | ● | Blocked | Unblocked | ● |

Save Reset

**B. When you put the primary path back, the "WTR Remaining" will start to count down for 1 min before changing primary and standby paths back to normal status.**



ERPS Configuration 1 — Auto-refresh ☐ Refresh

Instance Data

| ERPS ID | Port 0 | Port 1 | Port 0 SF MEP | Port 1 SF MEP | Port 0 APS MEP | Port 1 APS MEP | Ring Type |
|---|---|---|---|---|---|---|---|
| 1 | 9 | 10 | 1 | 2 | 1 | 2 | Major Ring |

Instance Configuration

| Configured | Guard Time | WTR Time | Hold Off Time | Version | Revertive | VLAN config |
|---|---|---|---|---|---|---|
| ● | 500 | 1min | 0 | v2 | ☑ | VLAN Config |

RPL Configuration

| RPL Role | RPL Port | Clear |
|---|---|---|
| RPL_Owner | Port1 | ☐ |

Instance Command

| Command | Port |
|---|---|
| None | None |

Instance State

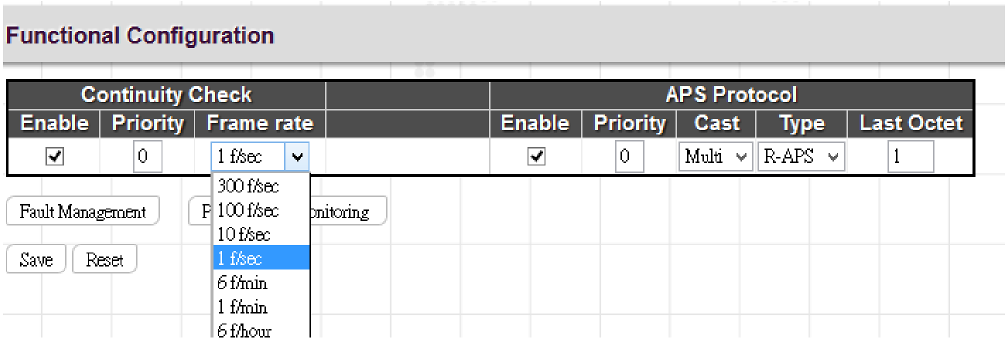
| Protection State | Port 0 | Port 1 | Transmit APS | Port 0 Receive APS | Port 1 Receive APS | WTR Remaining | RPL Un-blocked | No APS Received | Port 0 Block Status | Port 1 Block Status | FOP Alarm |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Pending | OK | OK | NR BPR0 | NR BPR0 00-02-AB-D6-68-99 | NR BPR0 00-02-AB-D6-68-99 | 45280 | ● | ● | Blocked | Unblocked | ● |

Save Reset

## Reference

The configuration can use a different MEP CCM frame rate to obtain the desired protection switching times. The following are rough switching times with configured CCM frame rates.

300 f/sec switching time is around 25ms
100 f/sec switching time is around 50ms
10 f/sec switching time is around 350ms
1 f/sec switching time is around 250ms ~ 3.5s




These settings must be made for each switch and for each (Instance) MEP ID. Care must be taken if performing this configuration remotely since changing the CCM on one side of an RPL will block that link until both sides of the RPL have equal CCM frame rate settings. If management for that remote unit depends on the link, be sure to change the remote end of RPL first then change the local end, at which point the RPL will again be unblocked and the remote device will be manageable.

# APPENDIX C. ACRONYMS

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

**ACL**
ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights. ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

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

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

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

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

**ARP Inspection**
ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

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

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

**CDP**
CDP is an acronym for Cisco Discovery Protocol.

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

**DES**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

**HTTPS**

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

**ICMP**

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

**IEEE 802.1X**

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

**IGMP**

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

IGMP Querier

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

**IMAP**

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

**IP**

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

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

**IPMC**

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

**IPMC Profile**

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

**IP Source Guard**

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

**LACP**

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

**LLC**

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

**LLDP**

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

**LLDP-MED**

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

**LLQI**

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

**LOC**

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

**MAC Table**

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

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

**MEP**

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

**MD5**

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

**Mirroring**

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

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

**MLD**

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

**MLD Querier**

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

**MSTP**

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

**MVR**

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

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

**NAS**

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

**NetBIOS**

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

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

**NFS**

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

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

**NTP**

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

**OAM**

OAM is an acronym for Operation Administration and Maintenance.

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

**Optional TLVs.**

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

**OUI**

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

**PCP**

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

**PD**

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

**PHY**

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

**PING**

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

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

**PoE**

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

**Policer**

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

**POP3**

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

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

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

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

**PPPoE**

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

**Private VLAN**

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

**PTP**

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

**QCE**

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

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

**QCI**

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

**QCL**

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

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

**QL**

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

**QoS**

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

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

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

**QoS class**

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

**Querier Election**

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

**RARP**

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

**RADIUS**

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

**RDI**

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

Router Port

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

**RSTP**

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

**SAMBA**

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

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

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

**sFlow**

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

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

**SHA**

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

**Shaper**

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

**SMTP**

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

**SNAP**

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

**SNMP**

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

**SNTP**

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

**SPROUT**

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

**SSID**

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

**SSH**

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

**SSM**

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

**STP**

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

**Switch ID**

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

**SyncE**

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

**TACACS+**

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

**Tag Priority**

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

**TCP**

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

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

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

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

**TELNET**

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

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

**TFTP**

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

**ToS**

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

**TLV**

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

**TKIP**

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

**UDP**

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

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

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

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

**UPnP**

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

**User Priority**

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

**VLAN**

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

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

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

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

**VLAN ID**

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

Voice VLAN

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

**WEP**

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

**WiFi**

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

**WPA**

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

**WPA-PSK**

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

**WPA-Radius**

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

**WPS**

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

**WRED**

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

**WTR**

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

*This page is intentionally left blank.*

www.ctcu.com

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