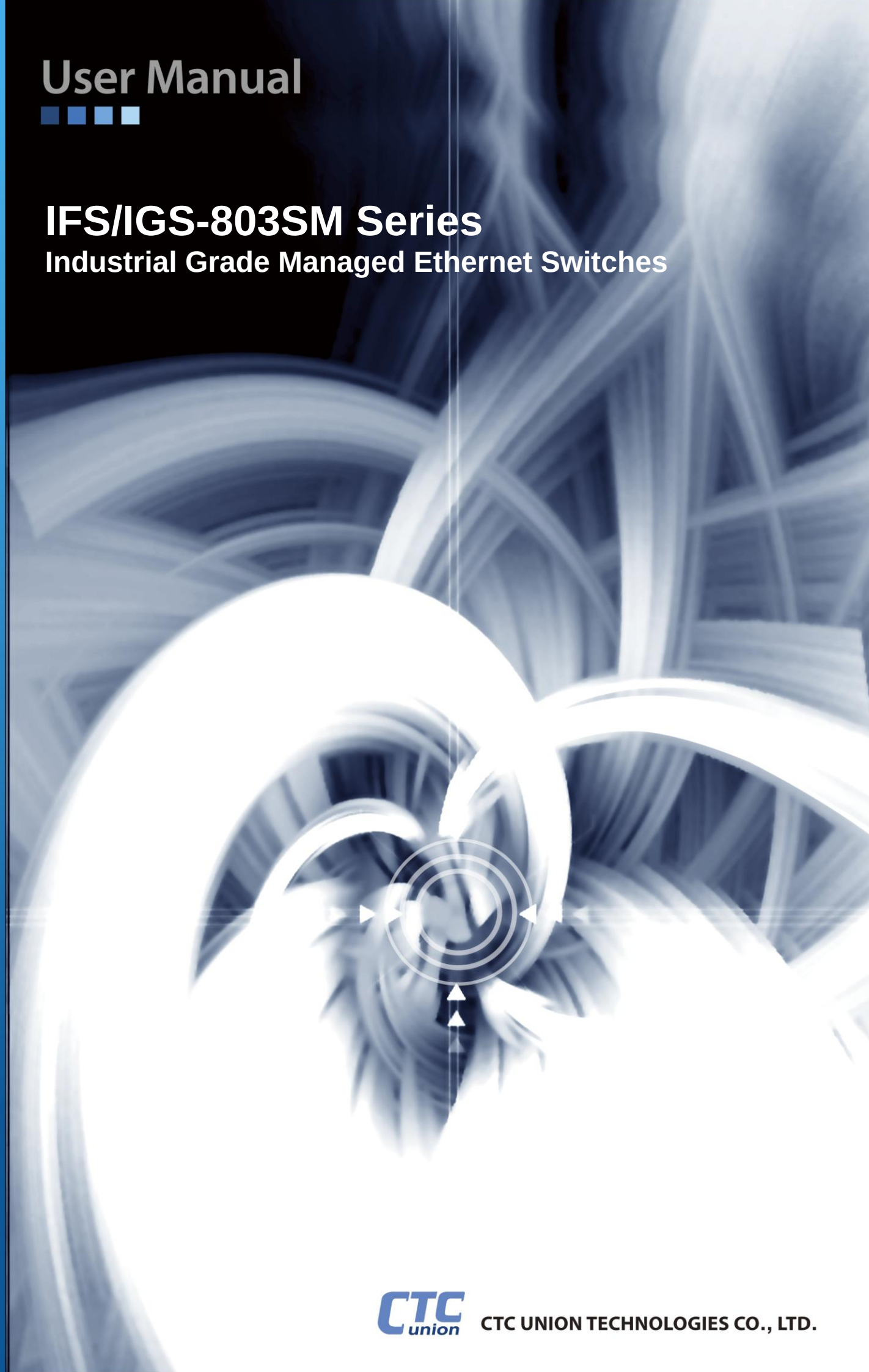
User Manual

IFS/IGS-803SM Series

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.

TRADEMARKS

Microsoft is a registered trademark of Microsoft Corp.
HyperTerminal™ is a registered trademark of Hilgraeve Inc.
ActiPHY™ and VeriReach™ are registered trademarks of Vitesse® Semiconductor

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 1.0 March 2014

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.

©2014 CTC Union Technologies Co.,Ltd.
All Rights Reserved
The contents of this document are subject to change without any prior notice.

CHAPTER 1. INTRODUCTION 9

1.1 WELCOME 9
1.2 PRODUCT DESCRIPTION 9
1.2.1 IFS-803GSM 9
1.2.2 IGS-803SM 10
1.2.3 IFS-803GSM-8PH24 10
1.2.4 IGS-803SM-8PH24 11
1.3 PRODUCT FEATURES 12
1.4 PRODUCT SPECIFICATIONS 13

CHAPTER 2. PANELS & INSTALLATION 15

2.1 VIEWS OF PANELS 15
2.2 LAN CONNECTIONS 16
2.3 POE 16
2.4 FIBER CONNECTIONS 17
2.5 CONSOLE PORT CONNECTION 17
2.5.1 RJ-45 Pin Assignment 18
2.5.2 Accessory Cable 18
2.6 POWER & ALARM 18
2.7 LED INDICATORS 19
2.8 INSTALLATION 20
2.8.1 Mounting 20
2.8.2 Un-mounting 20

CHAPTER 3. INTRODUCTION TO CLI 21

3.1 INTRODUCTION 21
3.2 CONSOLE OPERATION 21
3.2.1 CLI Online Help 22
3.2.2 TCP/IP Configuration via CLI 23
3.2.2.1 IP Address 23
3.2.2.2 Default Gateway 23
3.2.2.3 DNS Server 23
3.2.2.4 Display TCP/IP Settings 23
3.2.3 Factory Default 24
3.2.4 Reboot Device 24
3.2.5 Admin Password 24
3.2.6 Logout 24

CHAPTER 4. WEB OPERATION & CONFIGURATION 25

4.1 HOME PAGE 25
4.1.1 Login 25
4.1.2 Port Status 26
4.1.3 Refresh 26
4.1.4 Help System 26
4.1.5 Logout 26
4.2 SYSTEM 27
4.2.1 System Configuration 27
4.2.2 System Information 28
4.2.3 System IP 28
4.2.4 System IP Status 30
4.2.5 System NTP 30
4.2.6 System Time 31
4.2.7 System Log Configuration 32
4.2.8 System Log Information 32
4.2.9 System Detailed Log 33
4.2.10 System CPU Load 33

4.2.11 System SMTP 34
4.3 GREEN ETHERNET 35
4.3.1 Green Ethernet LED 35
4.3.2 Green Ethernet Configuration 36
4.3.3 Green Ethernet Status 37
4.4 PORTS 37
4.4.1 Ports Configuration 38
4.4.2 Ports State 39
4.4.3 Ports Traffic Overview 40
4.4.4 Ports QoS Statistics 40
4.4.5 Ports QCL Status 41
4.4.6 Ports Detailed Statistics 42
4.4.7 Ports VeriPHY™ 43
4.4.8 Ports SFP 44
4.5 SECURITY 45
4.5.1 Switch 45
4.5.1.1 Users 45
4.5.1.2 Privilege Levels 46
4.5.1.3 Auth Method 47
4.5.1.4 SSH 48
4.5.1.5 HTTPS 48
4.5.2 Access Management 49
4.5.2.1 Access Management Configuration 49
4.5.2.2 Access Management Statistics 49
4.5.3 SNMP 50
4.5.3.1 SNMP System Configuration 50
4.5.3.2 Alarm Configuration 51
4.5.3.3 SNMPv3 Community Configuration 54
4.5.3.4 SNMPv3 User Configuration 55
4.5.3.5 SNMPv3 Group Configuration 56
4.5.3.6 SNMPv3 View Configuration 56
4.5.3.7 SNMPv3 Access Configuration 57
4.5.4 RMON 58
4.5.4.1 RMON Statistics Configuration 58
4.5.4.2 RMON History Configuration 58
4.5.4.3 RMON Alarm Configuration 59
4.5.4.4 RMON Event Configuration 60
4.5.4.5 RMON Statistics Overview 60
4.5.4.6 History Overview 61
4.5.4.7 Alarm Overview 62
4.5.4.8 Event Overview 63
4.5.5 Network 63
4.5.5.1 Port Security 63
4.5.5.1.1 Limit Control 63
4.5.5.1.2 Switch Status 65
4.5.5.1.3 Port Statistics 66
4.5.5.2 NAS 66
4.5.5.2.1 Configuration 67
4.5.5.2.2 Switch Status 70
4.5.5.2.3 Port Statistics 70
4.5.5.3 ACL 72
4.5.5.3.1 Ports 72
4.5.5.3.2 Rate Limiters 73
4.5.5.3.3 Access Control List 73
4.5.5.3.4 ACL Status 77
4.5.5.4 DHCP 78
4.5.5.4.1 Snooping Configuration 79
4.5.5.4.2 Snooping Statistics 79

4.5.5.4.3 Relay Configuration 80
4.5.5.4.4 Relay Statistics 81
4.5.5.5 IP Source Guard 82
4.5.5.5.1 Configuration 82
4.5.5.5.2 Static Table 82
4.5.5.5.3 Dynamic Table 83
4.5.5.6 ARP inspection 83
4.5.5.6.1 Port Configuration 83
4.5.5.6.2 VLAN Configuration 84
4.5.5.6.3 Static Table 85
4.5.5.6.4 Dynamic Table Configuration 85
4.5.5.6.5 Dynamic Table Status 86
4.5.6 RADIUS 86
4.5.6.1 Configuration 86
4.5.6.2 RADIUS Overview 87
4.5.6.3 RADIUS Details 88
4.5.6.4 TACACS+ 90
4.6 AGGREGATION 91
4.6.1 Static 91
4.6.2 LACP 92
4.6.2.1 Port Configuration 92
4.6.2.2 System Status 93
4.6.2.3 Port Status 93
4.6.2.4 Port Statistics 94
4.7 REDUNDANCY 94
4.7.1 u-Ring 94
4.7.1.1 Configuration 95
4.7.1.2 Status 97
4.7.2 Loop Protection 98
4.7.2.1 Configuration 98
4.7.2.2 Status 99
4.7.3 Spanning Tree 99
4.7.3.1 Bridge Settings 100
4.7.3.2 MSTI Mapping 101
4.7.3.3 MSTI Priorities 102
4.7.3.4 CIST Ports 103
4.7.3.5 MSTI Ports 104
4.7.3.6 Bridge Status 104
4.7.3.7 Port Status 106
4.7.3.8 Port Statistics 107
4.7.4 MEP 107
4.7.5 ERPS 117
4.8 IPMC PROFILE 118
4.8.1 Profile Table 118
4.8.2 Address Entry 119
4.9 MVR 120
4.9.1 Configuration 120
4.9.2 MVR Statistics 122
4.9.3 MVR Channel Groups 122
4.9.4 MVR SFM Information 123
4.10 IPMC 123
4.10.1 IGMP Snooping 123
4.10.1.1 Basic Configuration 124
4.10.1.2 VLAN Configuration 125
4.10.1.3 Port Filtering Profile 126
4.10.1.4 Status 127
4.10.1.5 Groups Information 128
4.10.1.6 IPv4 SFM Information 128

4.10.2 MLD Snooping 128
4.10.2.1 Basic Configuration 129
4.10.2.2 VLAN Configuration 130
4.10.2.3 Port Filtering Profile 131
4.10.2.4 Status 131
4.10.2.5 Groups Information 132
4.10.2.6 IPv6 SFM Information 133
4.11 LLDP 133
4.11.1 Configuration 134
4.11.2 LLDP-MED 135
4.11.3 Neighbours 138
4.11.4 LLDP-MED Neighbours 138
4.11.5 LLDP PoE 138
4.11.6 LLDP EEE 139
4.11.7 LLDP Global Counters 140
4.12 PoE (for PoE models only) 141
4.12.1 PoE Configuration 141
4.12.2 PoE Check (PoE PD Auto Test/Auto Reset) 142
4.12.3 PoE Schedule 143
4.12.4 Status 144
4.13 MAC Table 144
4.13.1 MAC Address Table Configuration 145
4.13.2 MAC Address Table 146
4.14 VLAN Translation 146
4.14.1 Port to Group Mapping 147
4.14.2 VID Translation Mapping 147
4.15 VLANs 148
4.15.1 Membership Configuration 148
4.15.2 Ports Configuration 149
4.15.3 Membership Status 151
4.15.4 Port Status 151
4.16 Private VLANs 152
4.16.1 PVLAN Membership 152
4.16.2 Port Isolation 152
4.17 VCL 153
4.17.1 MAC-based 153
4.17.1.1 Membership Configuration 153
4.17.1.2 Membership Status 153
4.17.2 Protocol-based VLAN 154
4.17.2.1 Protocol to Group 154
4.17.2.2 Group to VLAN 155
4.17.3 IP Subnet-based VLAN 155
4.18 QoS 156
4.18.1 Port Classification 156
4.18.2 Port Policing 157
4.18.3 Queue Policing 158
4.18.4 Port Scheduler 159
4.18.5 Port Shaping 161
4.18.6 Port Tag Remarking 161
4.18.7 Port DSCP 163
4.18.8 DSCP-Based QoS 164
4.18.9 DSCP Translation 165
4.18.10 DSCP Classification 166
4.18.11 QoS Control List 166
4.18.12 Storm Control 169
4.19 Mirroring 170
4.20 UPnP 170
4.21 Diagnostics 171

4.21.1 Ping 171
4.21.2 Ping6 171
4.22 MAINTENANCE 172
4.22.1 Reboot 172
4.22.2 Factory Defaults 172
4.22.3 Software 172
4.22.3.1 Upload 172
4.22.3.2 Image Select 173
4.22.4 Configuration 173
4.22.4.1 Backup 173
4.22.4.2 Restore 173
APPENDIX A. u-Ring CONFIGURATION PROCEDURE 174
APPENDIX B. G.8032 CONFIGURATION PROCEDURE 184
APPENDIX C. VLAN BASIC CONFIGURATIONS 211
APPENDIX D. ACRONYMS 220

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.

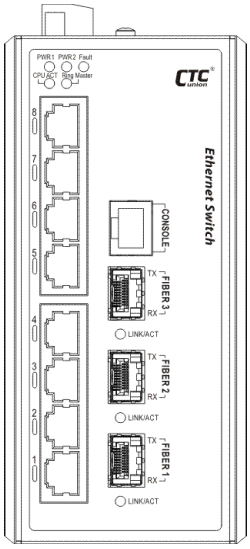
1.2 Product Description

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).

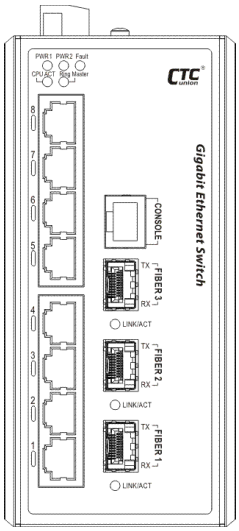
1.2.1 IFS-803GSM

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.



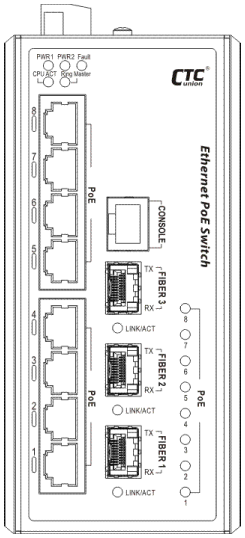
1.2.2 IGS-803SM

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.



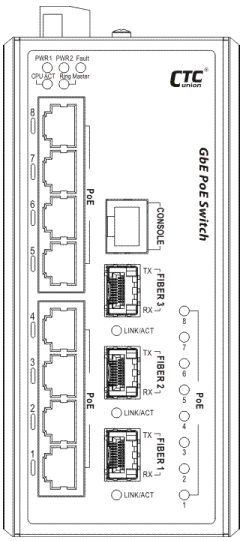
1.2.3 IFS-803GSM-8PH24

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

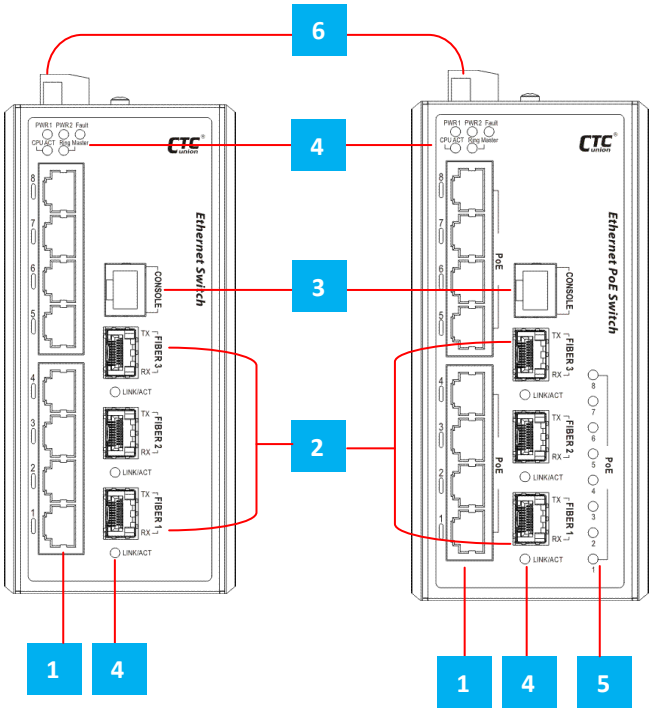
Standards	IEEE 802.3	10Base-T 10Mbit/s Ethernet
	IEEE 802.3u	100Base-TX, 100Base-FX, Fast Ethernet
	IEEE 802.3ab	1000Base-T Gbit/s Ethernet over twisted pair
	IEEE 802.3z	1000Base-X Gbit/s Ethernet over Fiber-Optic
	IEEE 802.1d	STP (Spanning Tree Protocol)
	IEEE 802.1w	RSTP (Rapid Spanning Tree Protocol)
	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 EN61000-4-3 (RS) Level3, Criteria A EN61000-4-4 (Burst) Level3, Criteria A EN61000-4-5 (Surge) Level3, Criteria B EN61000-4-6 (CS) Level3, Criteria A 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

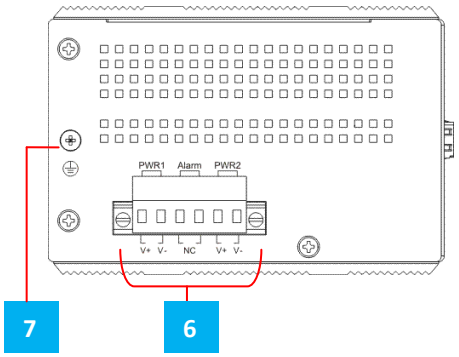
Each physical feature on the panels is indexed numerically and explained briefly in the reference box on the right hand side. Detailed descriptions for each feature are also provided in the following sub-sections.



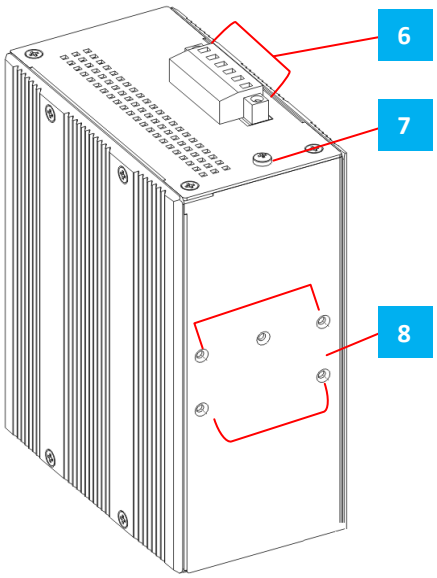
Front Panel

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

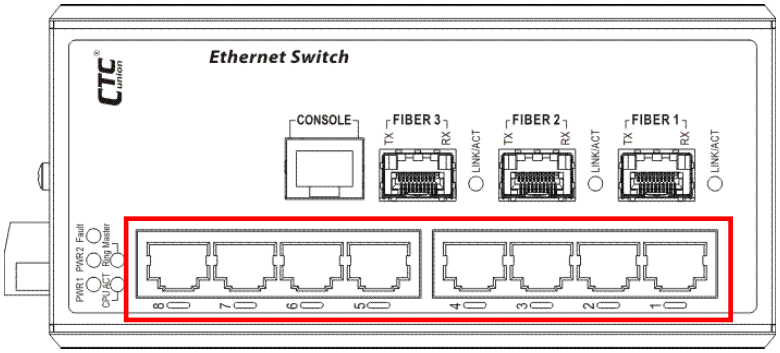


Top Panel



Side & Rear Panel

2.2 LAN Connections

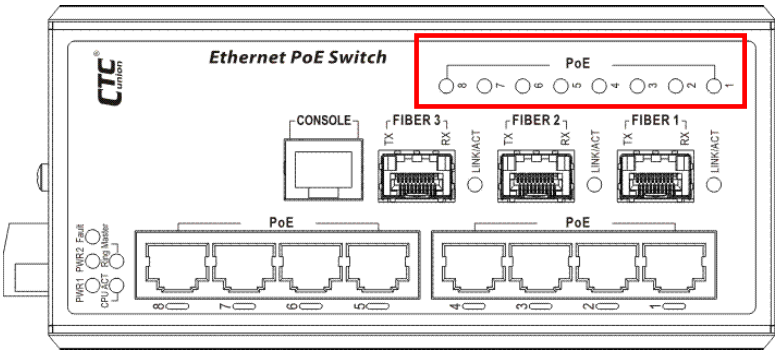


Front of unit

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.

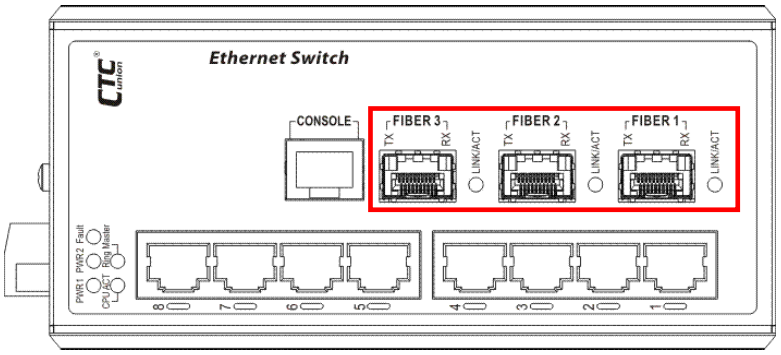


Front of unit

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



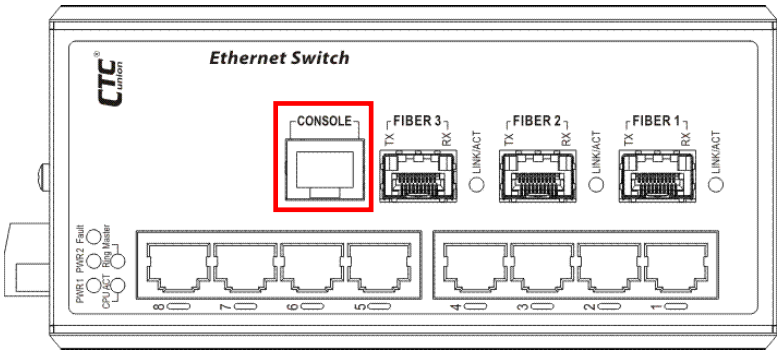
Front of unit

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

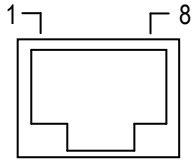
IFS/IGS-803 Series has an asynchronous terminal console port for local management via a serial terminal. The terminal provides management via a CLI (Command Line Interface) which will be familiar to many networking engineers. For most users, the CLI can be used to initially configure TCP/IP access so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



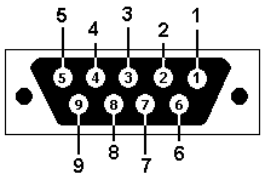
CONSOLE

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.

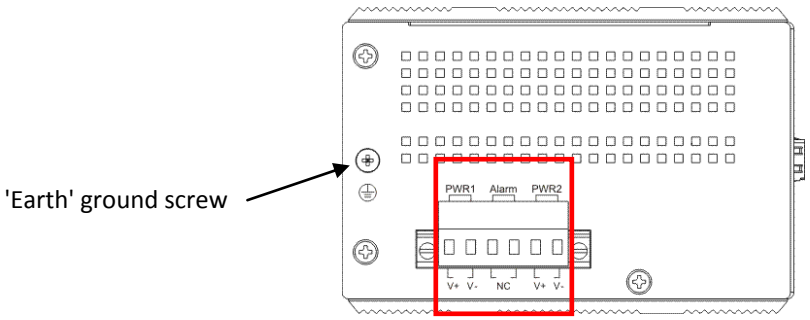
to PC COM Port



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.

A separate 'Earth' grounding terminal is provided for safety grounding of the **IFS/IGS-803**. 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.

A narrow, flat blade screwdriver is required to attach power and alarm lead wires to the terminal block. Ensure that the screws are tight enough to provide a good mechanical grip on the wires to avoid any intermittent power problems.

2.7 LED Indicators

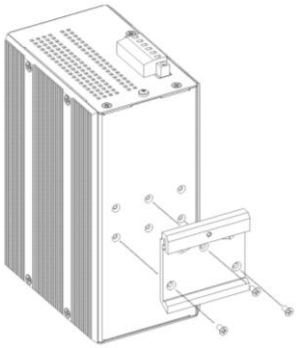
LED	Color	Status	Meaning
PWR 1	Green	On	Lit if power is connected and active at the PWR1 input terminal connection.
		Off	PWR1 input terminal is not connected.
PWR 2	Green	On	Lit if power is connected and active at the PWR2 input terminal connection.
		Off	PWR2 input terminal is not connected.
Fault	Amber	On	Lit when one or more of the programmable alarm conditions is active.
		Off	No programmable alarm conditions are active.
CPU Act	Green	On	During normal use, this green LED will be lit, indicating a healthy condition of the running CPU.
Ring Master	Yellow	On	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).
RJ-45 Link/Act	Green	On	Port link is up and works in 10M/100M.
		Blinking	Traffic is present.
	Amber (For IGS-803 only)	On	Port link is up and works in 1000M.
		Blinking	Traffic is present.
Fiber Link/Act	Green	On	Port link is up and works in 100M.
		Blinking	Traffic is present.
	Amber	On	Port link is up and works in 1000M.
		Blinking	Traffic is present.
PoE (For PoE models only)	Green	On	Lit when the respective LAN port has successfully negotiated PoE and is supplying output power to the remote connected PD device.
		Off	The respective LAN port has not successfully negotiated PoE and does not supply output power to the remote connected PD device.
		Blinking	One of the PoE faults (overload, short circuit, port failure at startup) occurs.

2.8 Installation

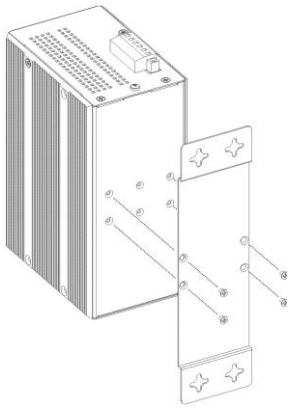
IFS/IGS Series is designed for wall mounting or DIN rail mounting. The units come with both wall mount and DIN rail hardware brackets from the factory.

2.8.1 Mounting

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



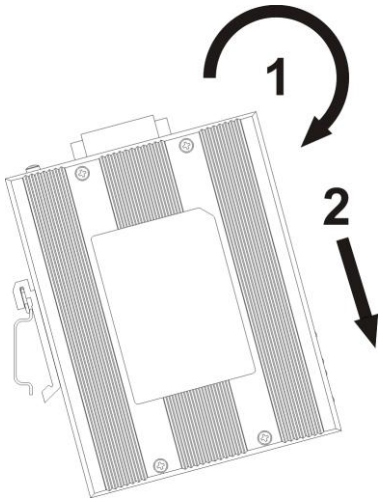
DIN Rail



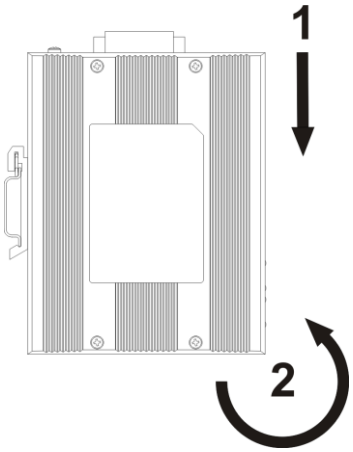
Wall Mount

2.8.2 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 Introduction

The **IFS/IGS-803SM Series** of industrial Ethernet switches provide a number of configuration/management methods. The first and very basic is serial console access. This method is only available when a terminal can be physically connected to the local **IFS/IGS-803SM Series** switch at the CONSOLE port.

The second method of configuration/management uses a Web Browser. This requires that networking be configured so that the device can be accessed via a LAN port. Accessing the **IFS/IGS-803SM** from a network allows for both local and remote management.

The 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-803SM** 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-803SM 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-803SM**.

3.2 CONSOLE Operation

Using the provided accessory cable, connect the **IFS/IGS-803** "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.

RedBoot> fi lo -d managed
Image loaded from 0x80040000-0x809d2a04
RedBoot> go

Username: admin
Password:

Welcome to CTC Union Command Line Interface (v1.0).
Type 'help' or '?' to get help.
>
```

3.2.1 CLI Online Help

While using the CLI, online help is always available by using 'help' command or typing '?' (question mark). Commands can be recalled by using the 'up/down arrow keys'.

NOTE: *When making corrections while typing, please be aware that unless the terminal emulation program specifically issues a [CTRL-H] for [Backspace] that the backspace action must use the key combination of [CTRL-H] as the [Backspace] character is not recognized by the CLI.*

```
> ?
General Commands:
-----------------
Help/?: Get help on a group or a specific command
Up    : Move one command level up
Logout: Exit CLI

Command Groups:
---------------
System       : System settings and reset options
IP           : IP configuration and Ping
Port         : Port management
MAC          : MAC address table
VLAN         : Virtual LAN
PVLAN        : Private VLAN
Security     : Security management
STP          : Spanning Tree Protocol
Aggr         : Link Aggregation
LACP         : Link Aggregation Control Protocol
LLDP         : Link Layer Discovery Protocol
LLDPMED      : Link Layer Discovery Protocol Media
GreenEthernet: Power savings features
PoE          : Power Over Ethernet
EPS          : Ethernet Protection Switching
MEP          : Maintenance entity End Point
QoS          : Quality of Service
Mirror       : Port mirroring
Config       : Load/Save of configuration via TFTP
Firmware     : Download of firmware via TFTP
UPnP         : Universal Plug and Play
MVR          : Multicast VLAN Registration
ERPS         : Ethernet Ring Protection Switching
Loop Protect : Loop Protection
IPMC         : MLD/IGMP Snooping
VCL          : VLAN Control List

Type '<group>' to enter command group, e.g. 'port'.
Type '<group> ?' to get list of group commands, e.g. 'port ?'.
Type '<command> ?' to get help on a command, e.g. 'port mode ?'.
Commands may be abbreviated, e.g. 'por co' instead of 'port configuration'.
>
```

3.2.2 TCP/IP Configuration via CLI

3.2.2.1 IP Address

syntax: IP Address <vlan> <ip_ifaddr>

```
>ip address 1 192.168.0.250/24
>
```

Note: The default <vlan> for untagged packets is VID 1.
The <ip_ifaddr> parameter must include the subnet class attribute.
Common class attributes include:
/30 = 255.255.255.252
/29 = 255.255.255.248
/28 = 255.255.255.240
/24 = 255.255.255.0
/16 = 255.255.0.0
/8 = 255.0.0.0

3.2.2.2 Default Gateway

syntax: IP Route Add <ip_net> <ip_gateway>

```
>ip route add 0.0.0.0/0 192.168.0.254
>
```

Note: The <ip_net> parameter must include the subnet mask class. A default gateway would use '0'.
In this example the <ip_gateway> is the default router for the subnet.

3.2.2.3 DNS Server

syntax: IP DNS Conf <dns_source>

```
>ip dns conf 192.168.0.1
>
```

Note: The <dns_source> parameter points to the static DNS server for the network.

3.2.2.4 Display TCP/IP Settings

syntax: IP Configuration
IP DNS Conf
IP Route List

```
>ip configuration
Mode: router
vlan1: mtu=1500 IPv4=192.168.0.250/24
route  0: IPv4 {network = 0.0.0.0/24, destination = 192.168.0.10}
>ip dns conf
Static dns server: 192.168.0.1
>ip route list
0.0.0.0/24 via VLAN1:192.168.0.254 <UP GATEWAY HW_RT>
127.0.0.1/32 via OS:lo:127.0.0.1 <UP HOST>
192.168.0.0/24 via VLAN1 <UP HW_RT>
224.0.0.0/4 via OS:lo:127.0.0.1 <UP>
::1/128 via OS:lo:::1 <UP HOST>
fe80:1::/128 via OS:lo:fe80:1::1 <UP>
fe80:1::1/128 via OS:lo <UP HOST>
fe80:2::/128 via VLAN1 <UP>
fe80:2::202:abff:fe01:203/128 via OS:lo:2:ab01:203:: <UP HOST>
ff01:1::/128 via OS:lo:::1 <UP>
ff01:2::/128 via VLAN1 <UP>
ff02:1::/128 via OS:lo:::1 <UP>
ff02:2::/128 via VLAN1 <UP>
```

3.2.3 Factory Default

syntax: System Restore Default <keep_ip>

```
>system restore default
>
```

Note: To restore factory default but keep TCP/IP settings, use: "system restore default keep_ip"

3.2.4 Reboot Device

syntax: System Reboot

```
>system reboot
>
```

3.2.5 Admin Password

syntax: Security Switch Users Add <username> <password> <privilege_level>

```
>security switch add admin secret 15
>
```

Note: sets the password "secret" for the admin user. (Admin user has highest privilege level of 15.)
To clear admin password, use a pair of double quotes to enter a null password.

```
>security switch add admin "" 15
>
```

3.2.6 Logout

syntax: Logout

```
>logout

Username:
```

Note: After the logout command is issued, the "Username:" login prompt will again be displayed.

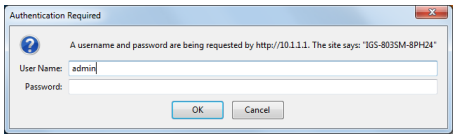
CHAPTER 4. WEB OPERATION & CONFIGURATION

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.

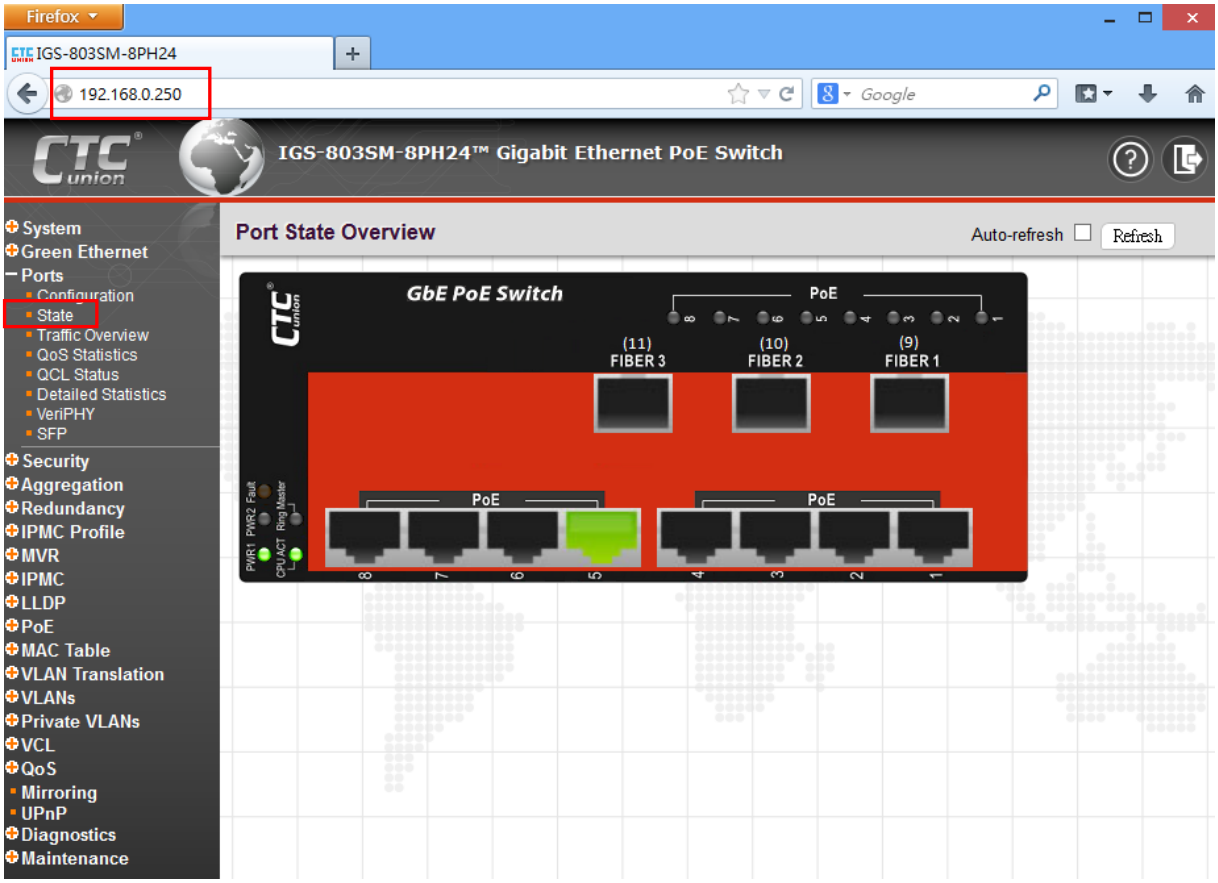
4.1.1 Login

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

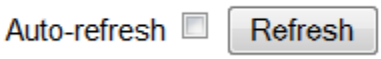
4.1.2 Port Status

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.

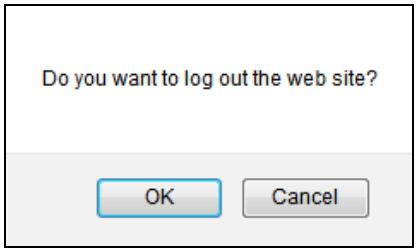
4.1.4 Help System

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.

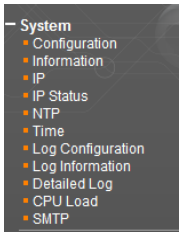
After clicking the logout icon, a confirmation screen will be displayed. Click "OK" to finish logging out or click "Cancel" to return to the web configuration GUI.



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.

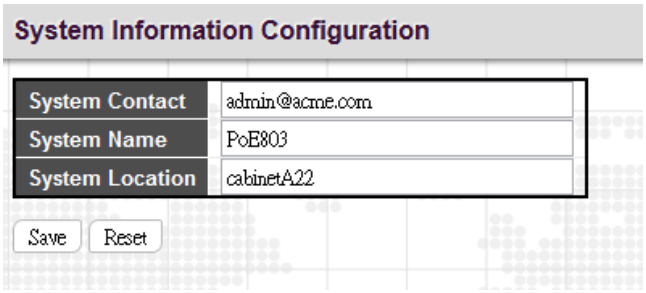
4.2 System

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.



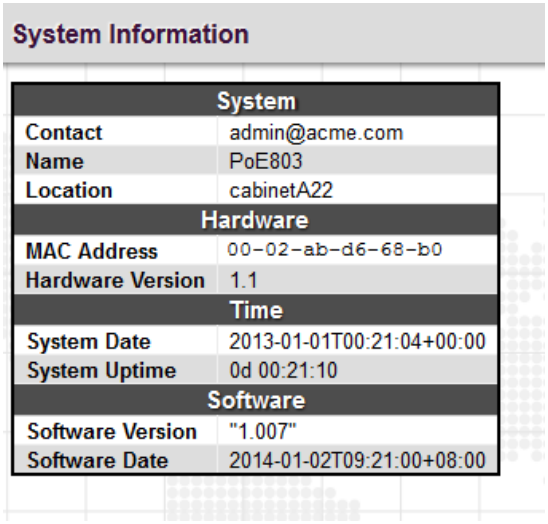
System Contact: Indicate the descriptive contact information. This could be a person’s name, email address or other descriptions. The allowed string length is 0~255 and the allowed content is the ASCII characters from 32~126.

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.

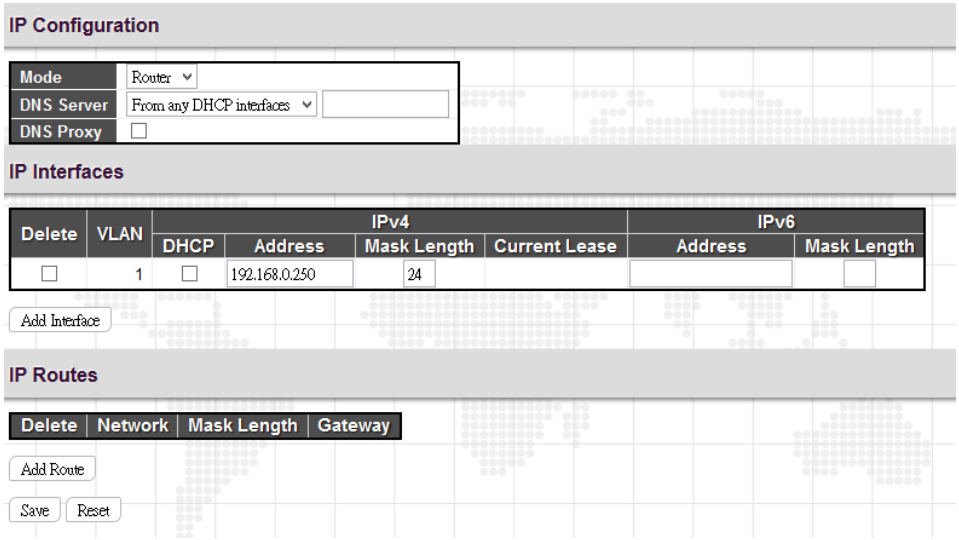
4.2.2 System Information

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

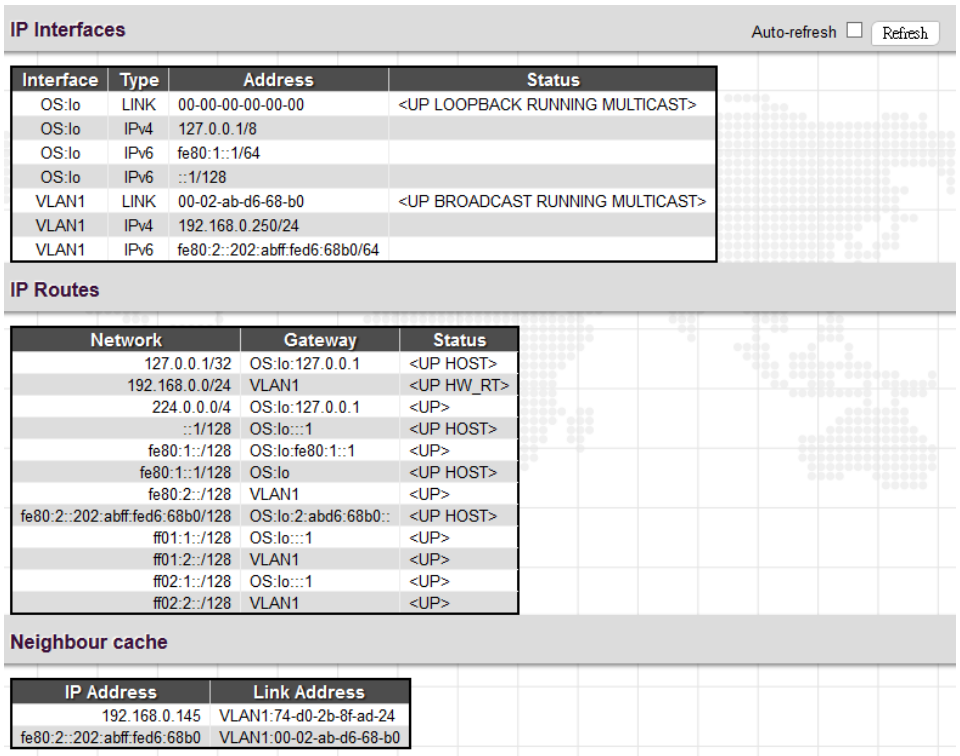
Route Network: The IP route is the destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or for IPv6 use the :: notation.

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>

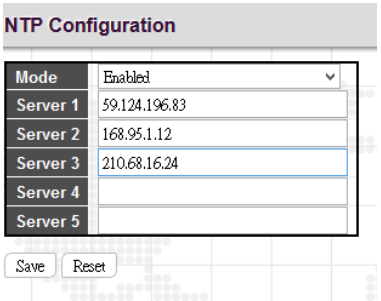
Neighbour cache

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.

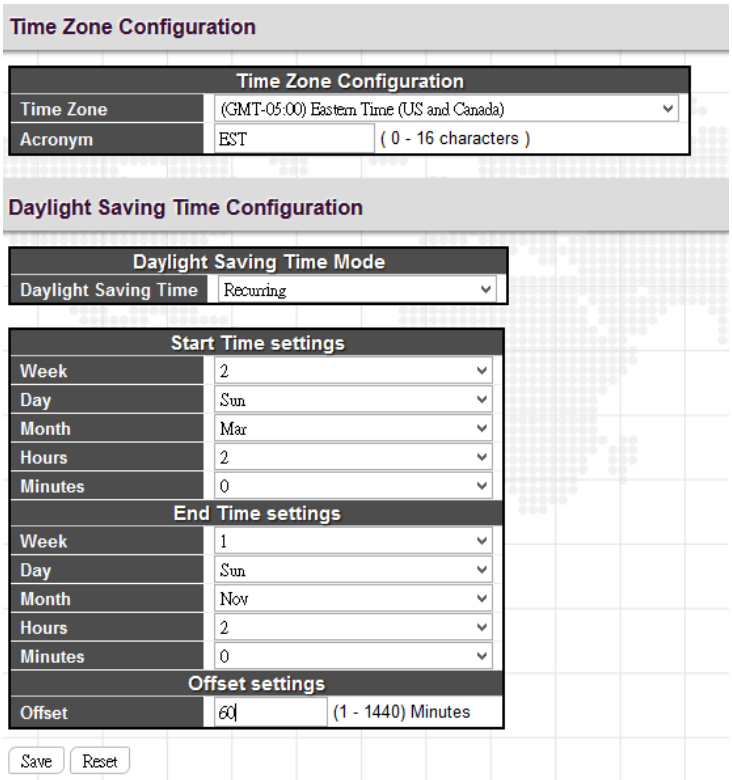
Disabled: Disable NTP client mode operation.

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).

Time Zone Configuration

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

Acronym: Set the acronym of the time zone.

Daylight Saving Time Configuration

Daylight Saving Time: This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select “Disable” to disable the Daylight Saving Time configuration. Select “Recurring” and configure the Daylight Saving Time duration to repeat the configuration every year. Select “Non-Recurring” and configure the Daylight Saving Time duration for single time configuration. (Default is Disabled)

Recurring & Non-Recurring Configurations:

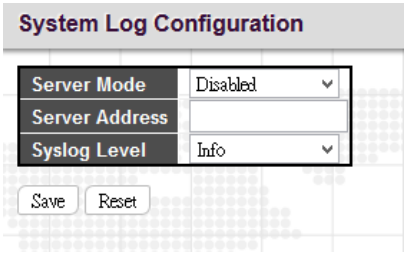
Start time settings: Select the starting week, day, month, year, hours, and minutes.

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

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

4.2.7 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:

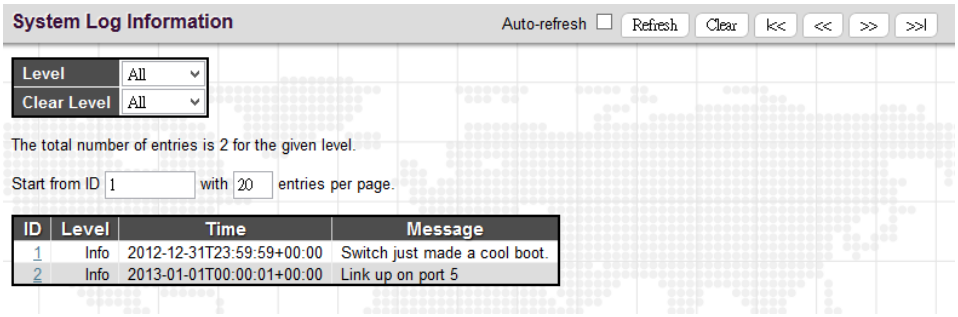
Info: Send information, warnings and errors.

Warning: Send warnings and errors.

Error: Send errors only.

4.2.8 System Log Information

Displays the collected log information.



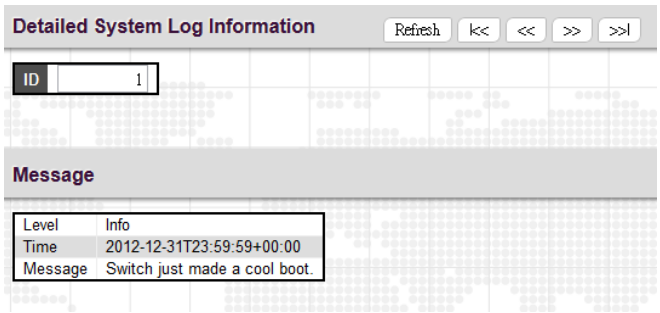
Level: Use this pull down to display all messages or messages of type info, warning or error.

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

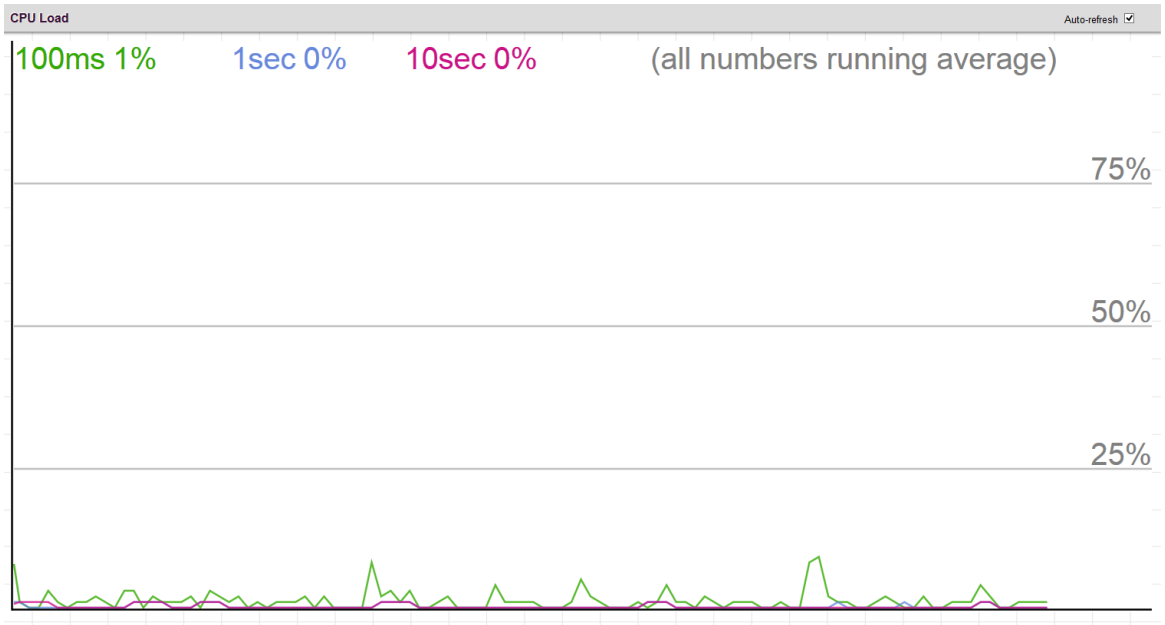
Displays individual log records.



View each log, by ID number.

4.2.10 System CPU Load

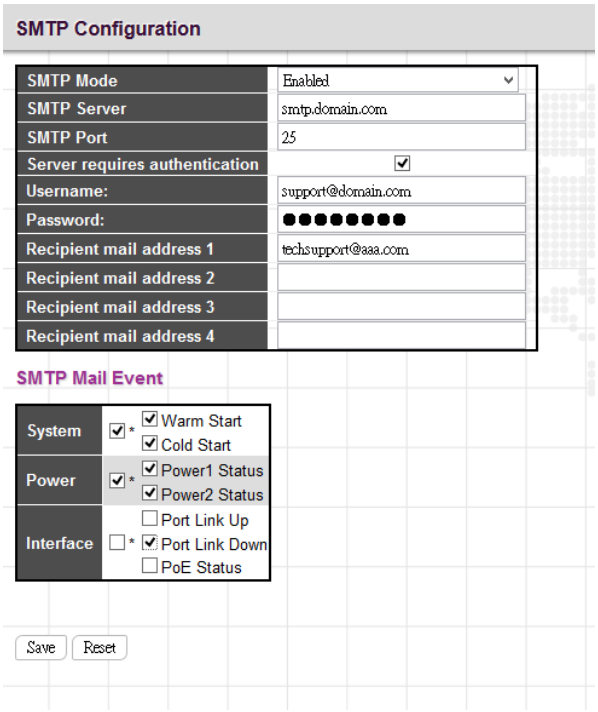
This page displays the CPU load, using an SVG graph.



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:

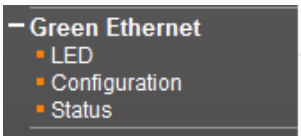
Port Link Up: Enable/disable Port Link up mail event.

Port Link Down: Enable/disable Port Link down mail event.

PoE Status: Enable/disable PoE Status mail event.

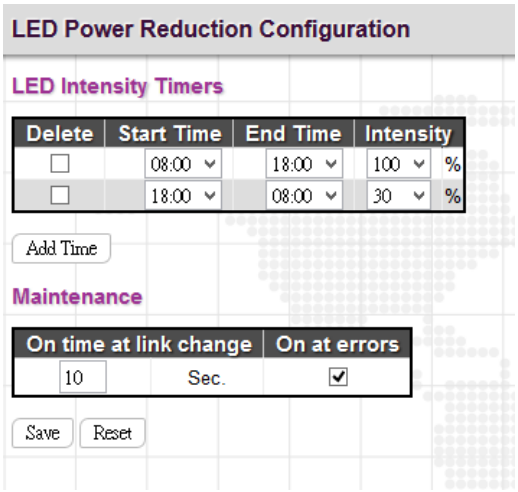
4.3 Green Ethernet

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.

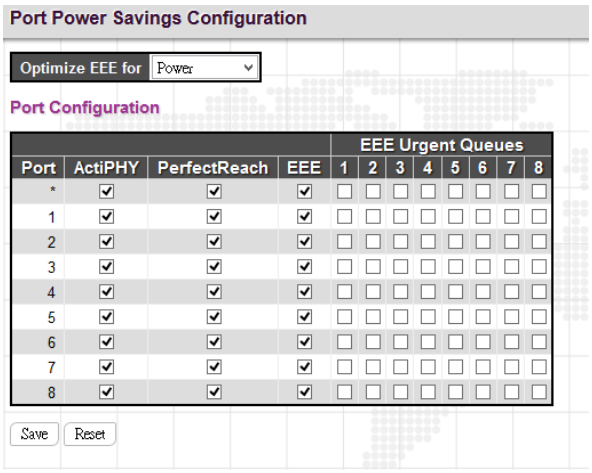


The LED light intensity may be adjusted in a percentage of intensity during programmable time periods. In the above setting example, the LED intensity has been adjusted to 50% during daylight hours and reduced to only 10% intensity during night hours.

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.



Port Power Savings Configuration

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.

Port Configuration

ActiPHY™: ActiPHY™ works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if an Ethernet cable is inserted. For ports with no cable connection, the PHY remains powered down to save energy.

PerfectReach™: PerfectReach™ is another power saving mechanism. PerfectReach™ works by determining the cable length and lowering the Ethernet transmit power for ports with short cables.

EEE (Energy-Efficient Ethernet): EEE is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE was developed through the IEEE802.3az task force of the Institute of Electrical and Electronic Engineers (IEEE). EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is called wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP (Link Layer Discovery Protocol) protocol. EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode. For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic. For traffic that should not be held back, urgent queues may be assigned to reduce latency yet still result in overall power saving.

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

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

4.3.3 Green Ethernet Status

Display the energy saving status for all ports.

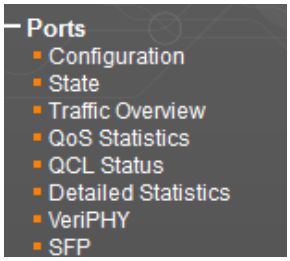
Port Power Savings Status

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.

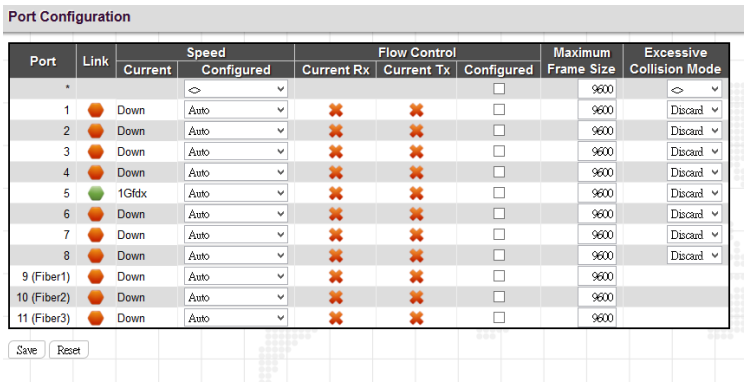
4.4 Ports

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.

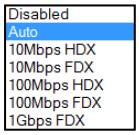


Port: This device is a industrial switch with 8 electrical LAN ports numbered 1~8 and 3 fiber optical ports (for SFP modules) numbered 9~11. Each logical port number is displayed in a row. The select all "*" port will apply actions on all ports.

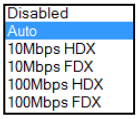
Link: The current link state for each port is displayed graphically. Green indicates the link is up and red that it is down.

Current Speed: This column provides the current link speed (10, 100, 1G) and duplex (fdx=Full Duplex, hdx=Half Duplex) of each port.

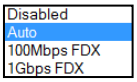
Configured Speed: This pull down selects any available link speed for the given switch port. Only speeds supported by the specific port are shown.



Options for **IGS803SM**



Options for **IFS803GSM**



Fiber options **IFS/IGS803**

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).

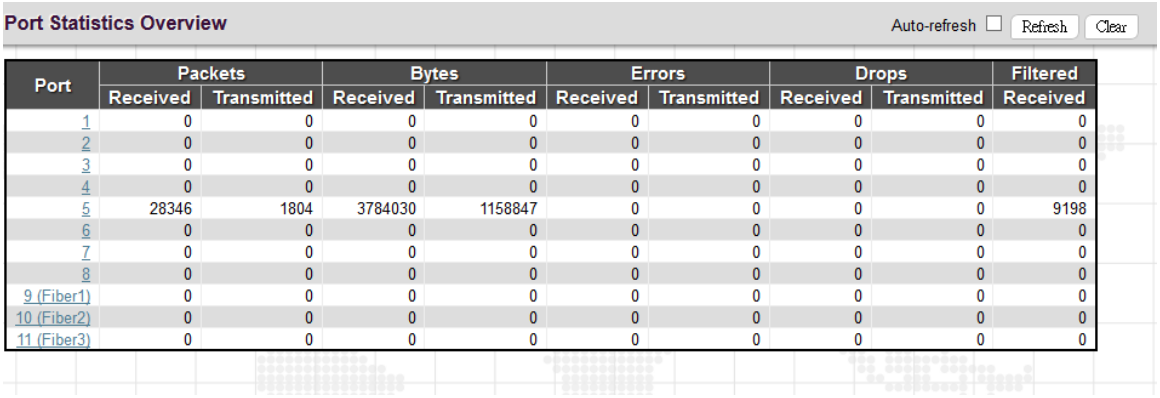
4.4.2 Ports State

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.

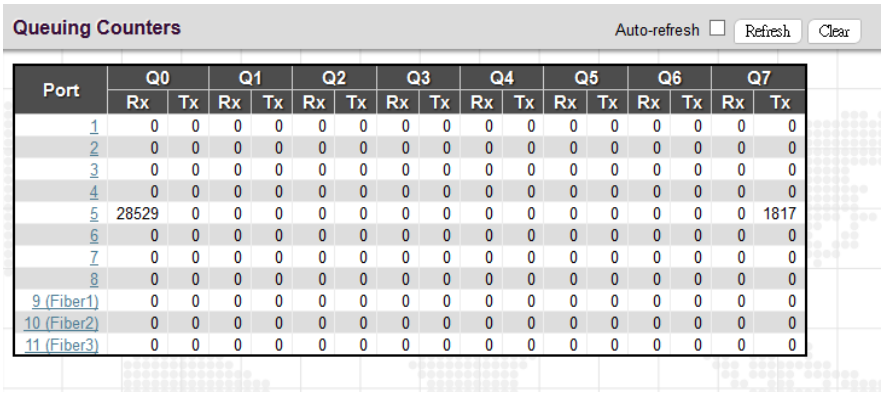
Drops: The number of frames discarded due to ingress or egress congestion.

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:

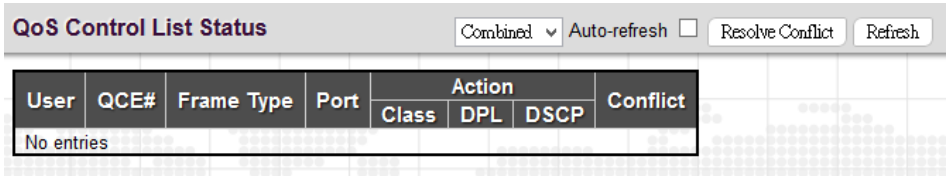
Port: The logical port for the settings contained in the same row.

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.

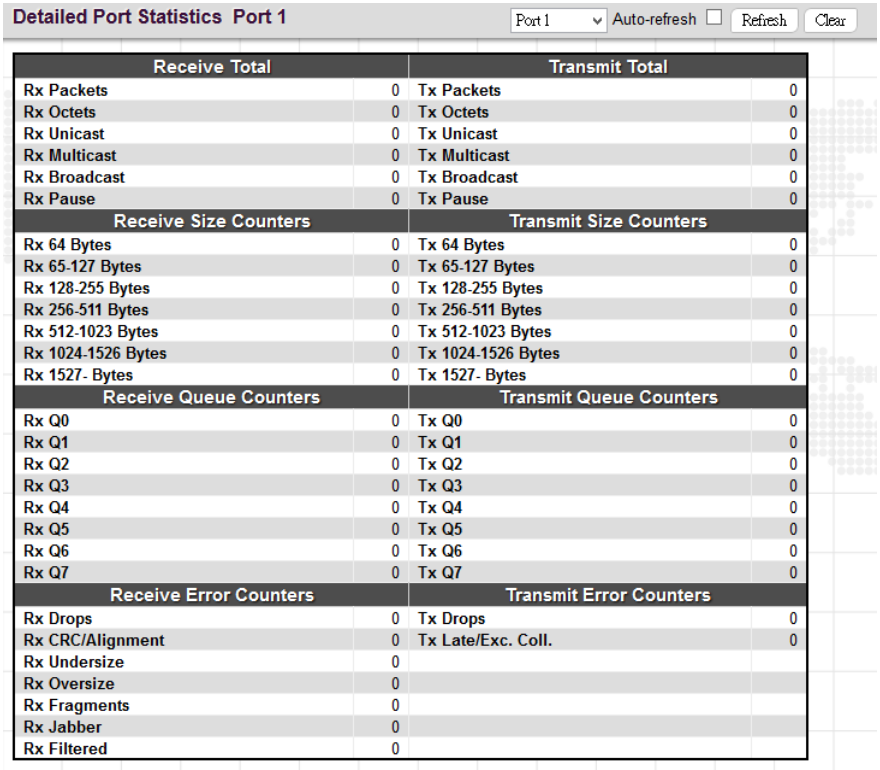
DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.

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.



Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Receive Total and Transmit Total

Rx and Tx Packets: The number of received and transmitted (good and bad) packets.

Rx and Tx Octets: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast: The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast: The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast: The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause: A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE.

Receive and Transmit Size Counters: 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.

Receive Error Counters

Rx Drops: The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment: The number of frames received with CRC or alignment errors.

Rx Undersize: The number of short [1] frames received with valid CRC.

Rx Oversize: The number of long [2] frames received with valid CRC.

Rx Fragments: The number of short [1] frames received with invalid CRC.

Rx Jabber: The number of long [2] frames received with invalid CRC.

Rx Filtered: The number of received frames filtered by the forwarding process.

[1] Short frames are frames that are smaller than 64 bytes.
[2] Long frames are frames that are longer than the configured maximum frame length for this port.

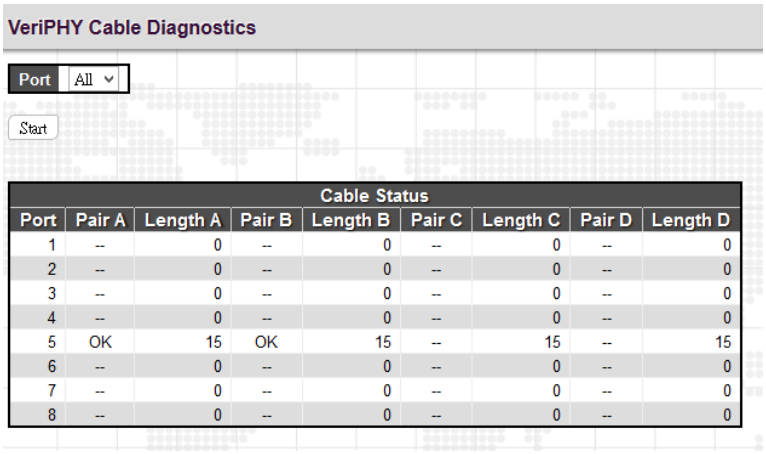
Transmit Error Counters

Tx Drops: The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.: The number of frames dropped due to excessive or late collisions.

4.4.7 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".



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

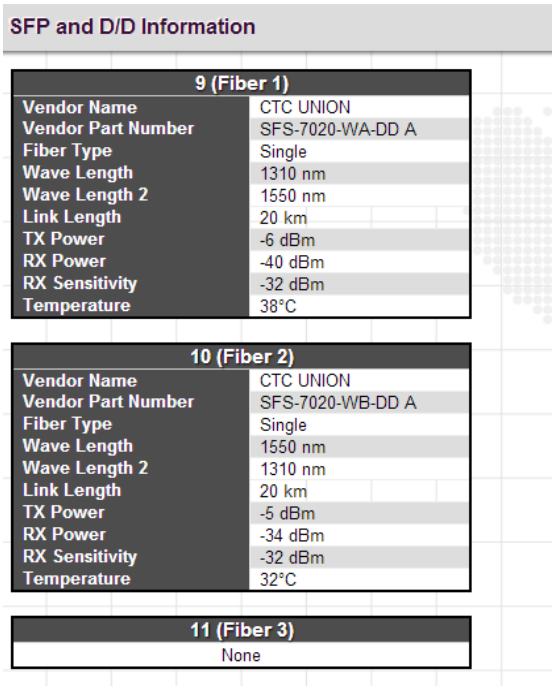
Cross D: Abnormal cross-pair coupling with pair D

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.



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).

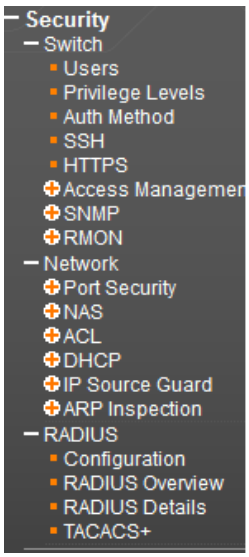
RX Power: The receive optical power is reported by SFP that support DDI.

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

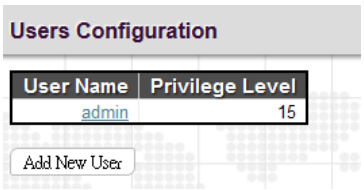
Under the security heading are three major icons, switch, network and RADIUS.



4.5.1 Switch

4.5.1.1 Users

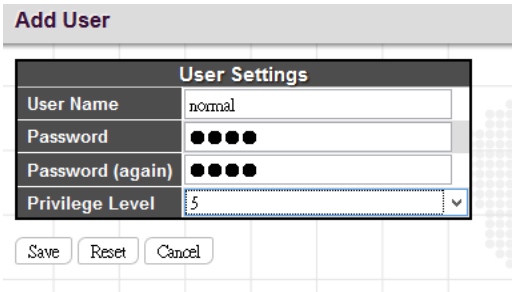
This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.



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.

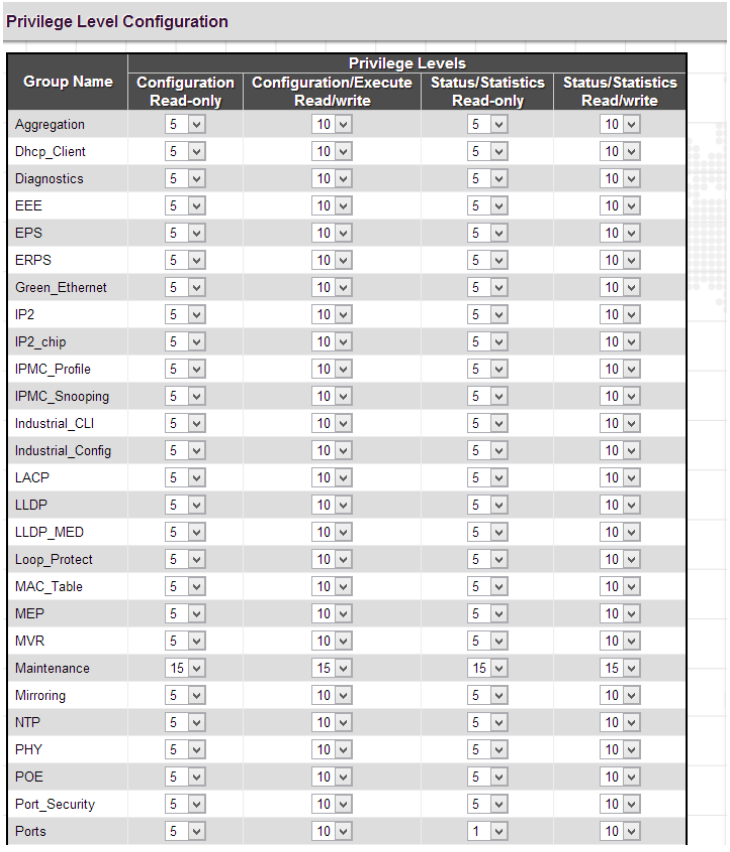
Password: Enter the password for this user account.

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.



Group Name: This name identifies the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:

System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.

IP: Everything except 'ping'.

Port: Everything except 'VeriPHY'.

Diagnostics: 'ping' and 'VeriPHY'.

Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

Debug: Only present in CLI.

Privilege Levels: Every group has an authorization Privilege level for the following sub groups:

configuration read-only

configuration/execute read-write

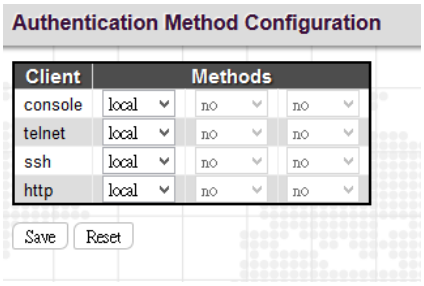
status/statistics read-only

status/statistics read-write (e.g. for clearing of statistics)

User Privilege should be the same or greater than the authorization Privilege level to have access to that group.

4.5.1.3 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.

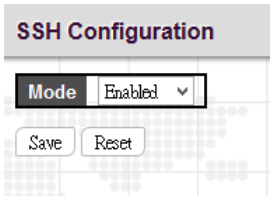
radius: Use remote RADIUS server(s) for authentication.

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:

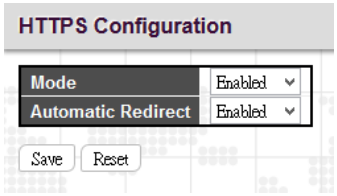
Enabled: Enable SSH mode operation. By default, SSH mode operation is enabled.

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:

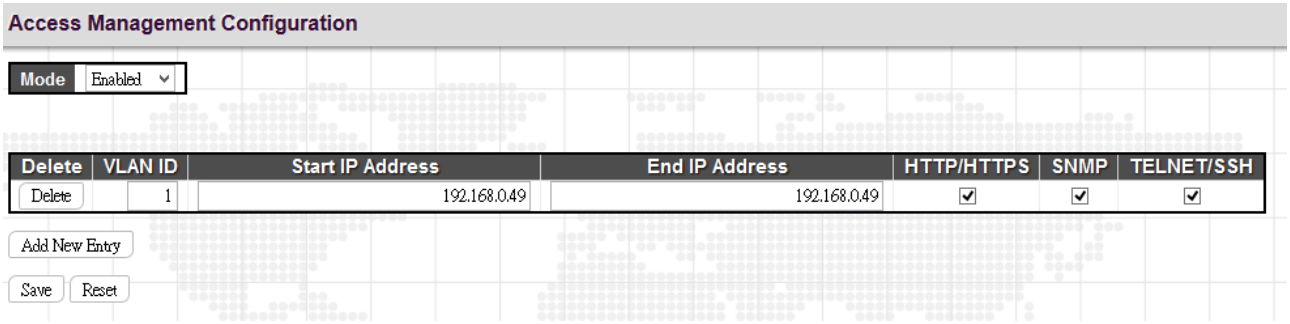
Enabled: Enable HTTPS redirect mode operation.

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.

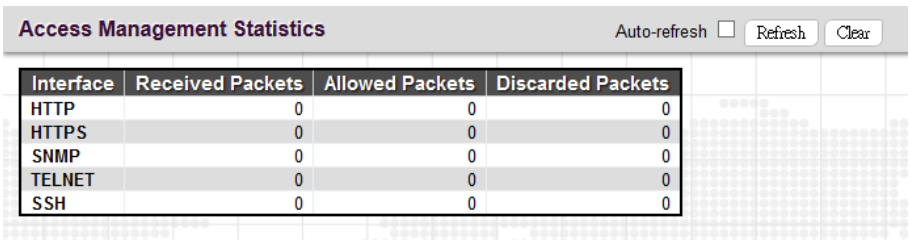
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

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: 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.

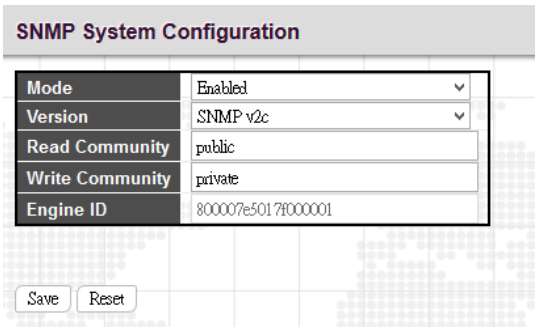
Allowed Packets: The number of allowed packets from the interface when access management mode is enabled.

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.

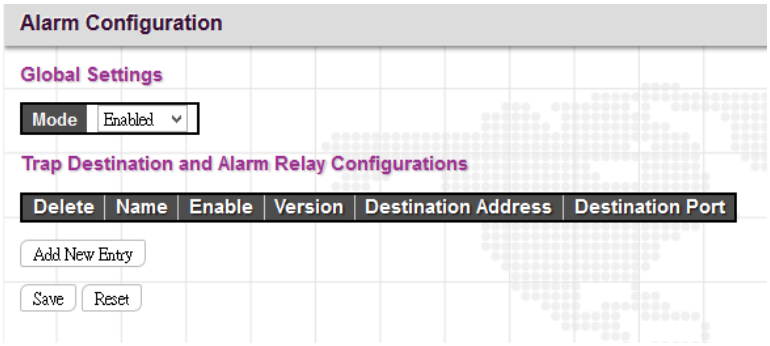
Read Community: Indicates the community read access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E.

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

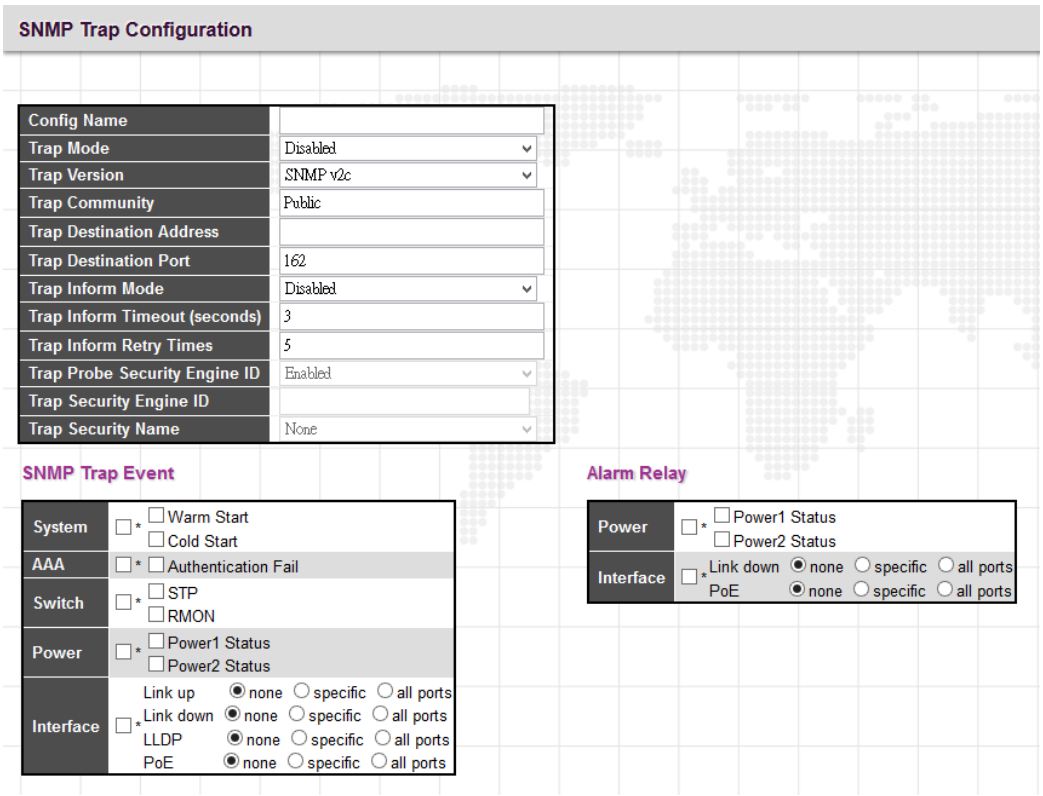
Configure SNMP trap on this page.



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:

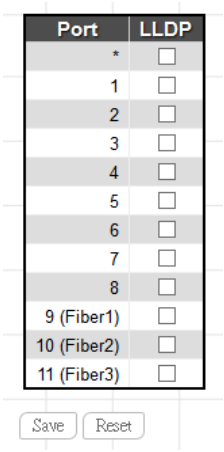
Link Up: none/specific/all ports Link up trap.

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.

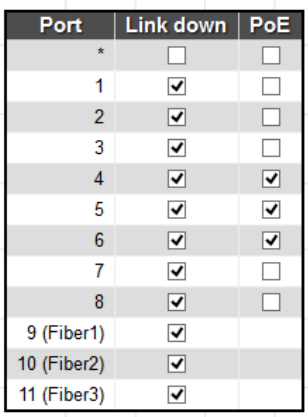
Power 2 Status: Select the checkbox to enable Power 2 status alarm relay function. Once power 2 fails, the alarm relay contacts are open and Fault LED indicator is on in amber. Clear the checkbox to disable Power 2 status alarm relay.

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.

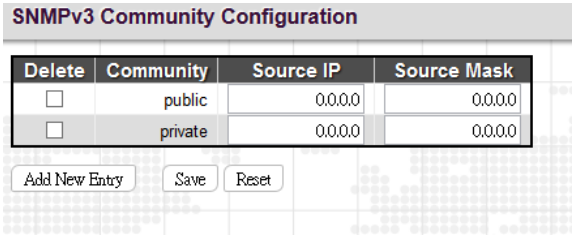


Port	Link down	PoE
*	☐	☐
1	☑	☐
2	☑	☐
3	☑	☐
4	☑	☑
5	☑	☑
6	☑	☑
7	☑	☐
8	☑	☐
9 (Fiber1)	☑	
10 (Fiber2)	☑	
11 (Fiber3)	☑	

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.



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

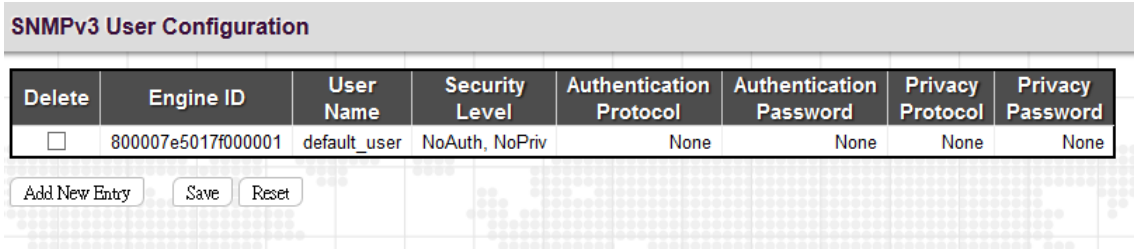
Community: Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string. This string is case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



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.

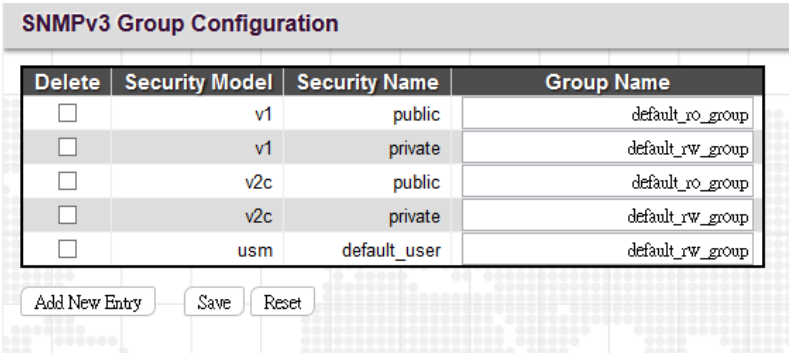
Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

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.

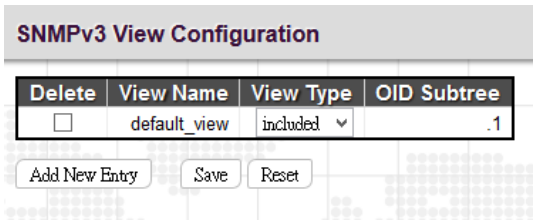
usm: User-based Security Model (USM) for SNMPv3.

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:

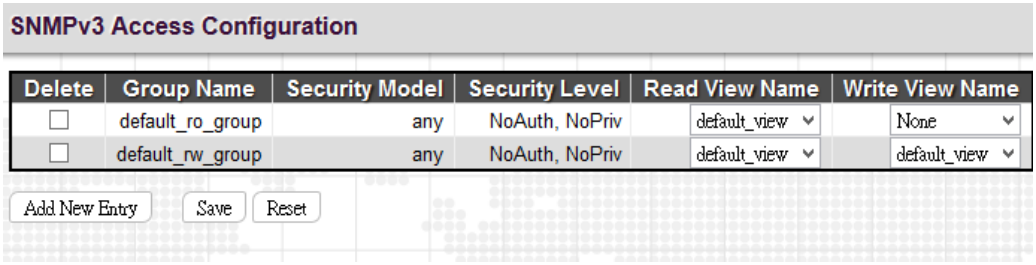
included: An optional flag to indicate that this view subtree should be included.

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.

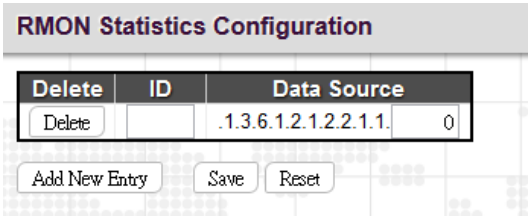
Read View Name: The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

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.



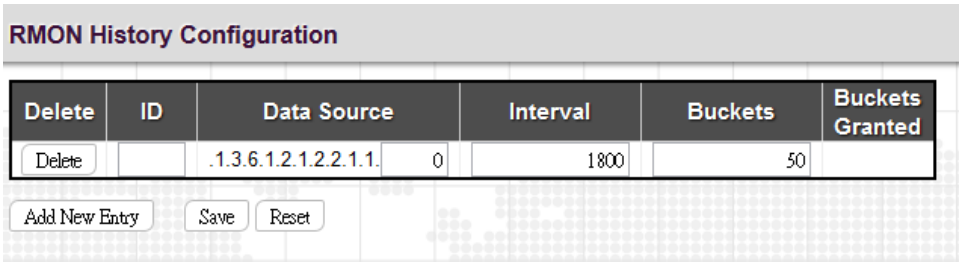
Delete: Check to delete the entry. It will be deleted during the next save.

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.

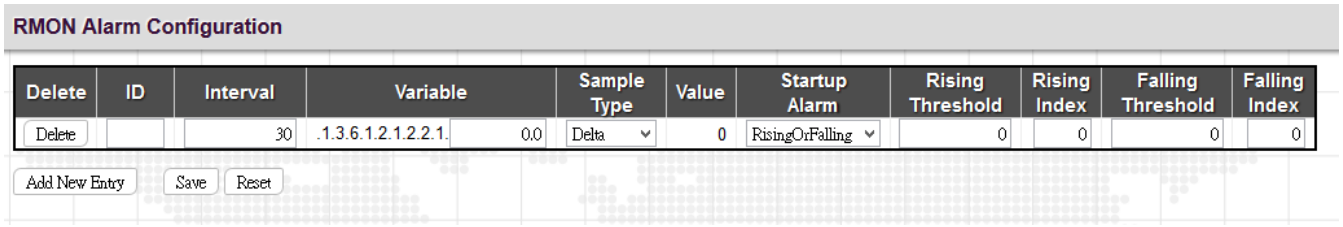
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

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.

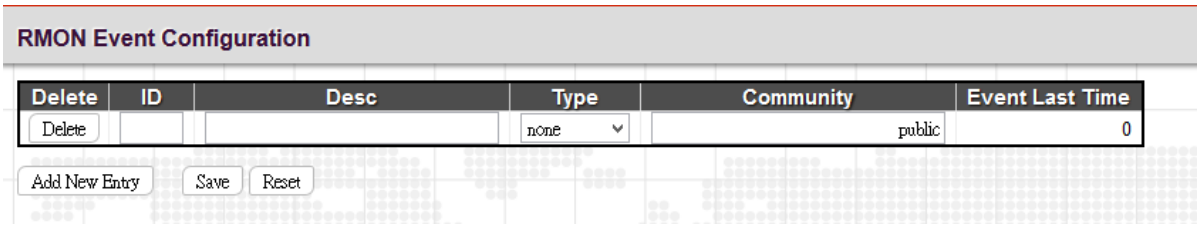
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

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.

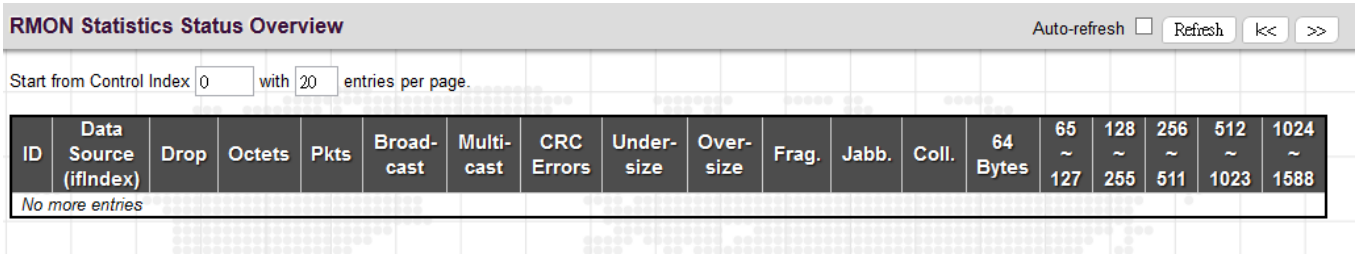
logandtrap: Logs an event and sends a trap message.

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.

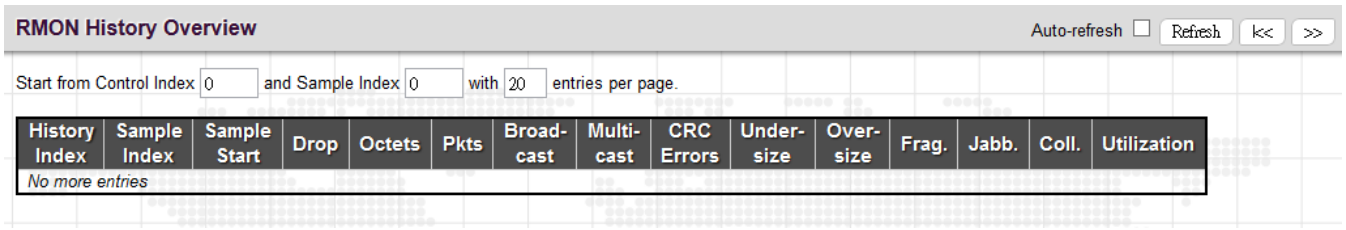
Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

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.

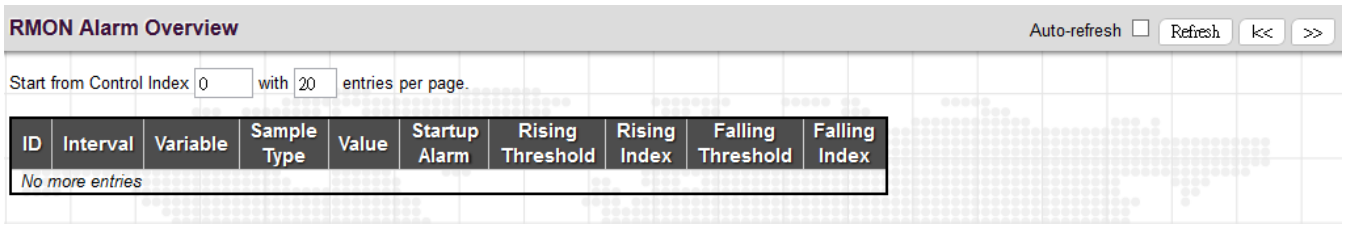
Frag.: The number of frames which size is less than 64 octets received with invalid CRC.

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.

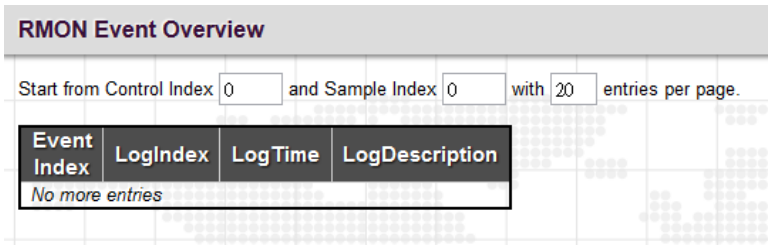
Rising Threshold: If the current value is greater than the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated.

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.

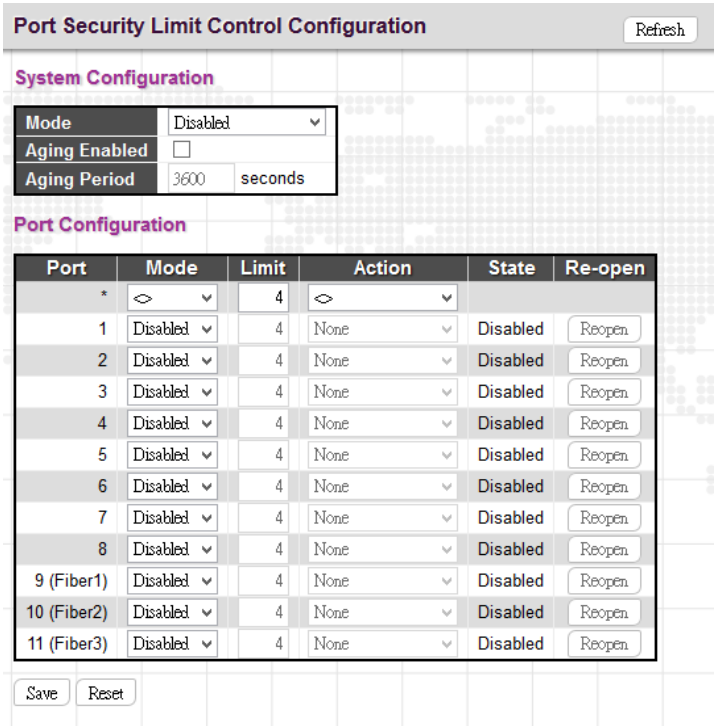
Log Description: Display Event description.

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.

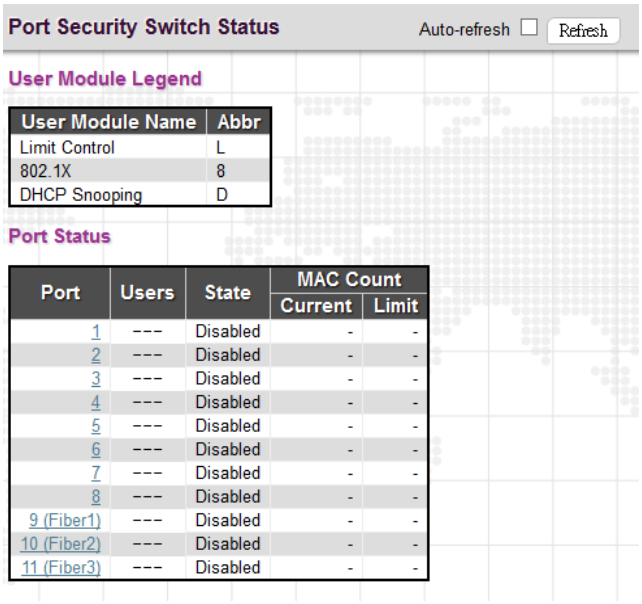
Ready: The limit is not reached yet.

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



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.

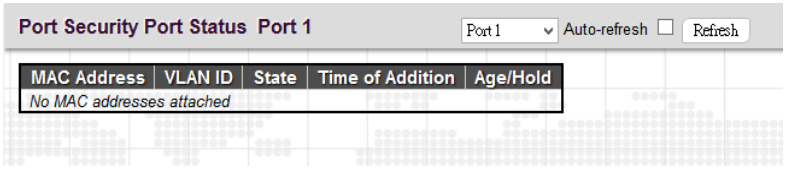
Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

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 Statistics



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.

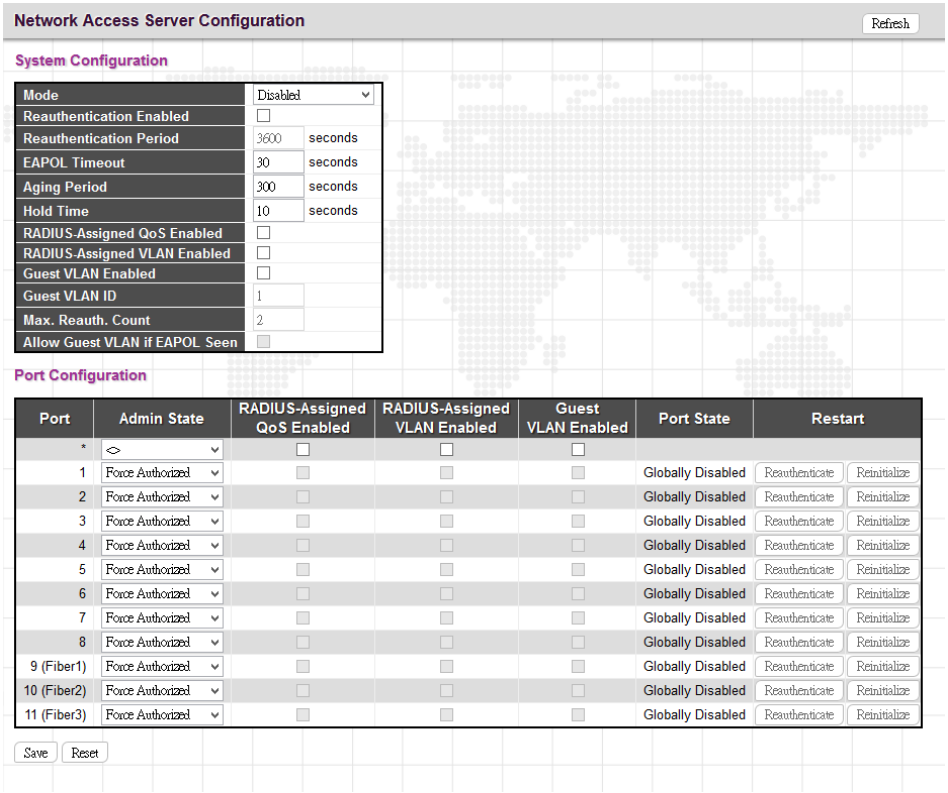
Age/Hold: If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check 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.

4.5.5.2 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.

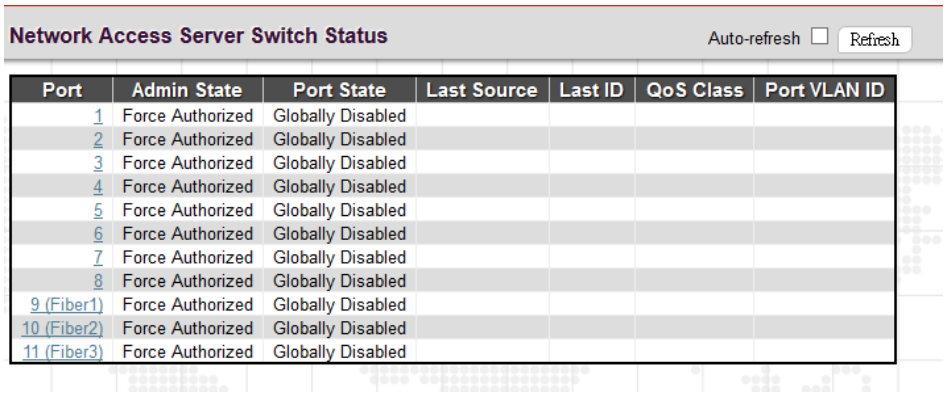
X Auth/Y Unauth: The port is in a multi-supplicant mode. X clients are authorized and Y are unauthorized.

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



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.

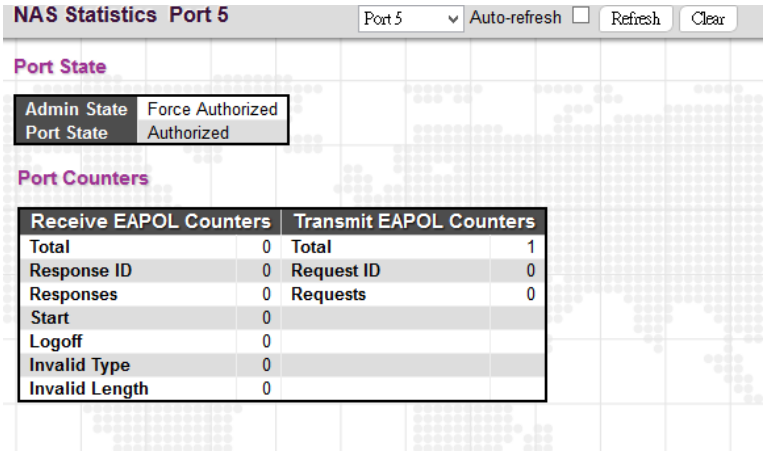
Last Source: The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication.

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



Port State

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.

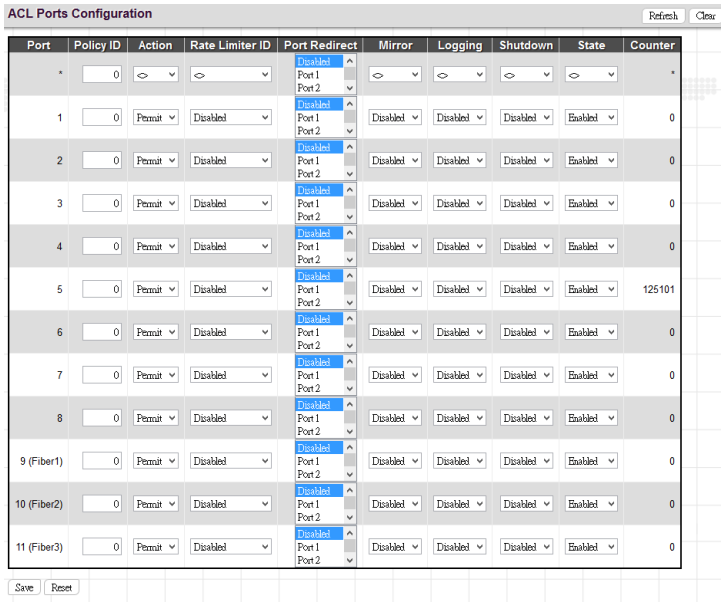
Request ID: The number of valid EAPOL Request Identity frames that have been received by the switch.

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.

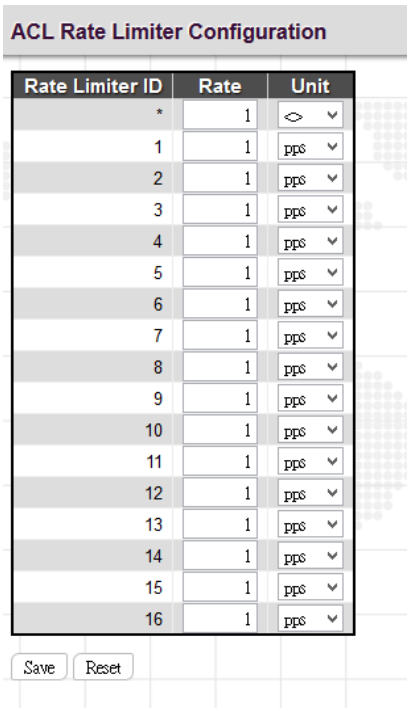
State: Select a port state.

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



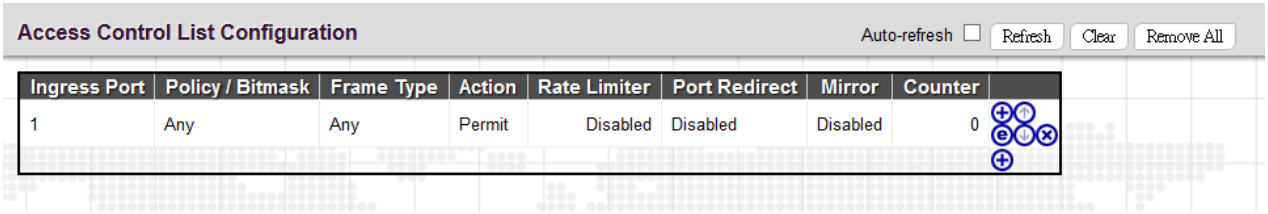
Rate Limiter ID: Display every rate limiter ID.

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.



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.

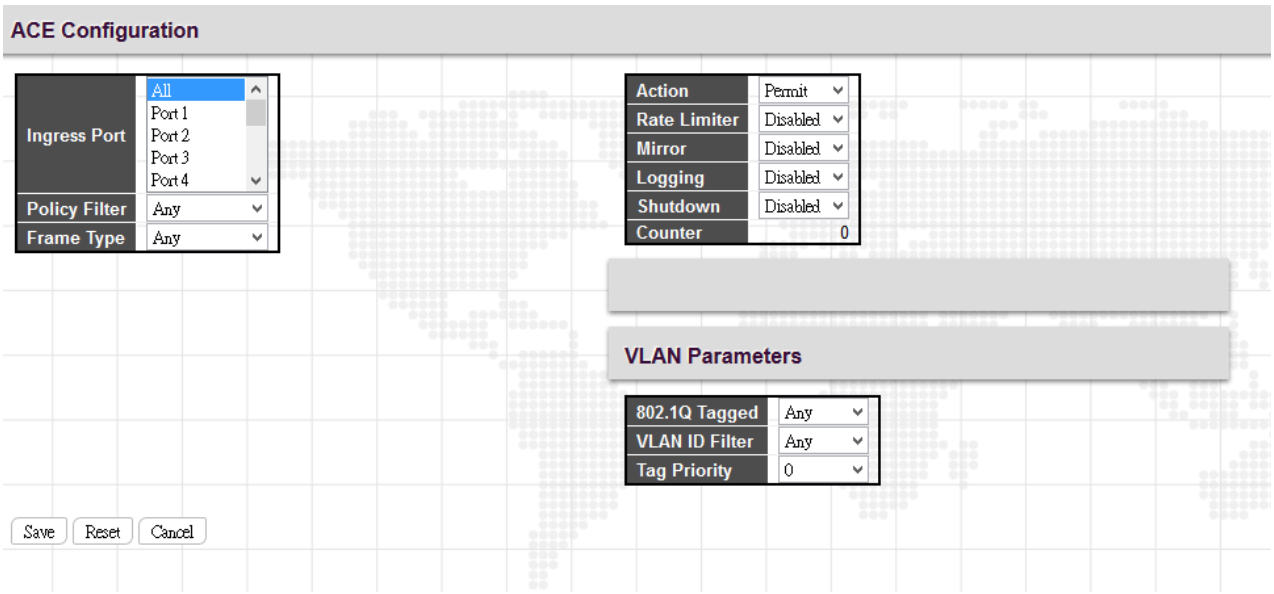
Rate Limiter: Display rate limiter is enabled or disabled when matched frames are found.

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.

IP Parameters

IP Protocol Filter: Select "Any", "ICMP", "UDP", "TCP", or "Other" protocol from the pull-down menu for IP Protocol filtering.

IP TTL: Select "Zero" to indicate that the TTL filed in IPv4 header is 0. If the value in TTL field is not 0, use "Non-Zero" to indicate that. You can also select "any" to denote the value which is either 0 or not 0.

IP Fragment: Select "Any" to allow any values. "Yes" denotes that IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must match this entry. "No" denotes that IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not match this entry.

IP Option: Specify the options flag setting for this rule. Select "Any" to allow any values. "Yes" denotes that IPv4 frames where the options flag is set must match this entry. "No" denotes that Pv4 frames where the options flag is set must not match this entry

SIP Filter: Select "Any", "Host", or "Network" for source IP filtering. If "Host" is selected, you need to indicate a specific host IP address. If "Network" is selected, you need to indicate both network address and subnet mask.

SIP Address: Specify a source IP address.

SIP Mask: Specify a source subnet mask.

DIP Filter: Select “Any”, “Host”, or “Network” for destination IP filtering. If “Host” is selected, you need to indicate a specific host IP address. If “Network” is selected, you need to indicate both network address and subnet mask.

DIP Address: Specify a destination IP address.

DIP Mask: Specify a destination subnet mask.

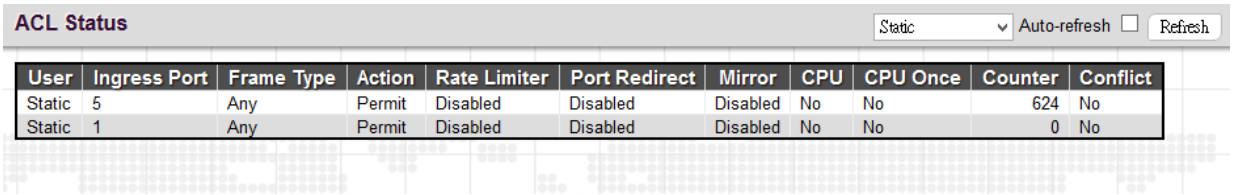
IPv6 Parameters

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

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

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

4.5.5.3.4 ACL Status



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

User: Display the ACL user.

Ingress Port: Display the ingress port of the ACE. This field could be all ports, a specific port or a range of ports.

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.

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

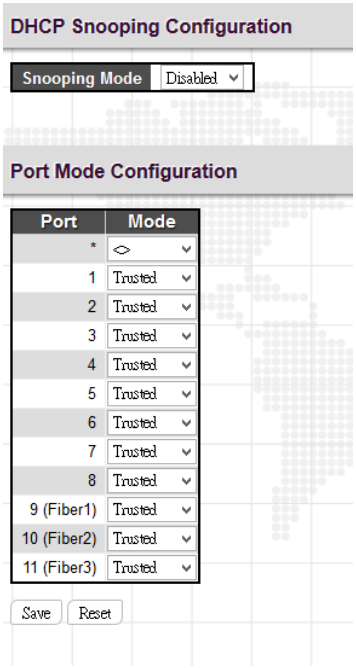
Counter: The counter indicates the number of times the ACE was hit by a frame.

Conflict: Indicate the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

4.5.5.4 DHCP

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.

4.5.5.4.1 Snooping Configuration



DHCP Snooping Configuration

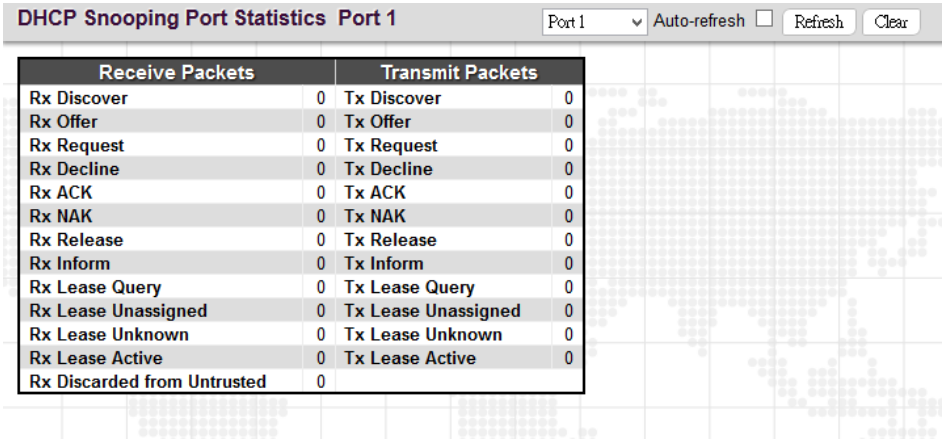
Snooping Mode: Enable or disable DHCP Snooping function globally. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

Port Mode Configuration

Port: Port number. "Port *" rules apply to all ports.

Mode: Select the DCHP Snooping port mode. Ports can be set to either “Trusted” or “Untrusted”.

4.5.5.4.2 Snooping Statistics



Rx and Tx Discover: The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer: The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request: The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline: The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK: The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK: The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release: The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform: The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query: The number of lease query (option 53 with value 10) packets received and transmitted.

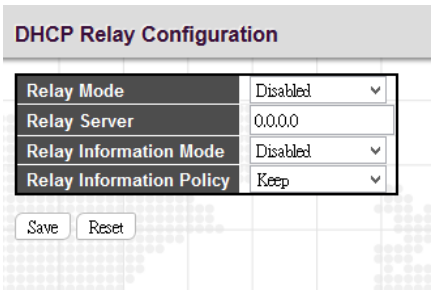
Rx and Tx Lease Unassigned: The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown: The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active: The number of lease active (option 53 with value 13) packets received and transmitted.

Rx and Tx Discarded from Untrusted: The number of discarded packet that are coming from untrusted port.

4.5.5.4.3 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.

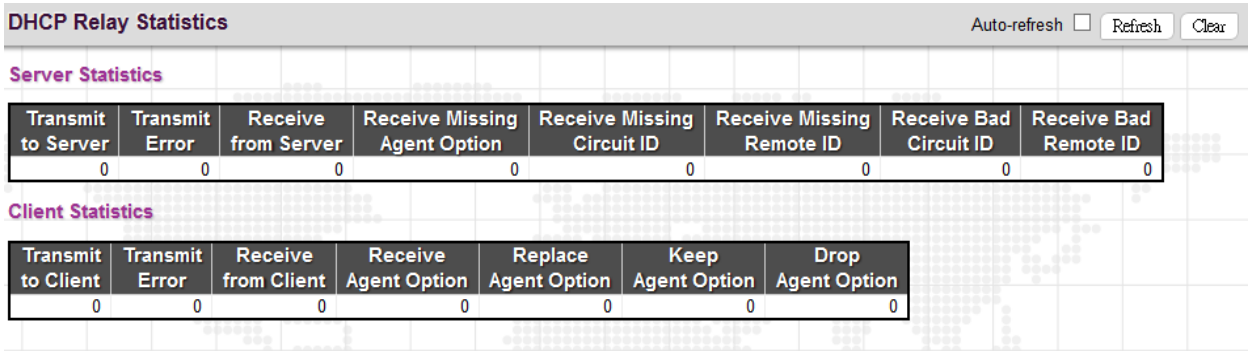
Relay Information Policy: Select Relay Information policy for DHCP client that includes option 82 information.

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.

4.5.5.4.4 Relay Statistics



DHCP Relay Statistics

Transmit to Server: The number of packets that are relayed from client to server.

Transmit Error: The number of packets that resulted in errors while being sent to clients.

Receive from Client: The number of packets received from server.

Receive Missing Agent Option: The number of packets received without agent information options.

Receive Missing Circuit ID: The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID: The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID: The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID: The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client: The number of relayed packets from server to client.

Transmit Error: The number of packets that resulted in error while being sent to servers.

Receive from Client: The number of received packets from server.

Receive Agent Option: The number of received packets with relay agent information option.

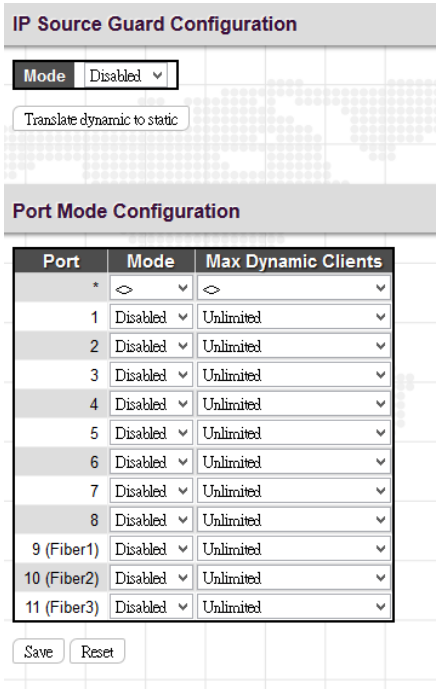
Replace Agent Option: The number of packets which were replaced with relay agent information option.

Keep Agent Option: The number of packets whose relay agent information was retained.

Drop Agent Option: The number of packets that were dropped which were received with relay agent information.

4.5.5.5 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.

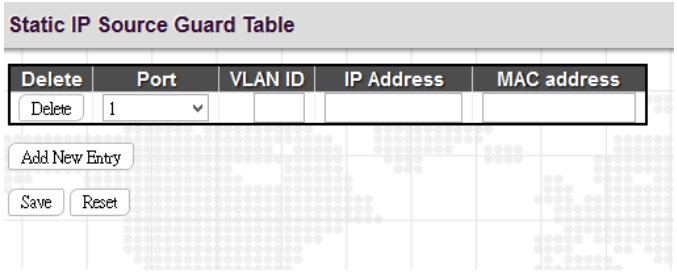
Port Mode Configuration

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.

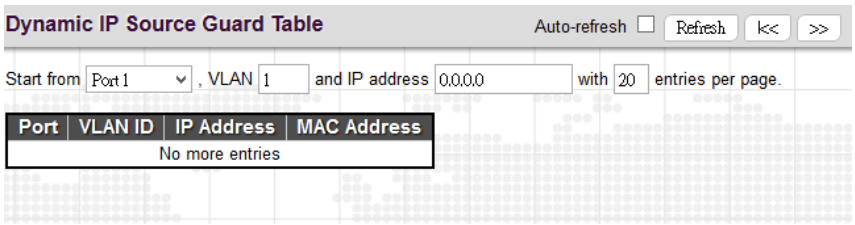
Select the “Delete” checkbox to remove the entry during the next save.

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

Click the “Reset” button to restore settings to default settings or previously configured settings.

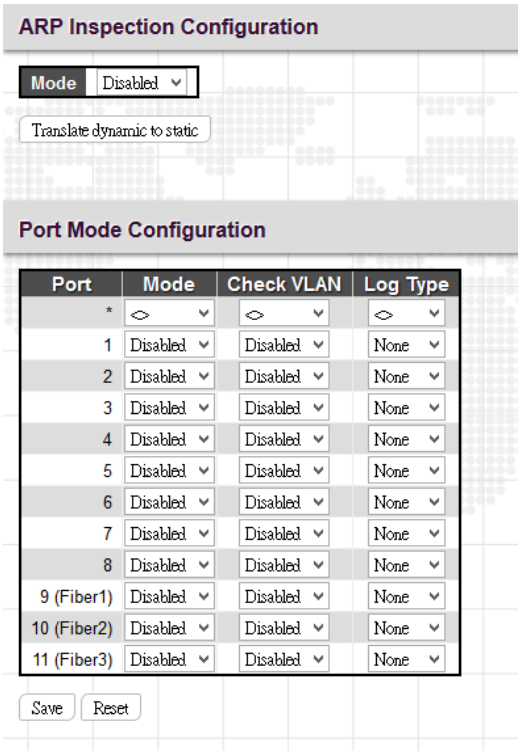
4.5.5.5.3 Dynamic Table

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



ARP Inspection Configuration

Mode: Enable or disable ARP inspection function globally.

Port Mode Configuration

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.

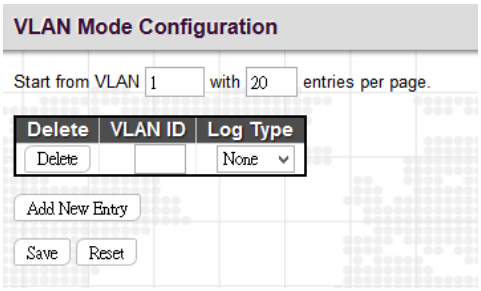
None: Log nothing.

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.

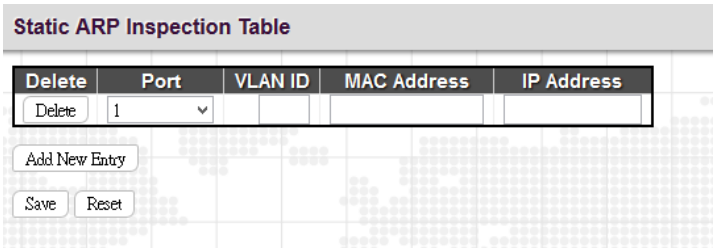
Click the “Add New Entry” button to insert an entry to the table.

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.

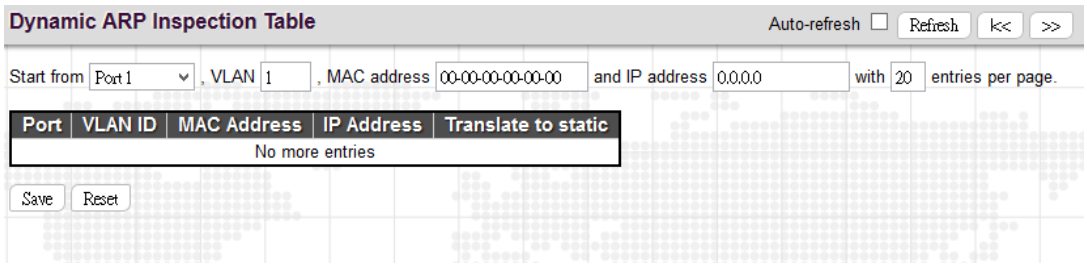
Click the “Add New Entry” button to insert an entry to the table.

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.

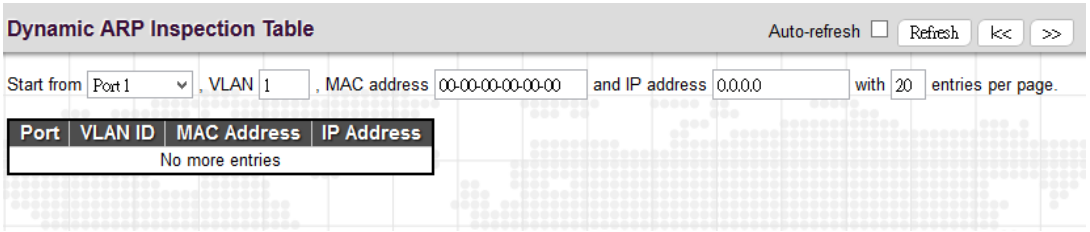
VLAN ID: VLAN ID in which the ARP traffic is permitted.

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



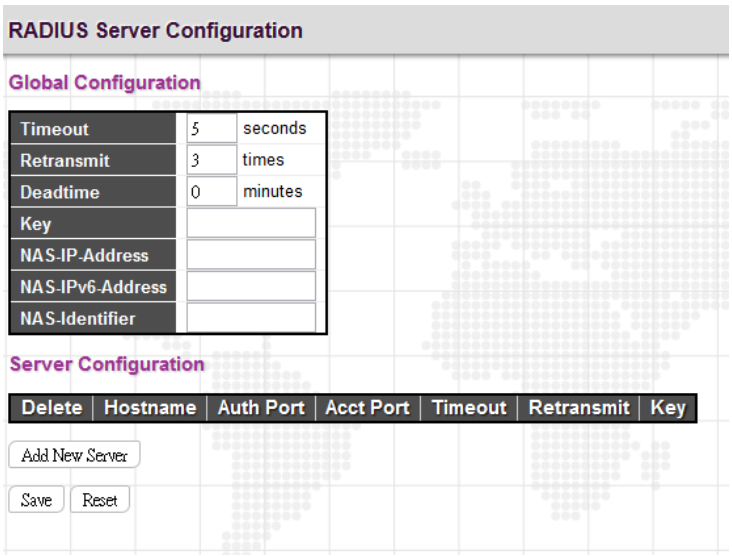
Port: The port number of this entry.

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



Global Configuration

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

Retransmit: Specify the number of times to retransmit request packets to an authentication server that does not respond. If the server does not respond after the last retransmit is sent, the switch considers the authentication server is dead.

Deadtime: Deadtime is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. The allowed deadtime range is between 0 to 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.

Sever Configuration

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

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

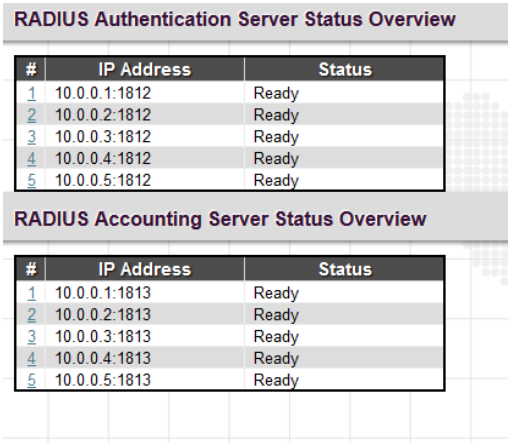
Acct Port: The UDP port to be used on the RADIUS server for accounting.

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

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

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

4.5.6.2 RADIUS Overview



#: 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.

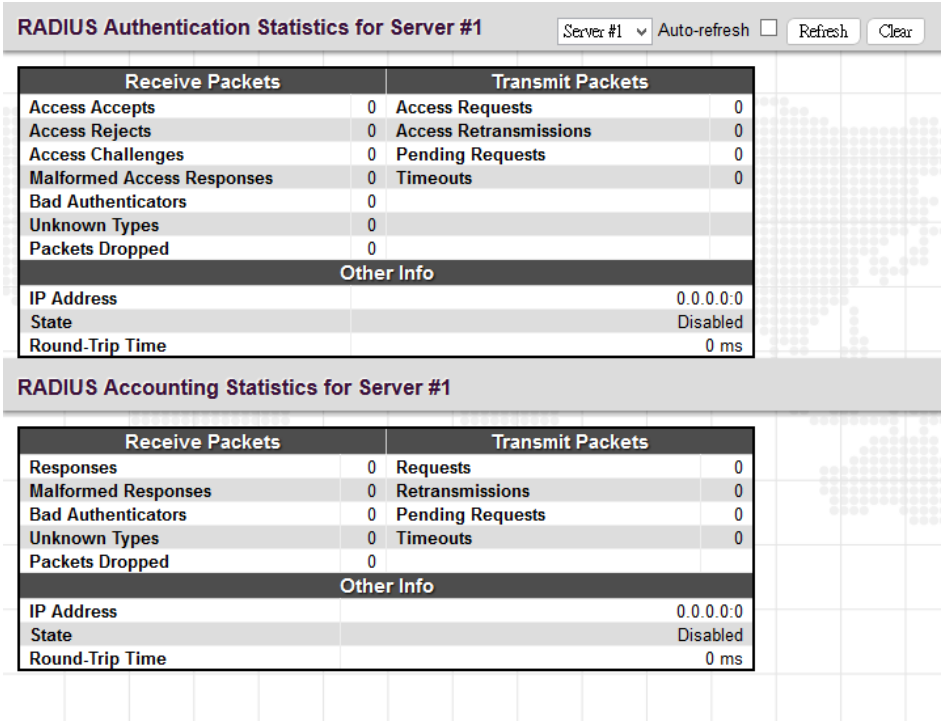
Status: The current state of RADIUS authentication server. Displayed states include the following:

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

Access Accepts: The number of RADIUS Access-Accept packets (valid or invalid) received from the server.

Access Rejects: The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

Access Challenges: The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

Malformed Access Responses: The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

Bad Authenticators: The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

Unknown Types: The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

Packets Dropped: The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

Access Requests: The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

Access Retransmissions: The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

Pending Requests: The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

Timeouts: The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

IP Address: IP address and UDP port for the authentication server in question.

State: Shows the state of the server. It takes one of the following values:

Disabled: The selected server is disabled.

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

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time: The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics for Server

Responses: The number of RADIUS packets (valid or invalid) received from the server.

Malformed Responses: The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.

Bad Authenticators: The number of RADIUS packets containing invalid authenticators received from the server.

Unknown Types: The number of RADIUS packets of unknown types that were received from the server on the accounting port.

Packets Dropped: The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

Requests: The number of RADIUS packets sent to the server. This does not include retransmissions.

Retransmissions: The number of RADIUS packets retransmitted to the RADIUS accounting server.

Pending Requests: The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.

Timeouts: The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

IP Address: IP address and UDP port for the accounting server in question.

State: Shows the state of the server. It takes one of the following values:

Disabled: The selected server is disabled.

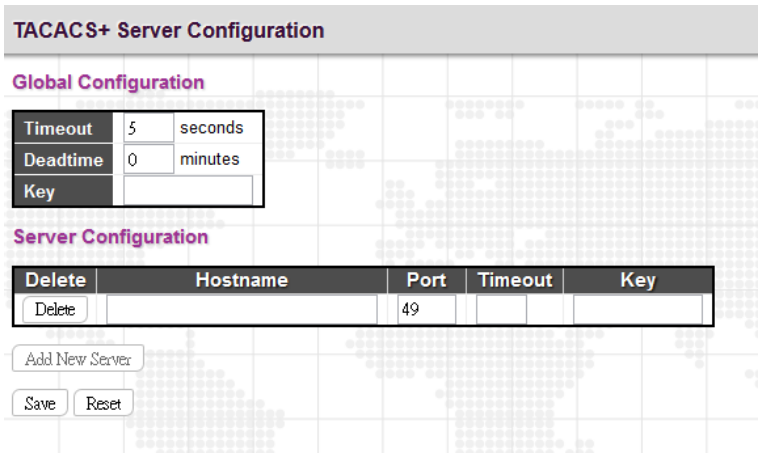
Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time: The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

4.5.6.4 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.

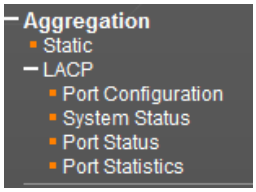
Timeout: If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

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.

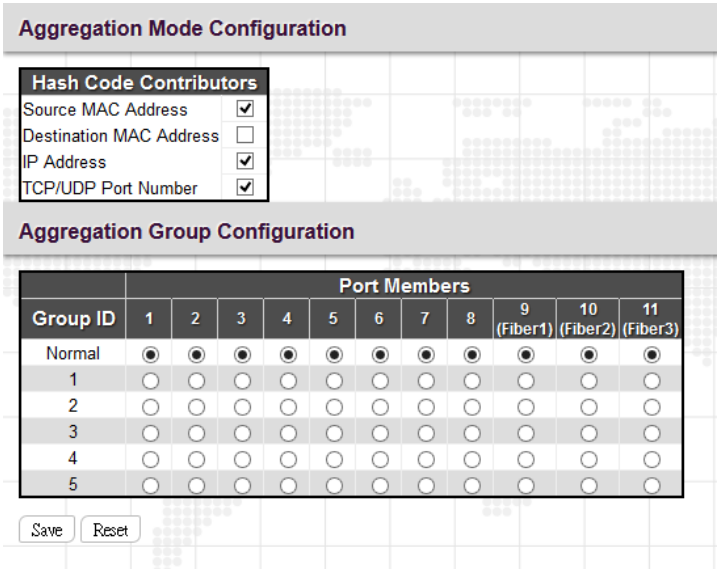
4.6 Aggregation

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



Aggregation Mode Configuration

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

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

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

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

Aggregation Group Configuration

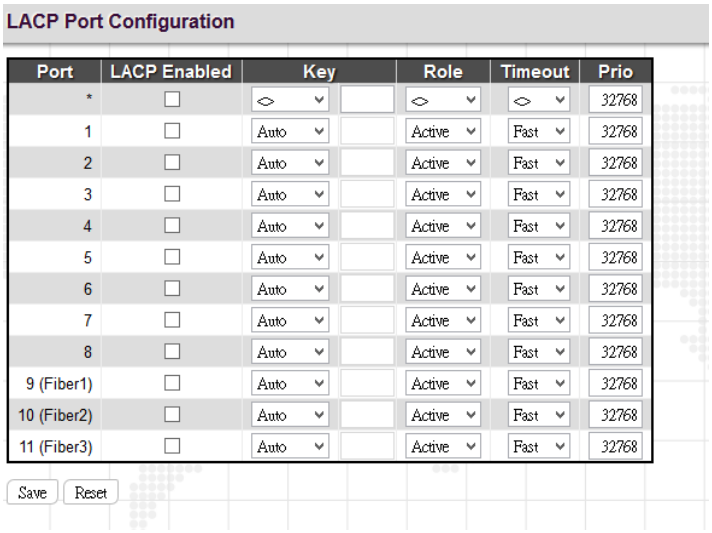
Group ID: Trunk ID number. “Normal” means that no aggregation is used. Five aggregation groups are available for use. Each group contains at least 2 to 10 links (ports). Please note that each port can only be used once in Group ID 1~5.

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



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.

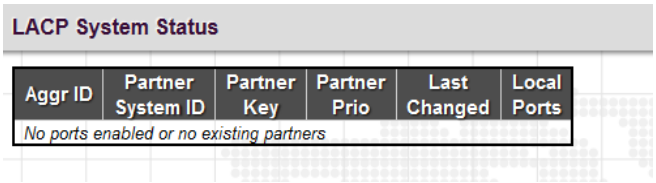
Ports that are designated as "Active" are able to process and send LACP control frames. Hence, this allows LACP compliant devices to negotiate the aggregated like so that the group may be changed dynamically as required. In order to add or remove ports from the group, at least one of the participating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

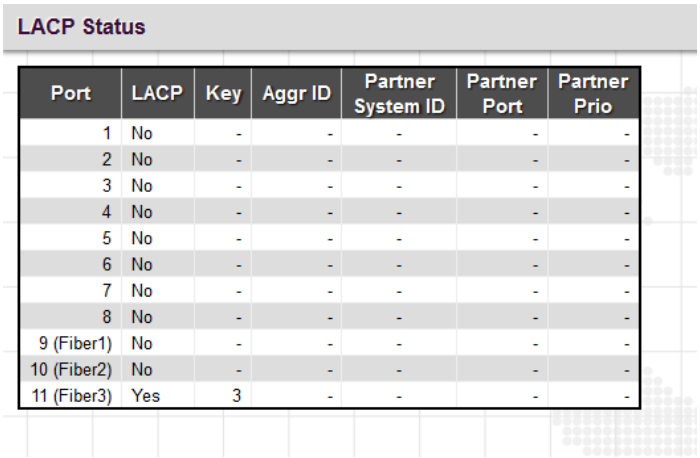
Partner Key: The partner key assigned to this LAG.

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.

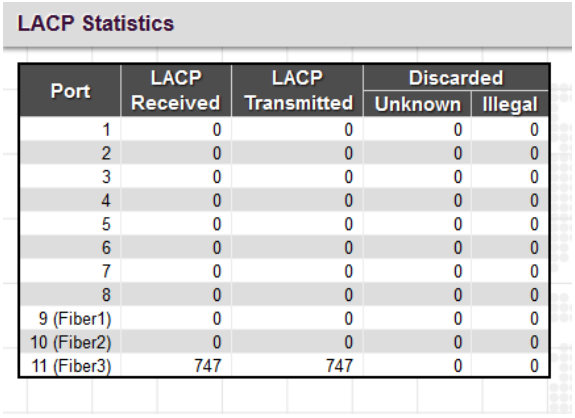
Aggr ID: Display the aggregation ID active on a port.

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.

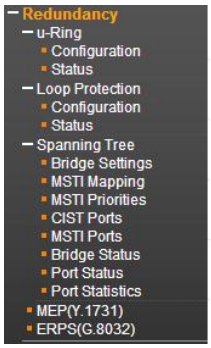
LACP Transmitted: The number of LACP packets transmitted by a port

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.



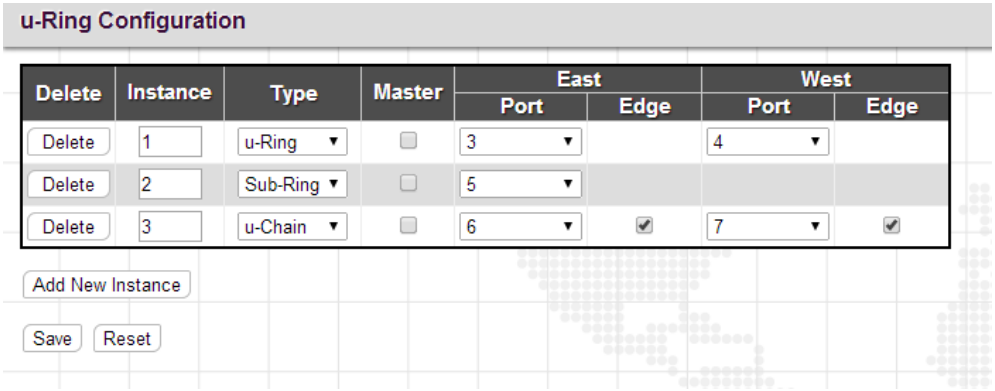
4.7.1 u-Ring

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



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

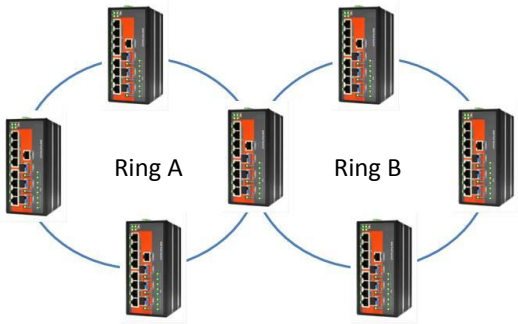


Figure 2. Two rings

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.

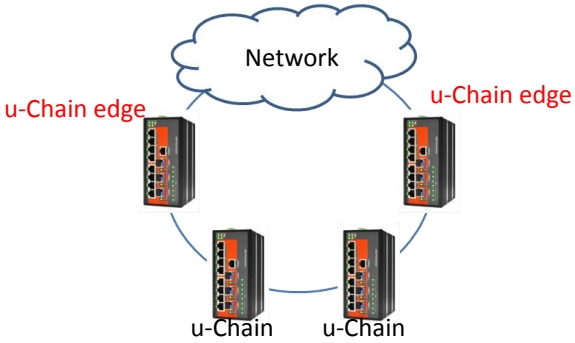


Figure 3. u-Chain ring connects to a network

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.

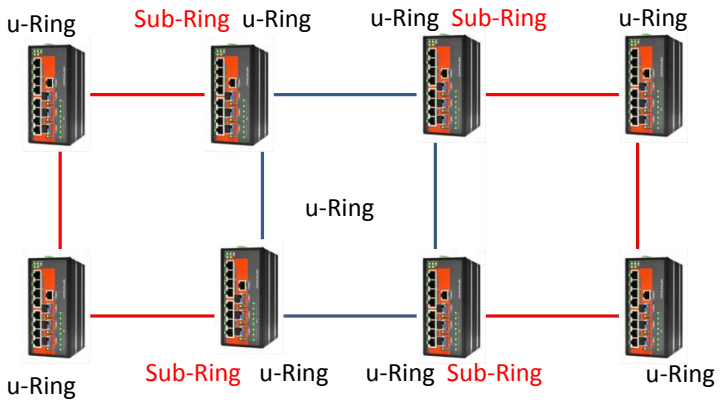


Figure 4. Sub-Ring

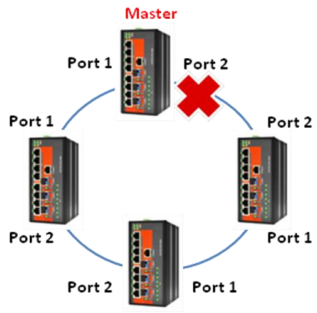
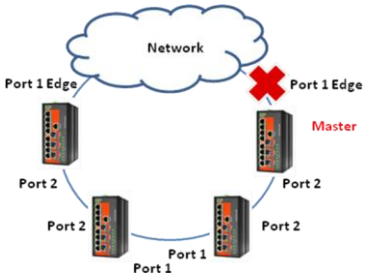
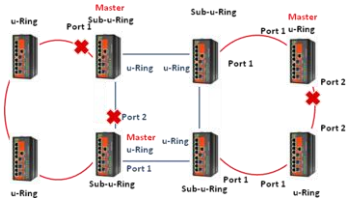
Master: The Master is generally used to decide which segment acts as a backup path. The user can manually select the checkbox to set the device in a ring as a Master. However, if all devices' Master checkboxes are left unchecked, the u-Ring protocol will assign one of the devices in the ring as the Master 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.

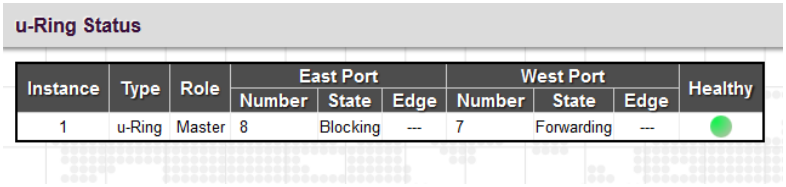
Edge: This field appears only when you select u-Chain type. Select the checkbox to set the selected port as a u-Chain edge port.

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. ● 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. ● 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. ●The device with a configured **edge port** that has the **biggest MAC address** is selected as the Master. ● 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. *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. ● 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. ● 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.

		● If the Master has two edge ports, the port with **higher port number** is blocked.	
Example			

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.

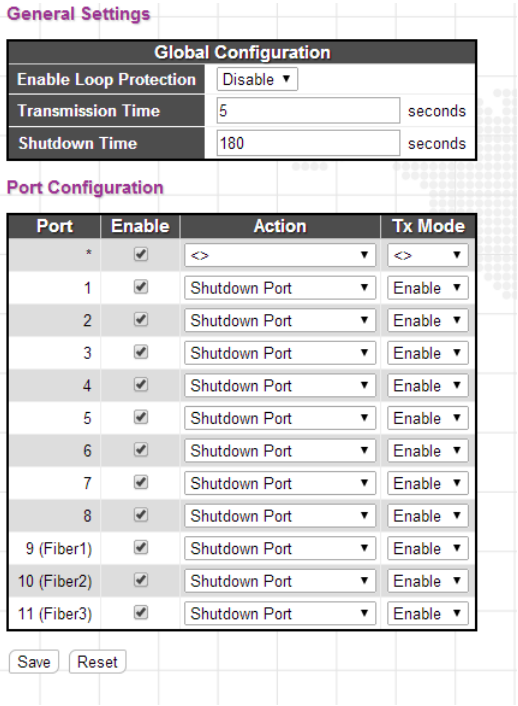
● **:** The Master is elected and backup path is blocked. The network with a redundant path works normally.

● **:** 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.

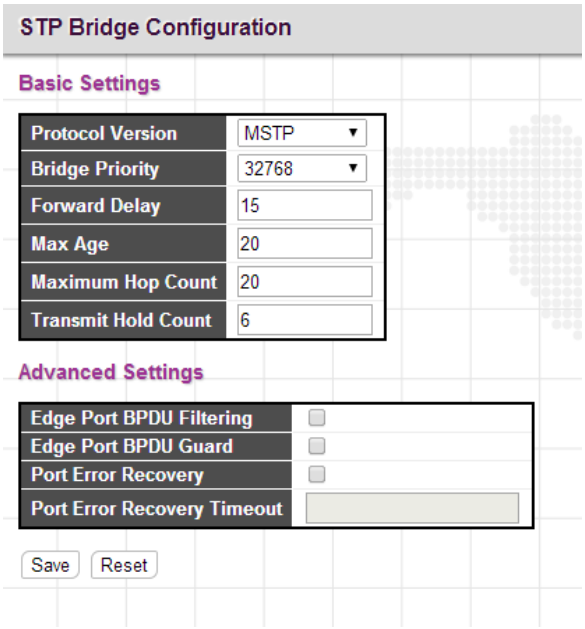
To solve problems causing by bridge loops, spanning tree allows a network design to include redundant links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manually enabling/disabling these backup links.

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.

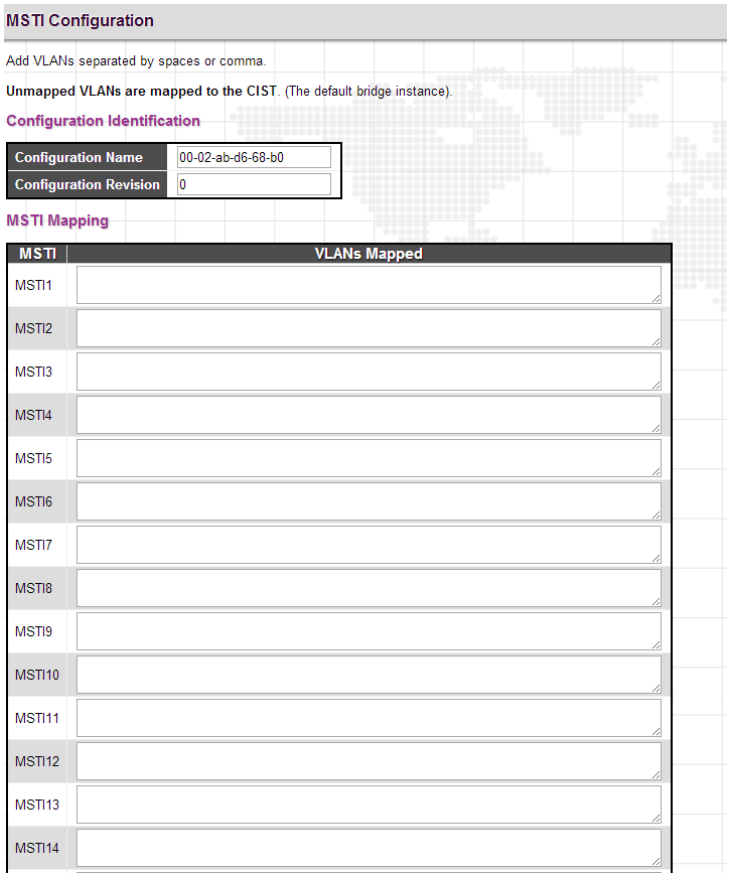
Edge Port BPDU Guard: Edge ports generally connect directly to PC, file servers or printers. Therefore, edge ports are configured to allow rapid transition. Under normal situations, edge ports should not receive configuration BPDUs. However, if they do, this probably is due to malicious attacks or mis-settings.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

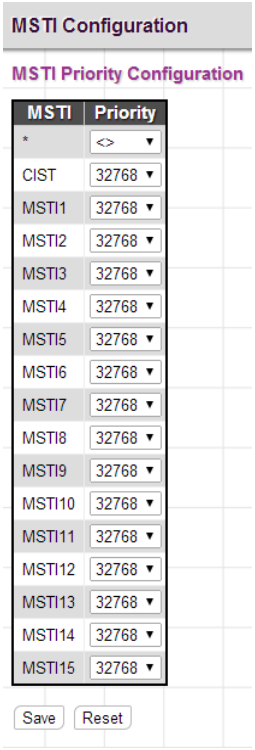
Configuration Revision: The revision number for this MSTI. The allowed range is 0~65535.

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.

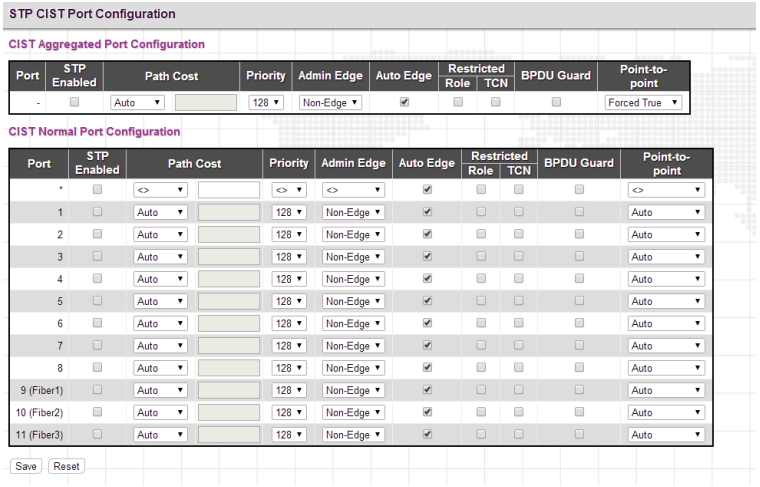
4.7.3.3 MSTI Priorities



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



CIST Aggregated Port Configuration

Port: The port number.

STP Enabled: Enable STP function

Path Cost: Path cost is used to determine the best path between devices. If "Auto" mode is selected, the system automatically detects the speed and duplex mode to decide the path cost. Select "Specific", if you want to use user-defined value. Valid values are 1 to 200000000. Please note that path cost takes precedence over port priority.

Priority: Select port priority.

Admin Edge: If an interface is attached to end nodes, you can set it to "Edge".

Auto Edge: Select the checkbox to enable this feature. When enabled, a port is automatically determined to be at the edge of the network when it receives no BPDUs.

Restricted Role: If enabled, this causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority.

Restricted TCN: If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports.

BPDU Guard: This feature protects ports from receiving BPDUs. It can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state. If enabled, the port will disable itself upon receiving valid BPDU's.

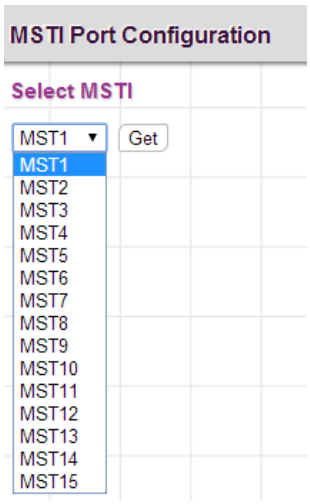
Point-to-Point: Select the link type attached to an interface.

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

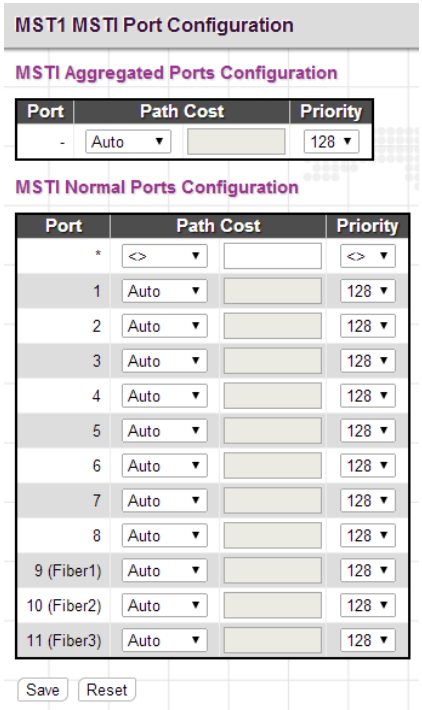
Forced True: It is a point-to-point connection.

Forced False: It is a shared medium connection.

4.7.3.5 MSTI Ports



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

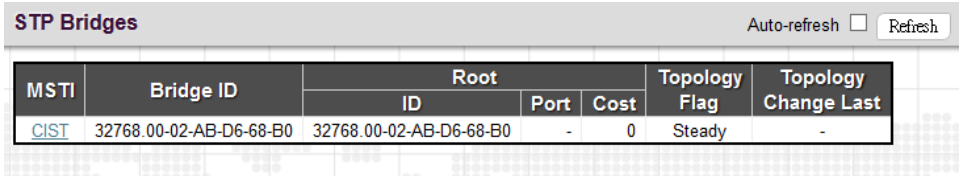


Port: The port number.

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.

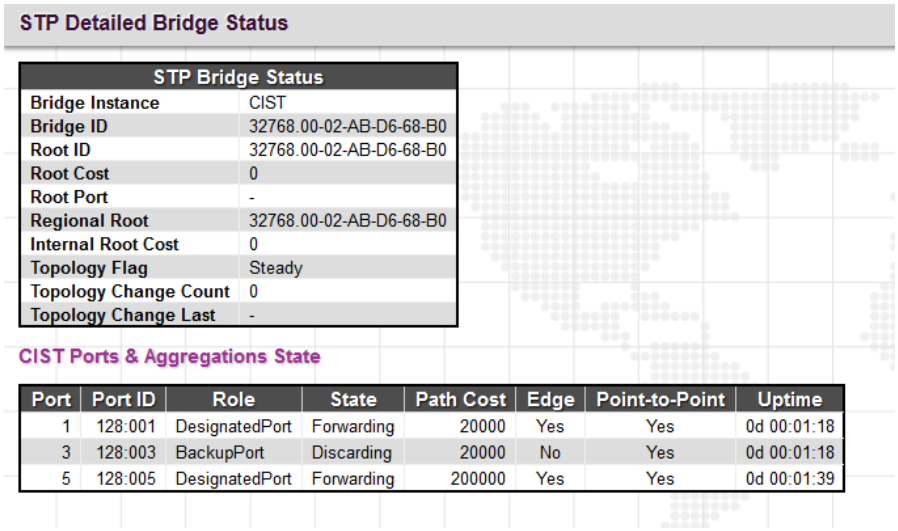
Root Port: The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

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

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

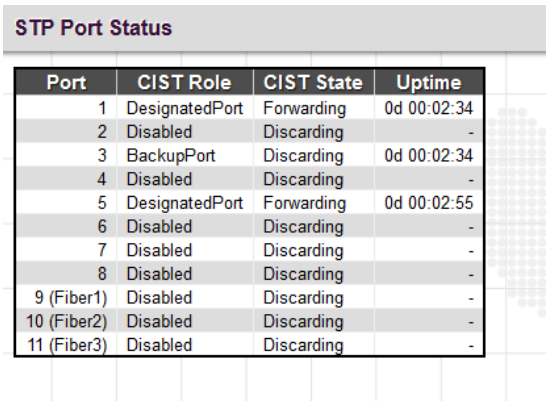
Forwarding: Ports forward packets and continue to learn addresses.

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



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:

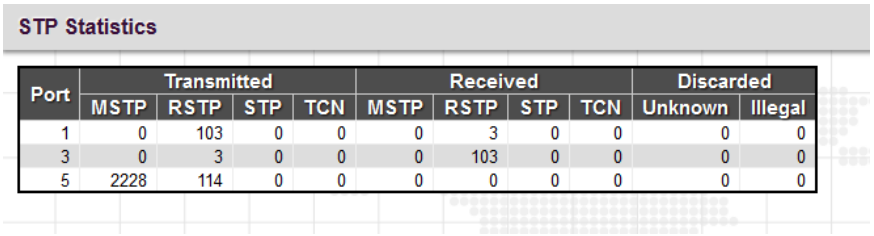
Discarding: Ports only receive BPDU messages but do not forward them.

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



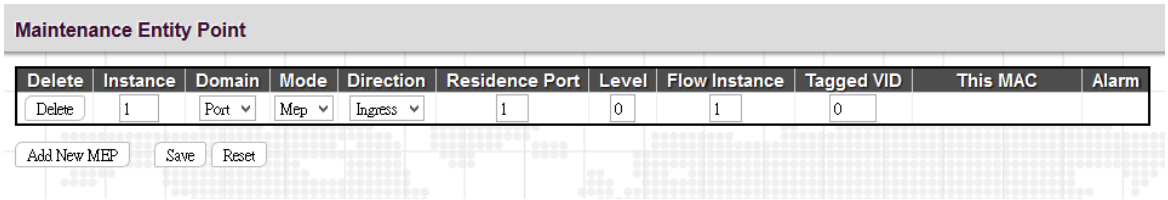
Port: Display the port number.

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. (Currently, Port is available for use.)

Esp: Future use

MEP: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC. The EVC must be created.

Mpls: Future use

Mode: Select either Mep (Maintenance Entity End Point) or Mip (Maintenance Entity Intermediate Point).

Direction: Select the traffic direction either Ingress or Egress for monitoring on a residence port.

Residence Port: Specify a port to monitor.

Level: The MGP level of this MEP.

Flow Instance: The MEP related to this flow.

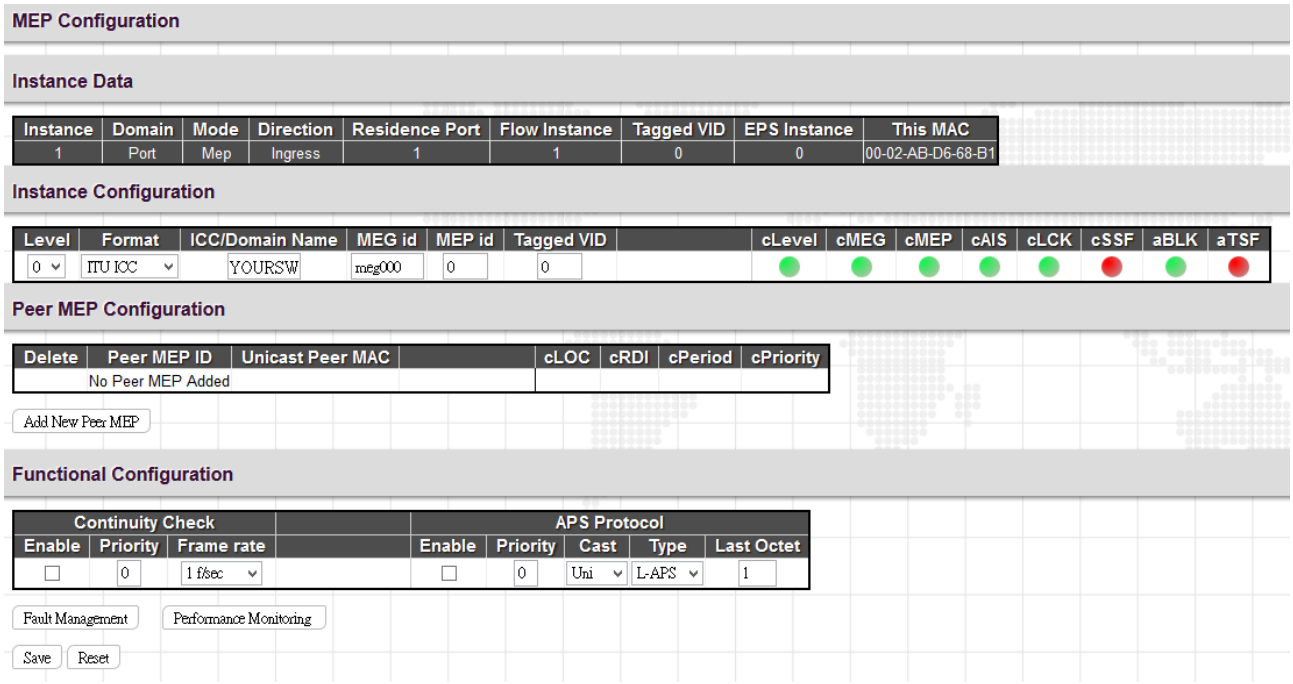
Tagged VID: A C-tag or S-tag (depending on VLAN port type) is added with this VID. Entering "0" means no tag will be added.

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. The maximum characters allowed for ICC format is 6. MEG id can allow 7 characters in maximum.
>
> **IEEE String:** This is defined by IEEE in 802.1ag. The Domain name and short name can be input is 8 characters long. MEG id can be 8 characters long as well.

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 a 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.

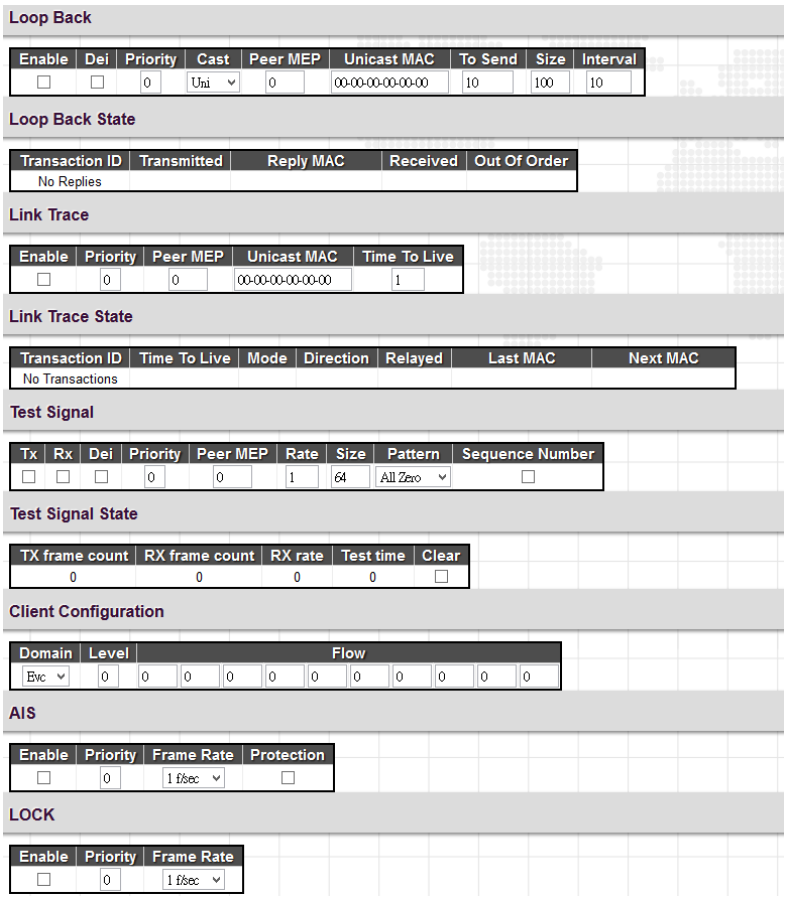
Type:

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.

Click the "Fault Management" button.



Loop Back

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.

Test Signal

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.

Test Signal State

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.

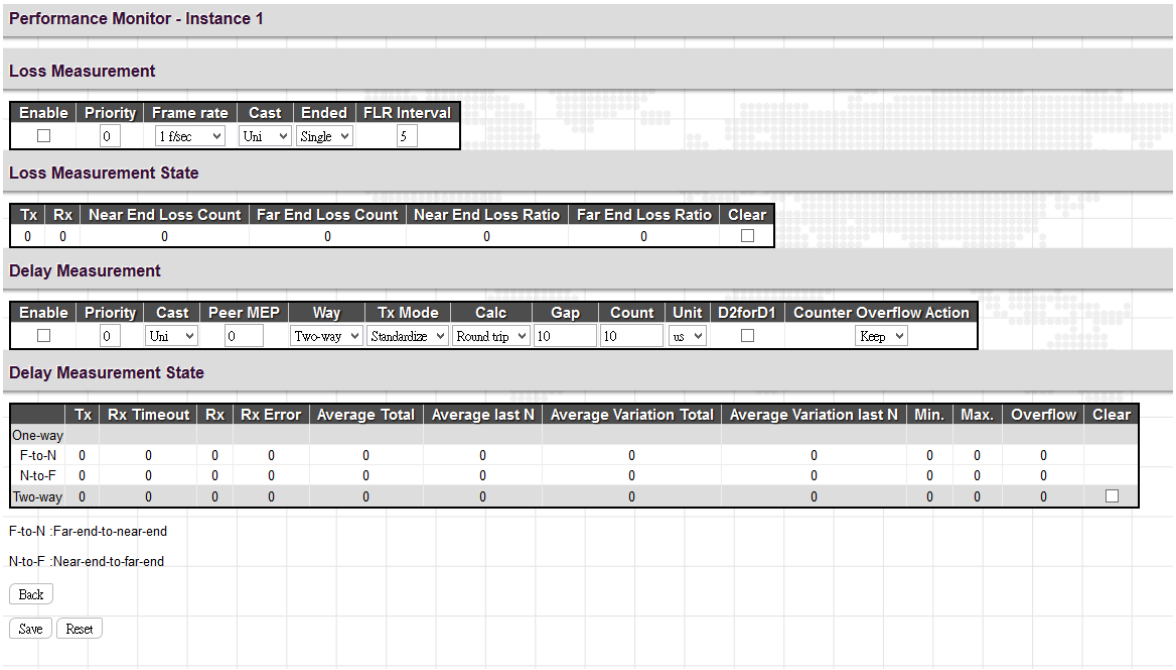
Lock

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.



Loss Measurement/Loss Measurement State

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 Ration: 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.

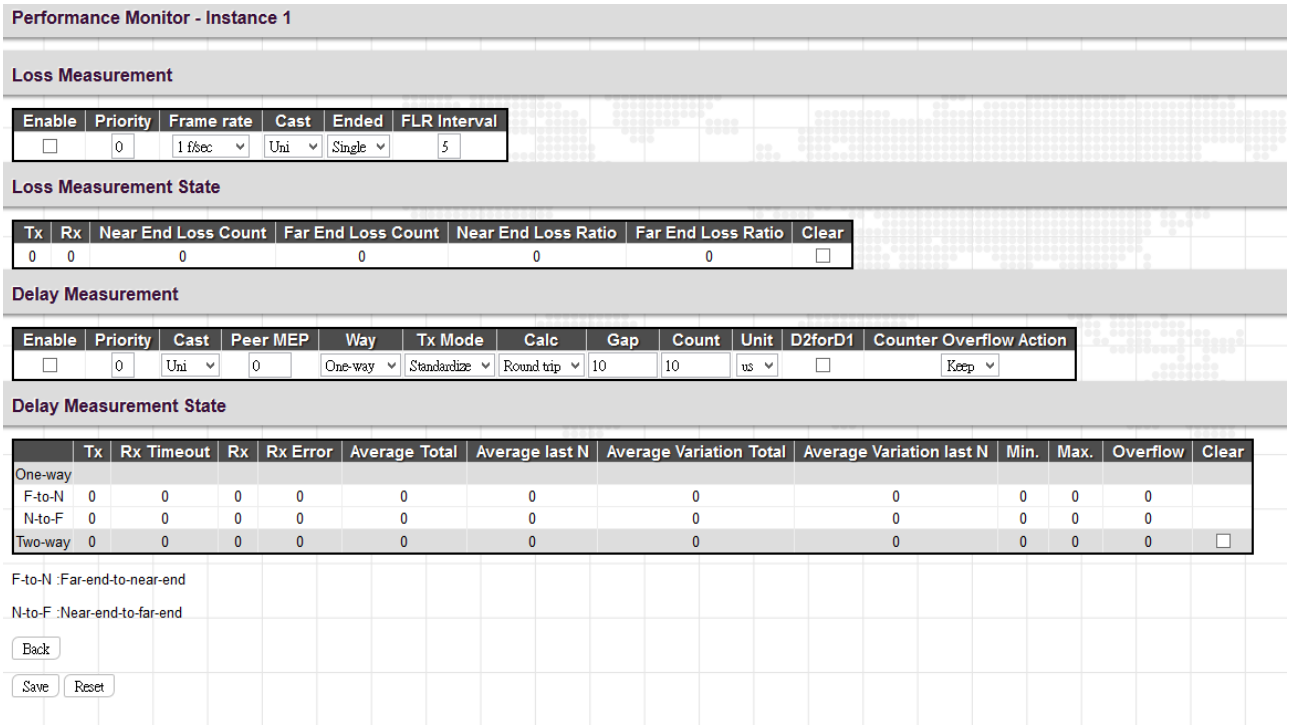
Count: The number of last records to calculate. The range is 10 to 2000.

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



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

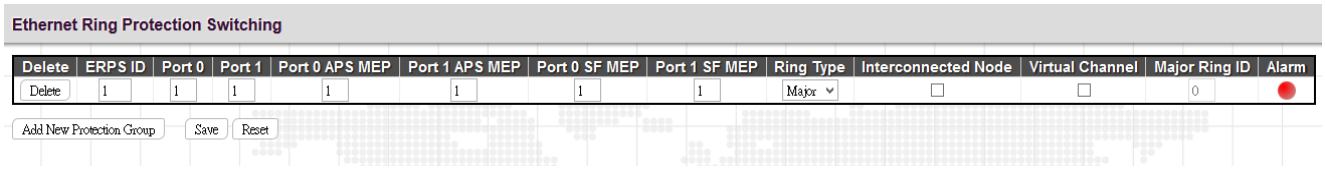
Ethernet Ring Protection Switching (ERPS), defined in ITU-T G8032, implements protection switching mechanism for Ethernet traffic in a ring topology. By performing ERPS function, potential loops in a network can be avoided by blocking traffic to flow to ring protection link (RPL) so as to protect the 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.

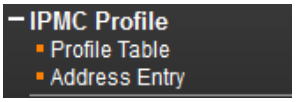
Click “Save” to save changes.

Click “Reset” to undo any changes made locally and restore changes to previously saved (default) values.

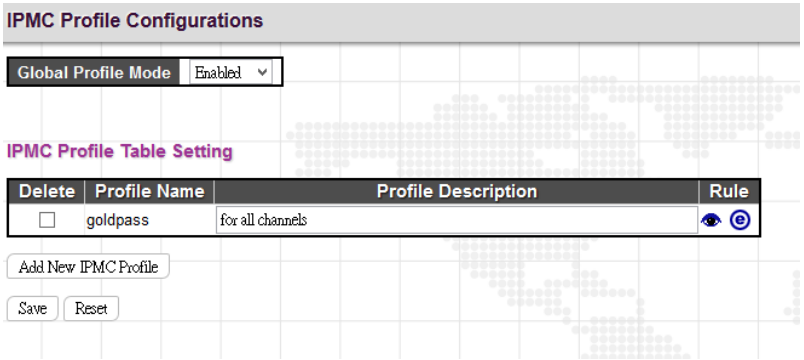
Click “Refresh” to manually refresh ERPS information.

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

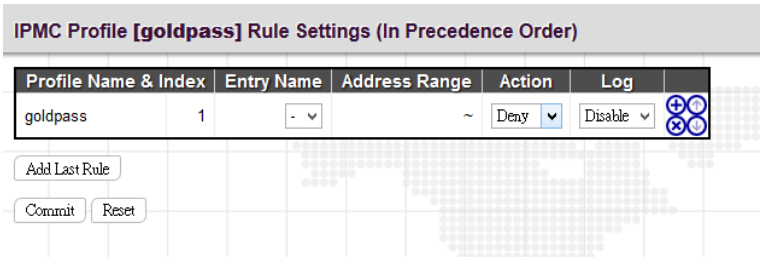
Profile Name: Enter a name for this profile.

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.

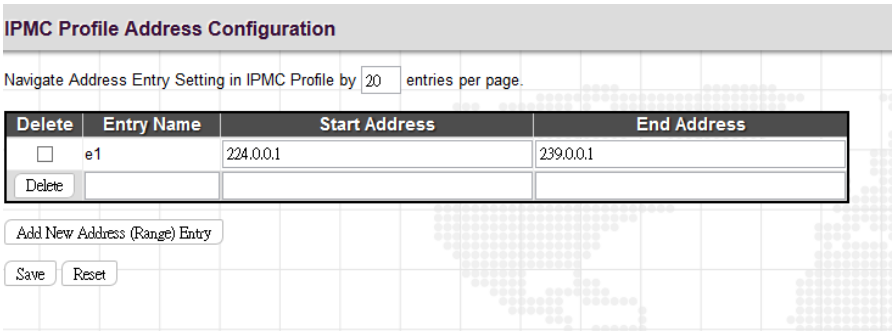
Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged.

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.

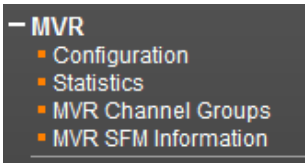
Select the "Delete" checkbox to delete an entry during the next save.

4.9 MVR

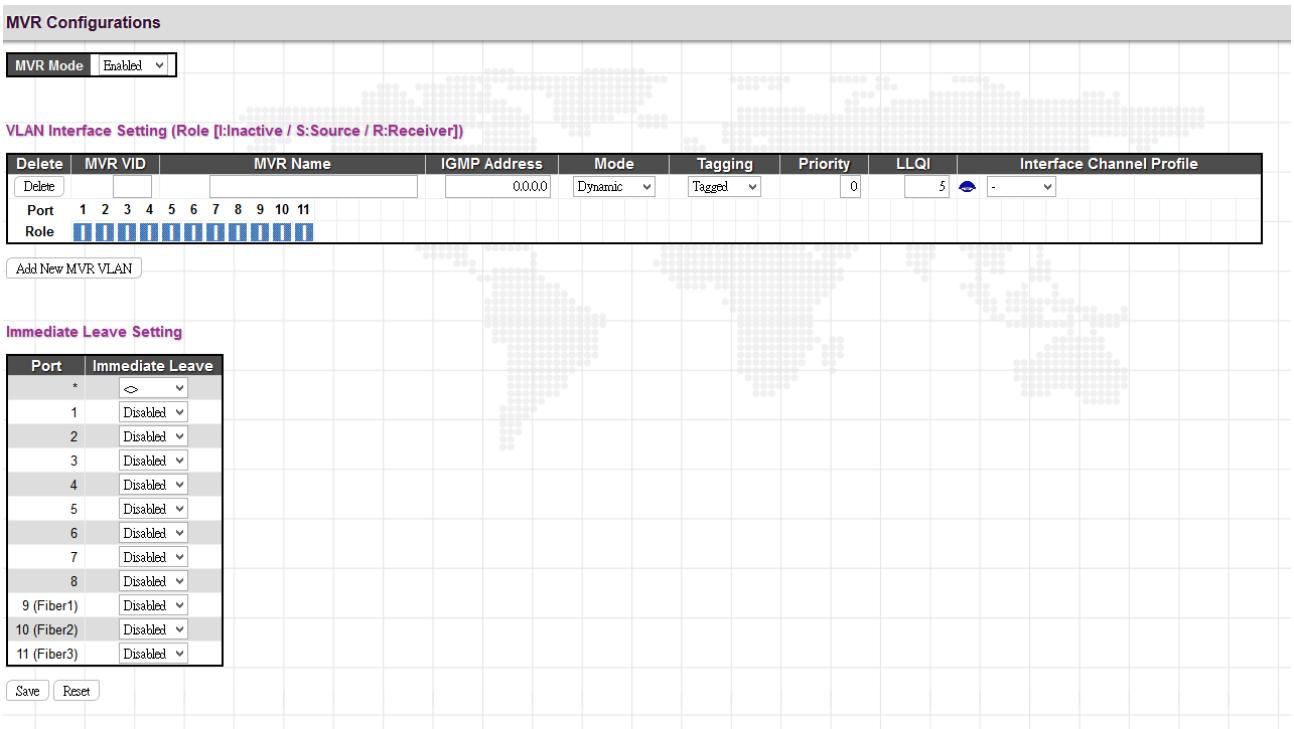
Multicast VLAN Registration protocol (MVR) allows a media server to transmit multicast stream in a single multicast VLAN when clients receiving multicast VLAN stream can reside in different VLANs. Clients in different VLANs intend to join or leave the multicast group simply by sending the IGMP Join or 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



MVR Configurations

MVR Mode: Enable or disable MVR feature globally on this device. Any multicast data from source ports will be sent to associated receiver ports registered in the table. By default, MVR feature is turned off.

VLAN Interface Setting

MVR ID: Specify multicast VLAN ID. Please note that MVR source ports are not recommended to be used as management VLAN ports. MVR source ports should be configured as members of the MVR VLAN, but MVR receiver ports should not be manually configured as members of this VLAN.

MVR Name: Optionally specify a user-defined name for this multicast VLAN. The maximum length of the MVR name string is 32. Both alphabets and numbers are allowed for use.

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.

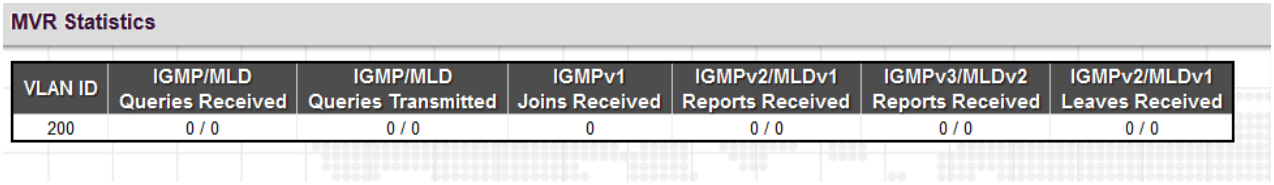
Receiver (R): Set a port to receiver port. Client or subscriber ports are configured to receiver ports so that they can issue IGMP/MLD messages to receive multicast data.

Immediate Leave Setting

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.

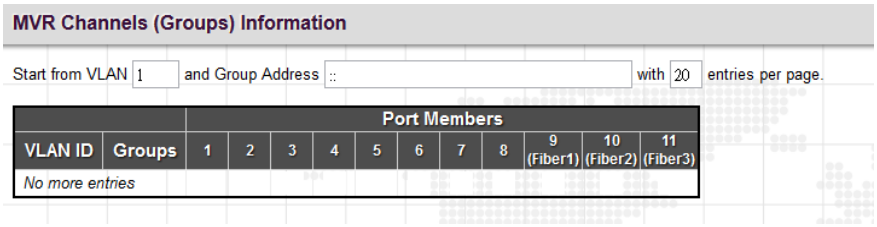
IGMPv1 Joins Received: The number of IGMPv1 received joins

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.

		Port Members										
VLAN ID	Groups	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.

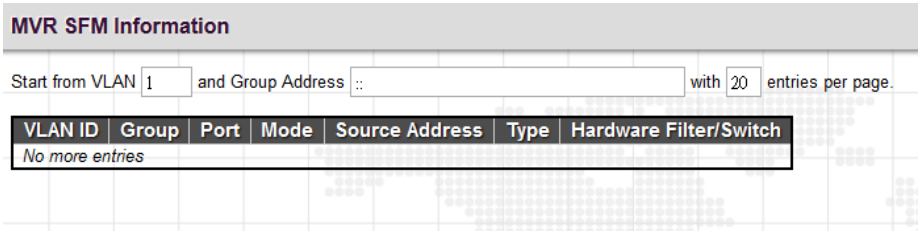
This table displays MVR channels (groups) information and is sorted by VLAN ID.

VLAN ID: VLAN ID of the group.

Groups: Group ID

Port Members: Ports that belong to this group.

4.9.4 MVR SFM Information



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.

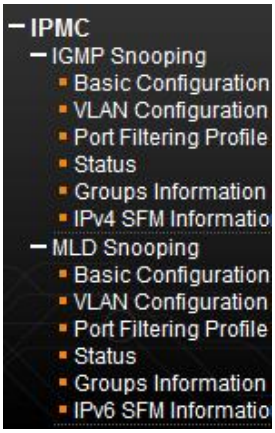
Source Address: The source IP Address. Currently, the system limits the total number of source IP addresses for filtering to be 128. When there is no source filtering address, "None" is shown in the Source Address field.

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

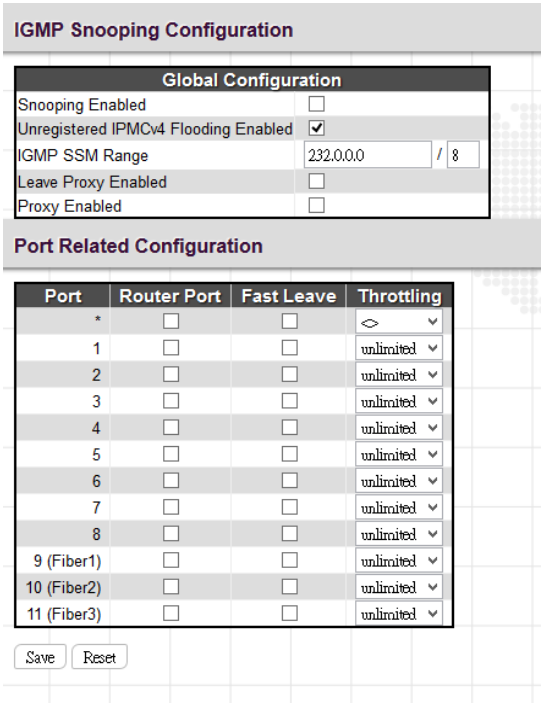
The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It can be used more efficiently when supporting activities, 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

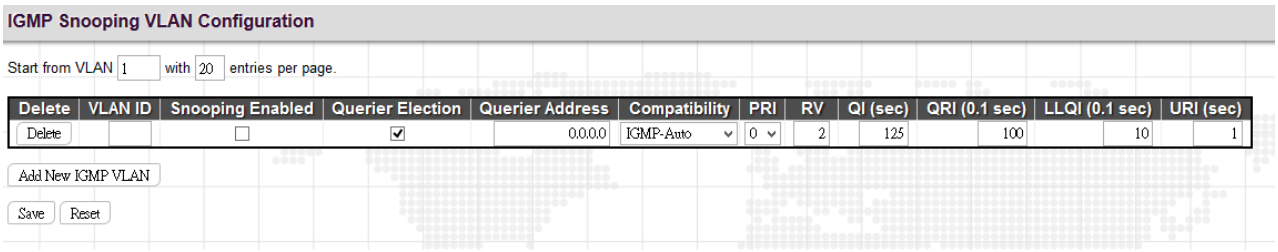
Port: The port number.

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.

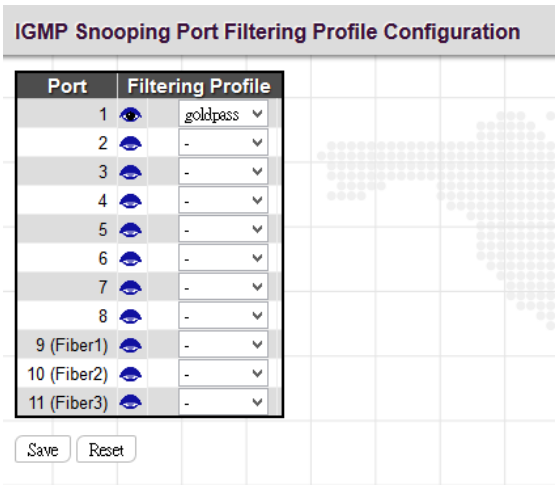
QRI: The Query Response Interval is the maximum amount of time that the IGMP router waits to receive a response to a General Query message. The QRI applies when the switch is acting as the querier and is used to inform other devices of the maximum time this system waits for a response to general queries. 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.

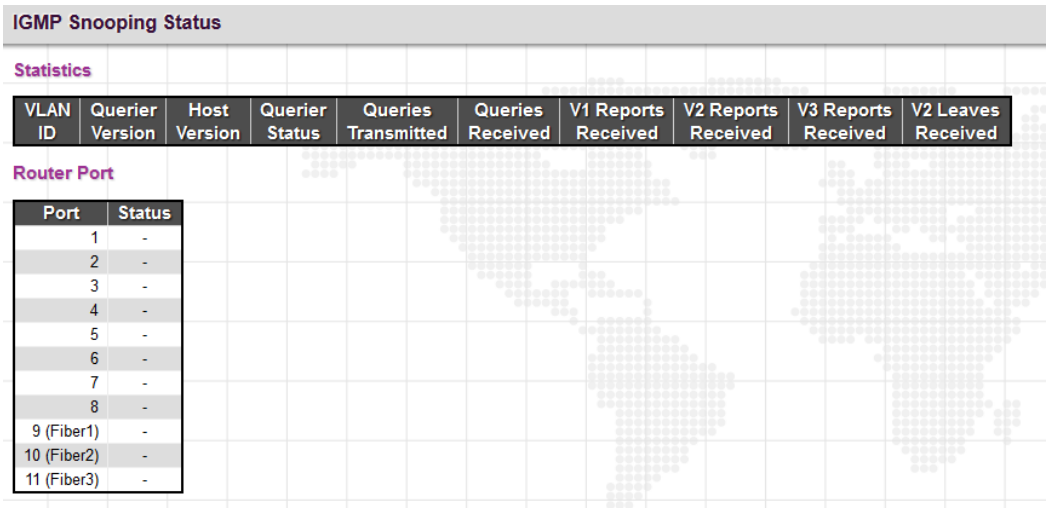


Port: The port number.

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.

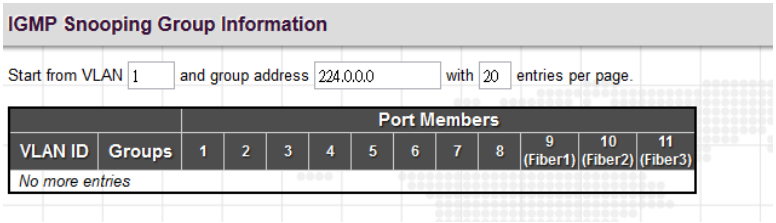
V2 Leaves Received: The number of Received V2 Leaves.

Router Port

Port: The port number.

Status: Indicate whether a specific port is a router port or not.

4.10.1.5 Groups Information



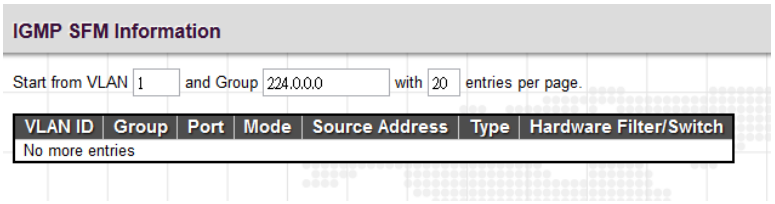
VLAN ID: Display the VLAN ID of the group.

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.

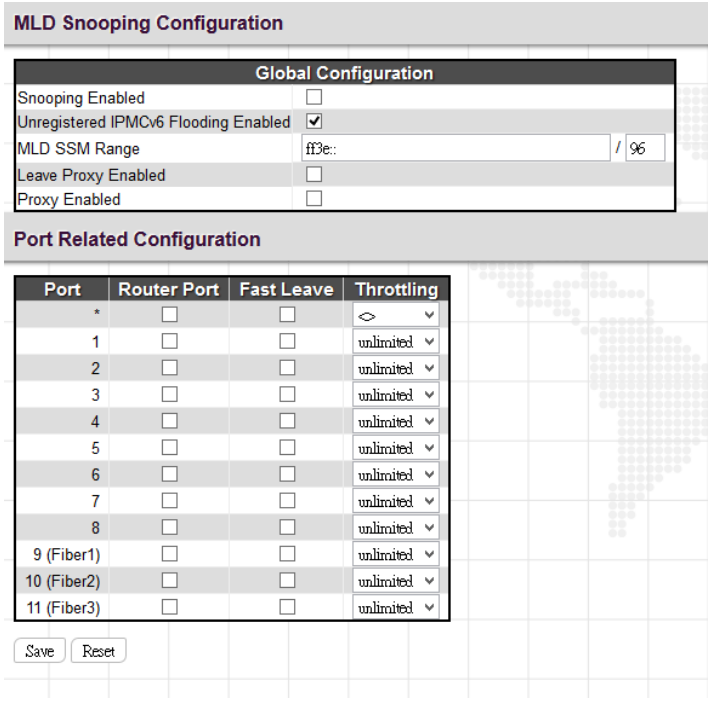
Type: Display either Allow or Deny type.

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



Global Configuration

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

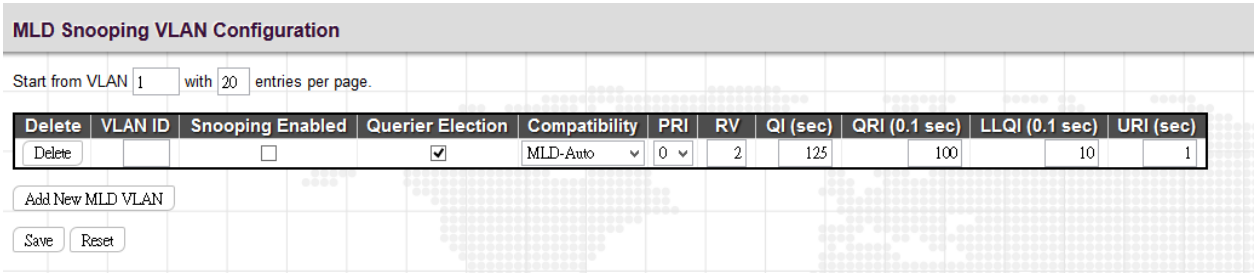
Port: The port number.

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.

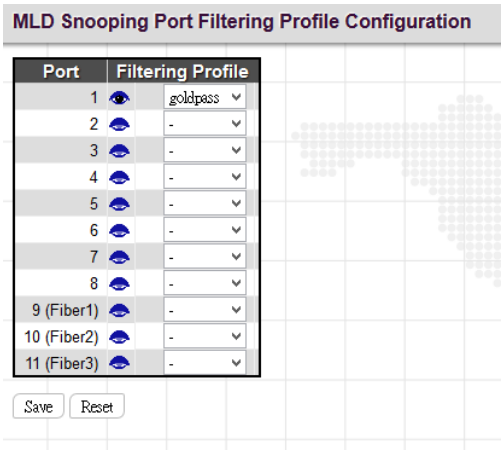
LLQI: The Last Listener Query Interval sets the interval that waits for a response to a group-specific or group-and-source specific query message.

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.

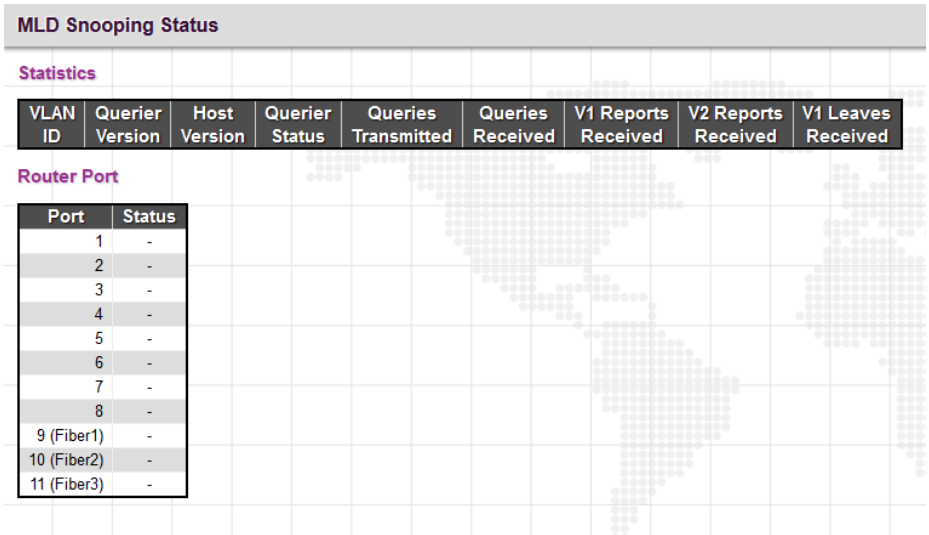


Port: List the number of each port.

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



Statistics

VLAN ID: The VLAN ID of this entry.

Querier Version: The current working Querier version.

Host Version: The current host version.

Querier Status: Show the Querier status that is either "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted: The number of queries transmitted.

Queries Received: The number of queries received.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

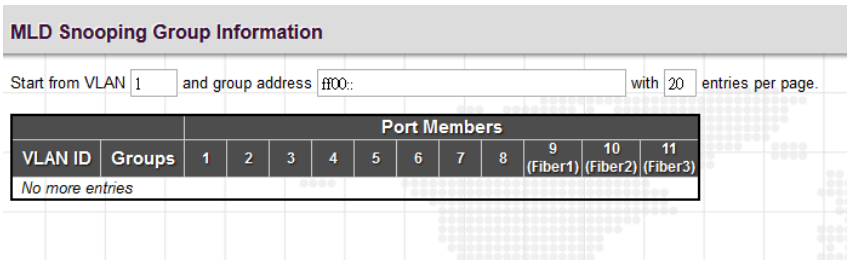
V2 Leaves Received: The number of Received V2 Leaves.

Router Port

Port: The port number.

Status: Indicate whether a specific port is a router port or not.

4.10.2.5 Groups Information



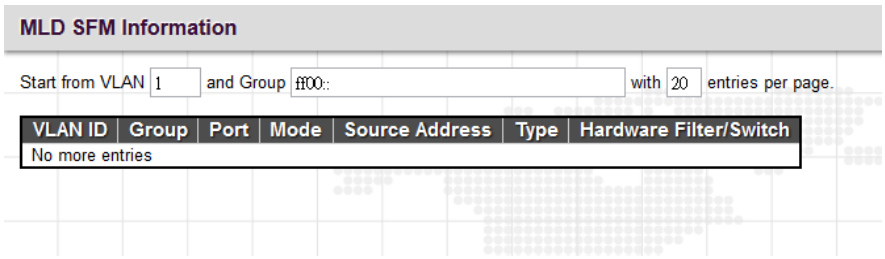
VLAN ID: Display the VLAN ID of the group.

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.

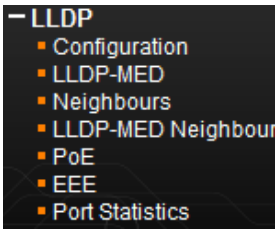
Type: Display either Allow or Deny type.

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.

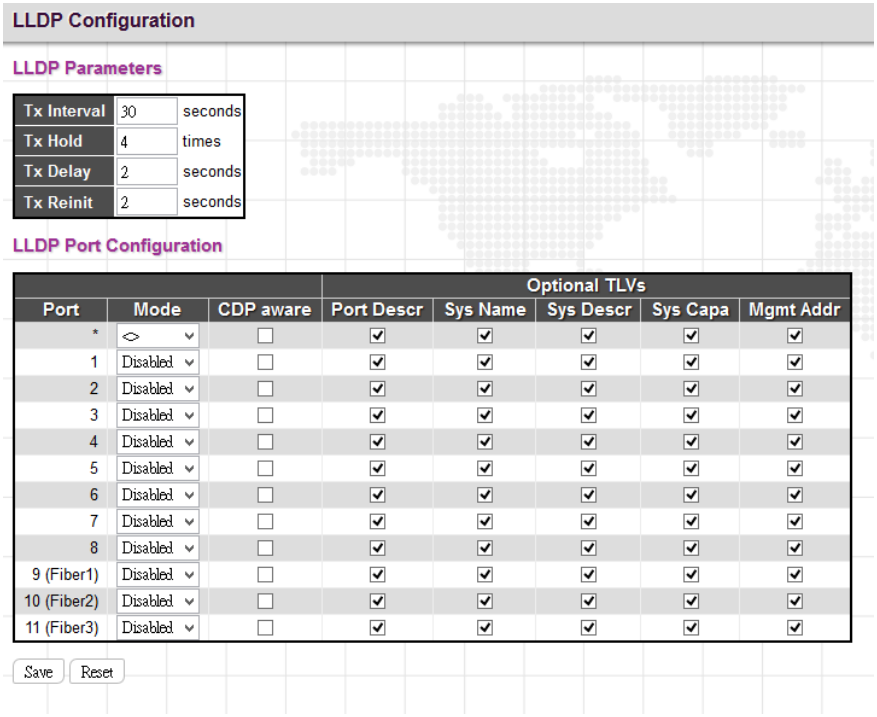
4.11 LLDP

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 Parameters

Tx Interval: Specify the interval between LLDP frames are sent to its neighbours for updated discovery information. The valid values are 5 - 32768 seconds. The default is 30 seconds.

Tx Hold: This setting defines how long LLDP frames are considered valid and is used to compute the TTL. Valid range is 2~10 times. The default is 4.

Tx Delay: Specify a delay between the LLDP frames that contain changed configurations. Tx Delay cannot be larger than 1/4 of the Tx interval value. The valid values are 1 - 8192 seconds.

Tx Reinit: Specify a delay between the shutdown frame and a new LLDP initialization. The valid values are 1~10 seconds.

LLDP Port Configuration

Port: The port number. "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.

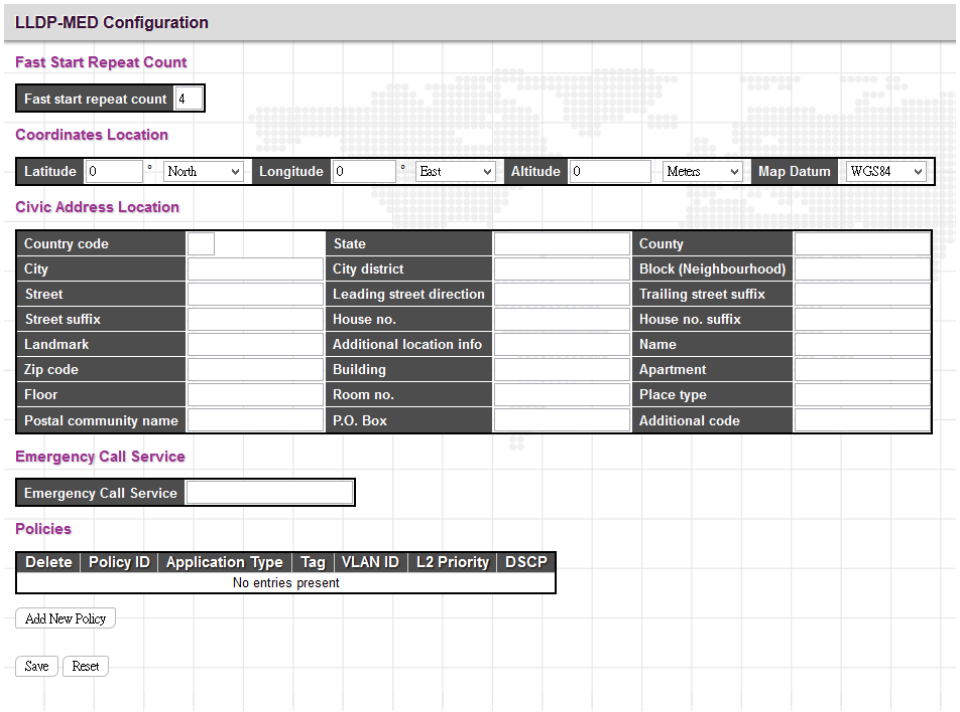
Tx Only: The switch will send out LLDP information but will drop LLDP information received from neighbours.

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”.

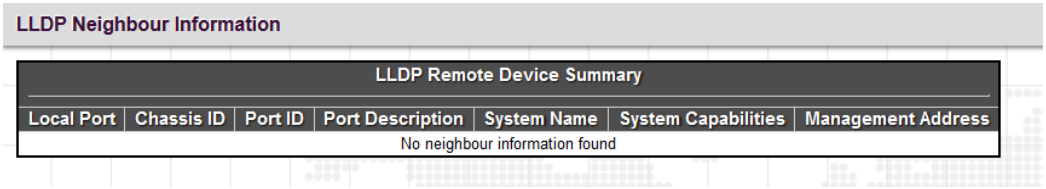
Tag: Tag indicating whether the specified application type is using a “tagged” or an “untagged” VLAN.

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.

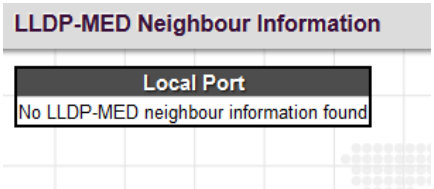
Port Description: A remote port's description.

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 (-).

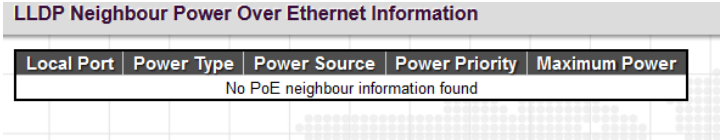
Management Address: The IPv4 address of the remote device. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. If the neighbor device allows management access, clicking on an entry in this field will re-direct the web browser 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.

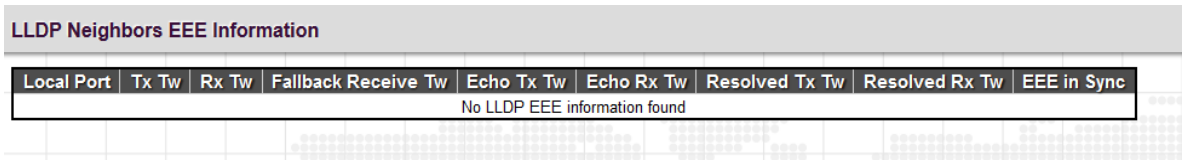
Power Type: This displays whether the device is Power Sourcing Entity (PSE) or Powered Device (PD). If the power type is unknown, it shows "Reserved".

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



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.

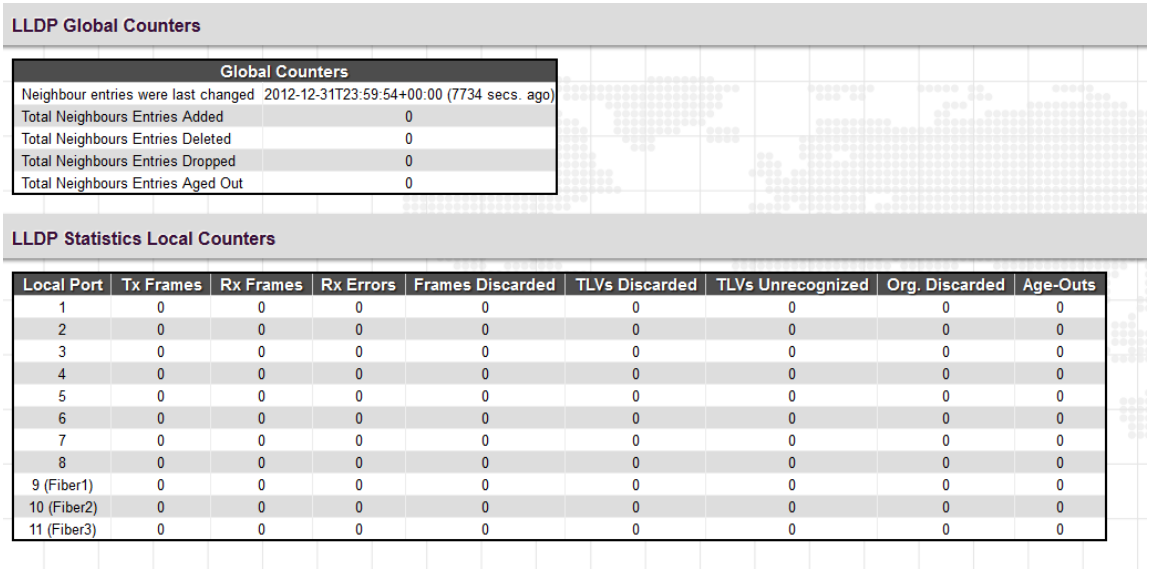
Resolved Rx Tw: The resolved Rx Tw for this link.

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.

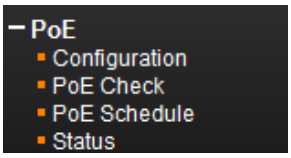
Org. Discarded: The number of organizational TLVs discarded.

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.

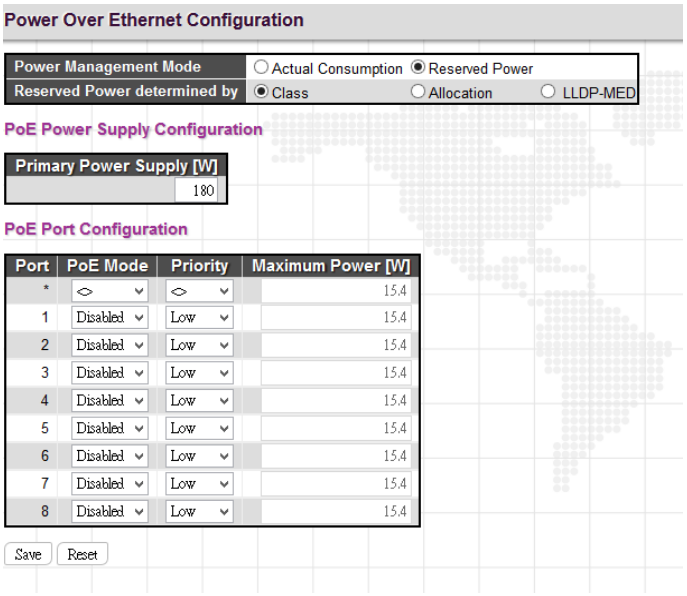
4.12 PoE (for PoE models only)

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



Power Over Ethernet Configuration

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.

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 34.2 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.*

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.

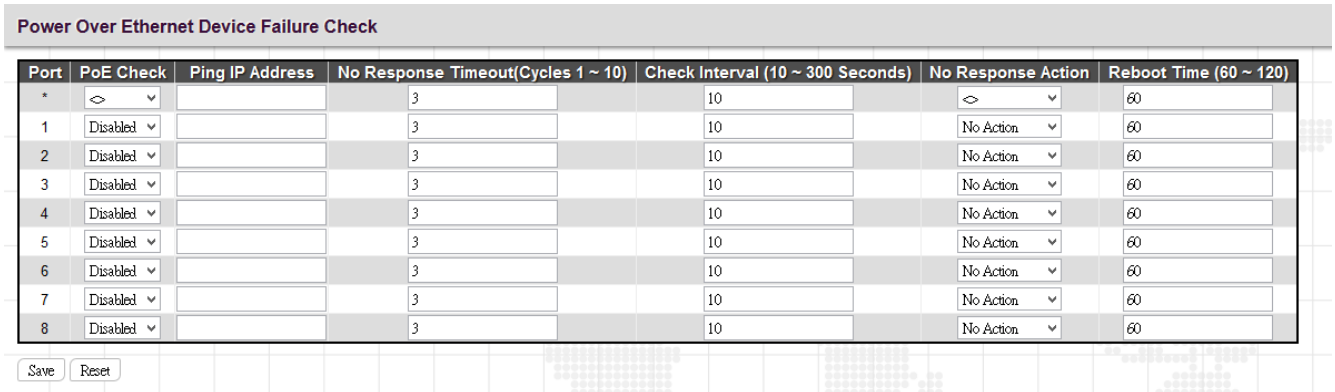
PoE: Enable IEEE 802.3af (Class 4 PDs limited to 15.4W).

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)



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.

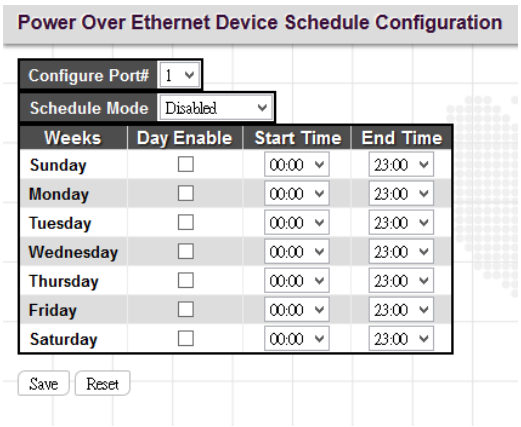
No Response Action: If PDs fails to respond ping requests sent by the switch (PSE), then the switch (PSE) can take an appropriate action selected here.

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.

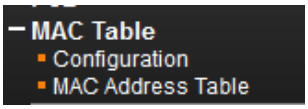
Current Used: How much current the PD is currently using.

Priority: The port's configured priority level.

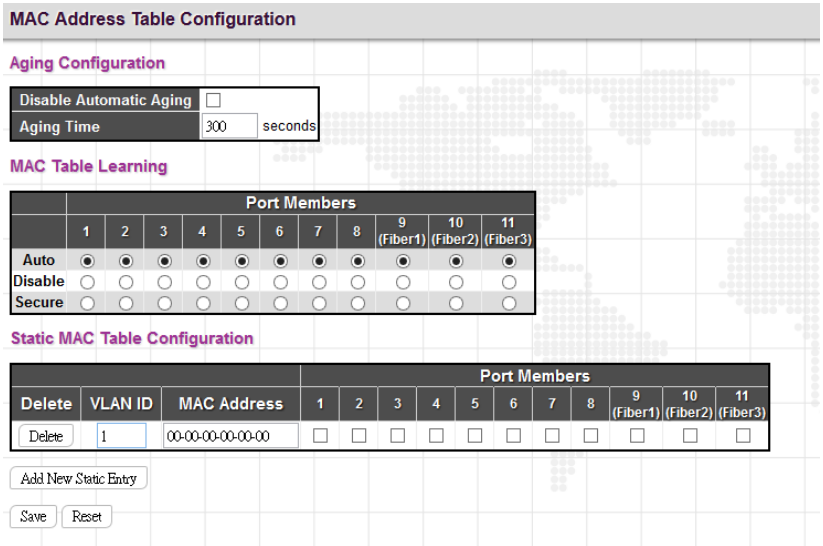
Port Status: PoE service status for the attached device.

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.

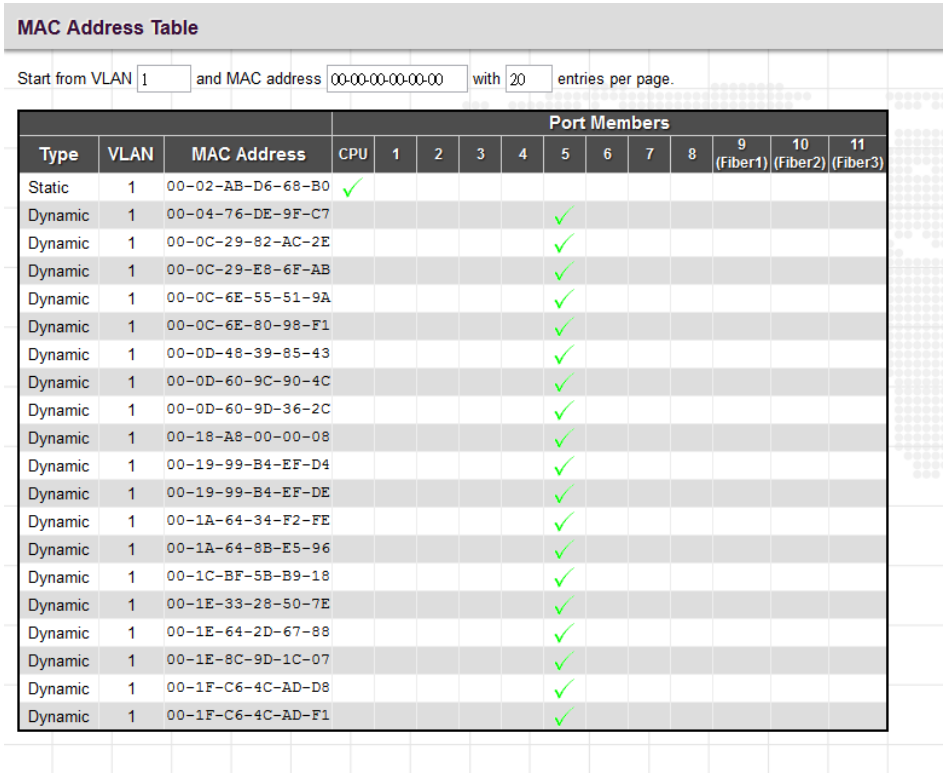
Delete: Delete this MAC address entry.

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.



			Port Members										
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9 (Fiber1)	10 (Fiber2)	11 (Fiber3)
Static	1	00-02-AB-D6-68-B0	✓											
Dynamic	1	00-04-76-DE-9F-C7						✓						
Dynamic	1	00-0C-29-82-AC-2E						✓						
Dynamic	1	00-0C-29-E8-6F-AB						✓						
Dynamic	1	00-0C-6E-55-51-9A						✓						
Dynamic	1	00-0C-6E-80-98-F1						✓						
Dynamic	1	00-0D-48-39-85-43						✓						
Dynamic	1	00-0D-60-9C-90-4C						✓						
Dynamic	1	00-0D-60-9D-36-2C						✓						
Dynamic	1	00-18-A8-00-00-08						✓						
Dynamic	1	00-19-99-B4-EF-D4						✓						
Dynamic	1	00-19-99-B4-EF-DE						✓						
Dynamic	1	00-1A-64-34-F2-FE						✓						
Dynamic	1	00-1A-64-8B-E5-96						✓						
Dynamic	1	00-1C-BF-5B-B9-18						✓						
Dynamic	1	00-1E-33-28-50-7E						✓						
Dynamic	1	00-1E-64-2D-67-88						✓						
Dynamic	1	00-1E-8C-9D-1C-07						✓						
Dynamic	1	00-1F-C6-4C-AD-D8						✓						
Dynamic	1	00-1F-C6-4C-AD-F1						✓						

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.

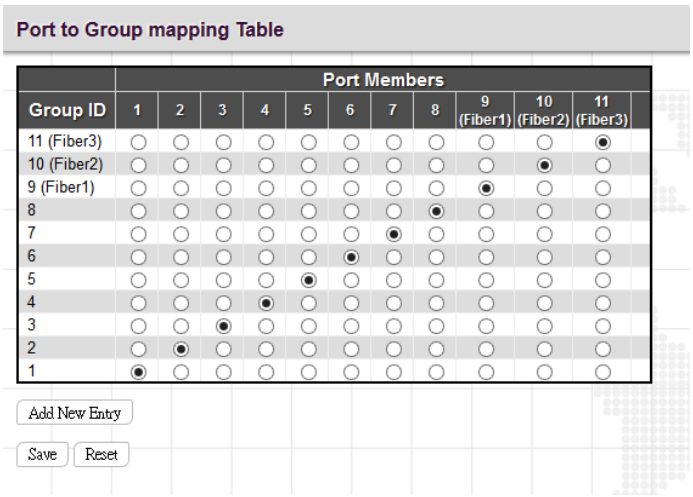
Port Members: Ports associated with this entry.

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

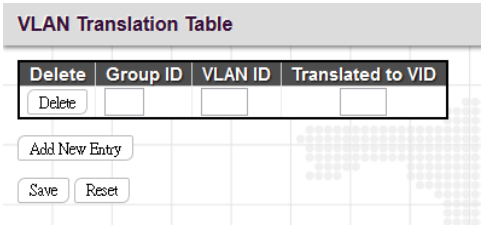


Group ID: The total VLAN Translation group can be used is 11 which is automatically created in Group Mapping Table when entering "Port to Group Mapping" page. A port can be mapped to any of the groups. Multiple ports can be mapped to a single group with the same Group ID.

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

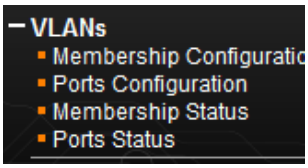
IEEE 802.1Q VLAN (Virtual Local Area Network) is a popular and cost-effectively way to segment your networking deployment by logically grouping devices with similar attributes irrespective of their physical connections. VLANs also segment the network into different broadcast domains so that packets are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

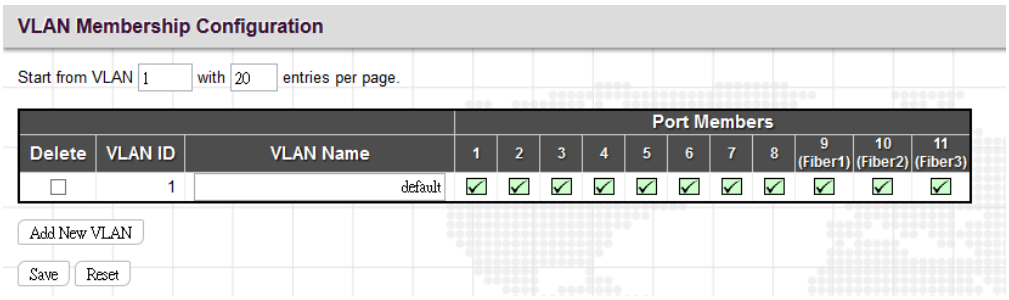
VLANs help control traffic: Traditionally, when networks are not segmented into VLANs, congestion can be easily caused by broadcast traffic that is directed to all devices. To minimize the possibility of broadcast traffic damaging the entire network, VLANs can help group devices that communicate frequently 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 set up the detailed configurations. An example is provided in Appendix C: VLAN Basic Configurations to guide users to configure basic VLAN settings.



4.15.1 Membership Configuration



This configuration page is used to set up and modify VLAN membership. By default, the configuration page shows 20 VLAN entries. However, you can change the starting VLAN and the total of VLAN membership information shown on this page by using “Start from VLAN ___ with ____ entries per page” setting. Up to 4096 VLANs are supported on this Switch.

By default, all ports belong to “default” VLAN with VLAN ID=1.

Delete: Delete this VLAN membership entry.

VLAN ID: Specify the VLAN ID. Valid values are 1 to 4095.

VLAN Name: Provide a description or a name for this VLAN. This field can be left blank. Both alphabets and numbers are allowed. However, if you want to input a description or name, make sure that the field is entered with at least one alphabet. The maximum length of the VLAN Name string is 32.

Port Members:

To include a port in a VLAN, check the box as ✓.

To include a port in a forbidden port list, check the box as shown ✗.

To remove or exclude the port from the VLAN, make sure the box is unchecked.

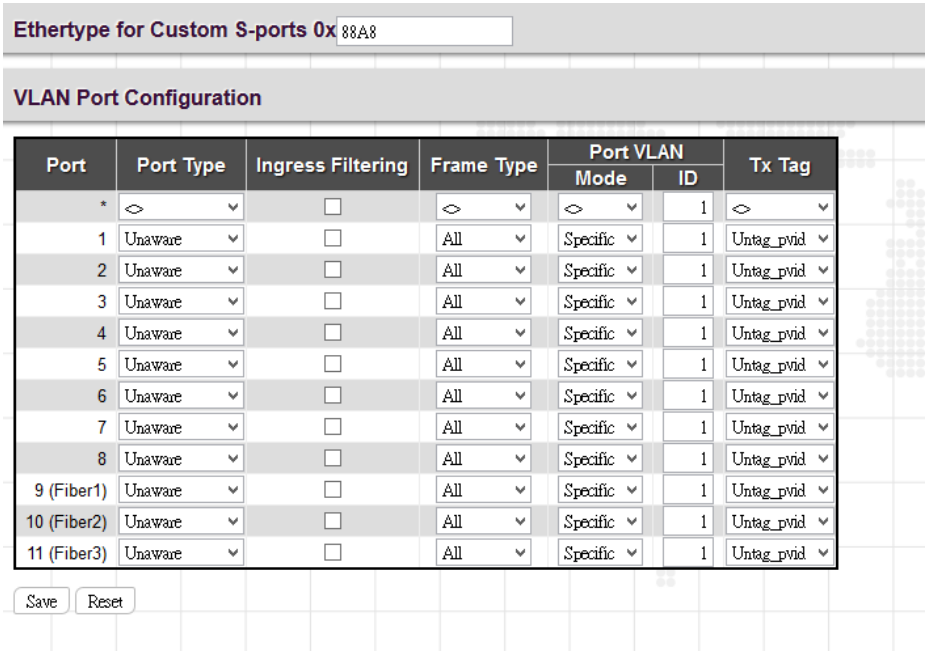
By default, no ports are members, and for every new VLAN entry all boxes are unchecked.

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.

4.15.2 Ports Configuration



Ethertype for Custom S-ports: Specify ether type used for customer s-ports.

VLAN Port Configuration

Port: List the number of each port. “Port *” settings apply to all ports.

Port Type: There are four port types available. Each port type's ingress and egress action is described in the following table.

Action / Port Type	Ingress Action	Egress Action
Unaware	When a tagged frame is received on a port, 1. If the tagged frame with TPID=0x8100, it becomes a double-tag frame and is forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by Unaware port will be set to 0x8100. The final status of the frame after egressing are also affected by egress rule.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
C-port	When a tagged frame is received on a port, 1. If a tagged frame with TIPID=0x8100, it is forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by C-port will be set to 0x8100.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-port	When a tagged frame is received on a port, 1. If a tagged frame with TPID=0x88A8, it is forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TPID of frame transmitted by S-port will be set to 0x88A8
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-custom port	When a tagged frame is received on a port, 1. If a tagged frame with TPID=0x88A8, it is forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TIPID of frame transmitted by S-custom-port will be set to an self-customized value, which can be set by the user using the column of Ethertype for Custom S-ports.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	

Ingress Filtering: If Ingress Filtering is enabled and the ingress port is not a member of a VLAN, the frame from the ingress port is discarded. By default, ingress filtering is disabled.

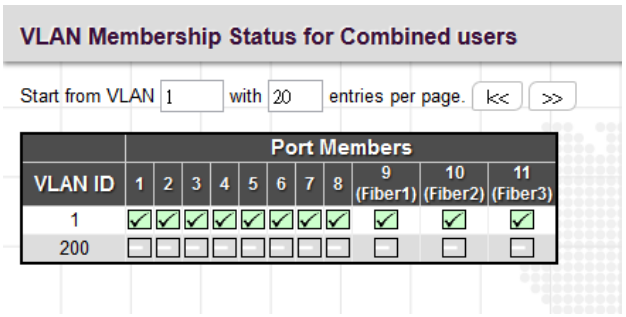
Frame Type: Select the accepted frame types. Available options include All (accept all frames), Tagged (accept only tagged frames), Untagged (accept only untagged frames). This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, frame type is set to All.

Port VLAN: Configures the VLAN identifier for the port. The allowed values are from 1 through 4095. The default value is 1.

NOTE: *The port must be a member of the same VLAN as the Port VLAN ID.*

Tx Tag: Determines egress tagging of a port. Untag_pvid - All VLANs except the configured PVID will be tagged. Tag_all - All VLANs are tagged. Untag_all - All VLANs are untagged.

4.15.3 Membership Status

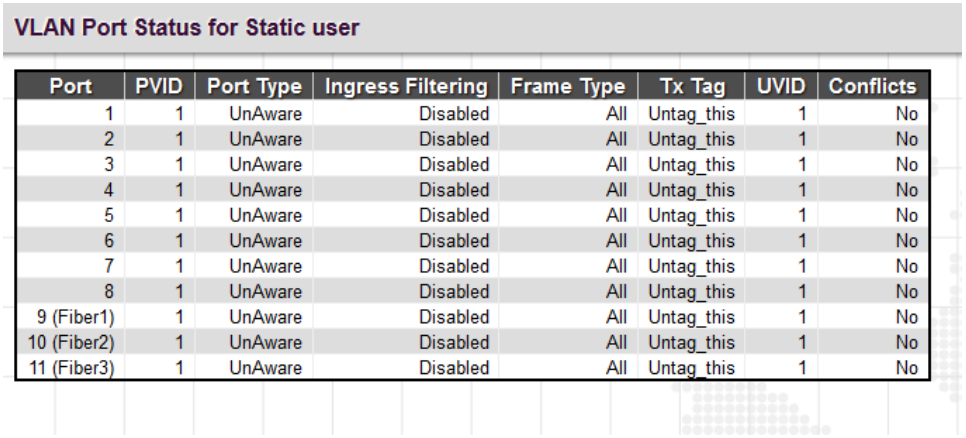


This page shows the current VLAN membership saved on the Switch.

VLAN ID: VLANs that are already created.

Port members: Display member ports on the configured VLANs.

4.15.4 Port Status



VLAN Port Status for Static user

Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag_this	1	No
2	1	UnAware	Disabled	All	Untag_this	1	No
3	1	UnAware	Disabled	All	Untag_this	1	No
4	1	UnAware	Disabled	All	Untag_this	1	No
5	1	UnAware	Disabled	All	Untag_this	1	No
6	1	UnAware	Disabled	All	Untag_this	1	No
7	1	UnAware	Disabled	All	Untag_this	1	No
8	1	UnAware	Disabled	All	Untag_this	1	No
9 (Fiber1)	1	UnAware	Disabled	All	Untag_this	1	No
10 (Fiber2)	1	UnAware	Disabled	All	Untag_this	1	No
11 (Fiber3)	1	UnAware	Disabled	All	Untag_this	1	No

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

Port: The port number.

PVID: The port VLAN ID assigned to a port.

Port Type: Display the selected port type on a port.

Ingress Filtering: Display whether Ingress Filtering is enabled or disabled.

Frame Type: Display the accepted frame type on a port.

Tx Tag: Display the Egress action on a port.

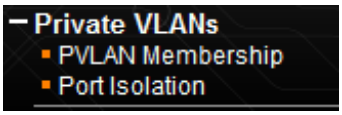
UVID: Display the untagged VLAN ID. A port's UVID determines the packet's behavior at the egress side. If the VID of Ethernet frames leaving a port match the UVID, these frames will be sent untagged.

Conflicts: Display whether conflicts exist or not. When a software module requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

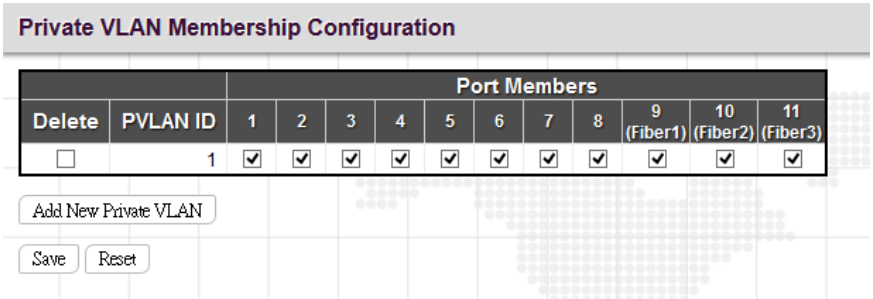
*Functional conflicts between features.
*Conflicts due to hardware limitations.
*Direct conflicts between user modules.

4.16 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.

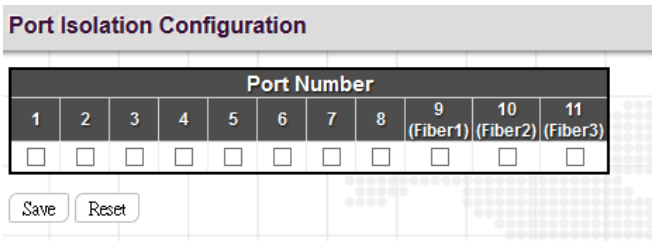
Delete: Delete this VLAN membership entry.

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

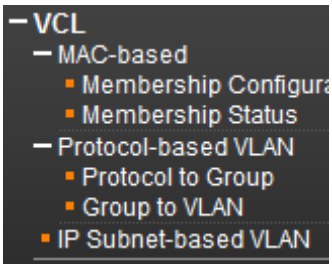


Private VLAN is used to group ports together so as to prevent communications within PVLAN. Port Isolation is used to prevent communications between customer ports in a same Private VLAN. The port that is isolated from others cannot forward any unicast, multicast or broadcast traffic to any other ports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

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

4.17 VCL

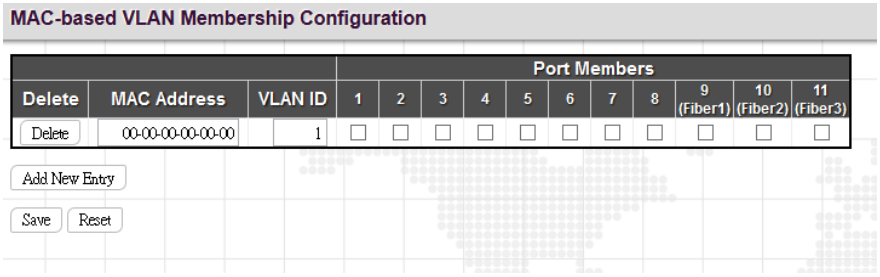
The “VCL” menu contains the following sub menus.



4.17.1 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).

4.17.1.1 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.

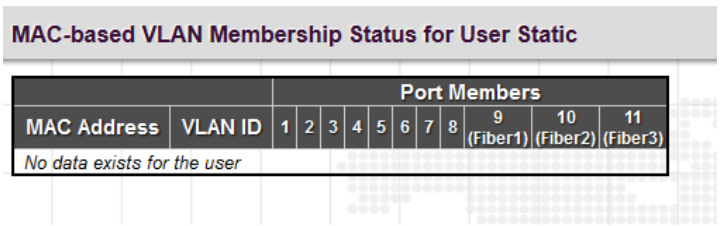
Port Members: Ports that belong to this VLAN.

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.

4.17.1.2 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.

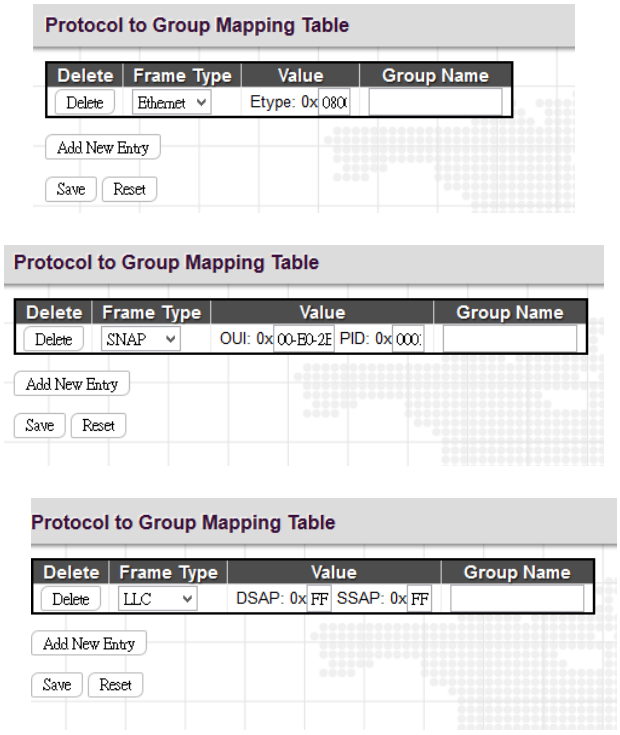
Port Members: Display ports that accept the configured MAC address.

4.17.2 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.

4.17.2.1 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.

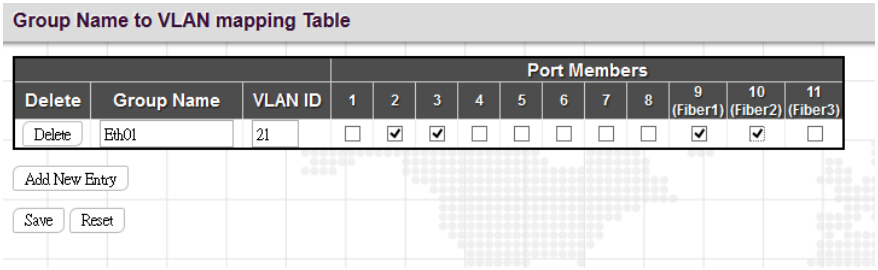
OUI: A value in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value in the ranges of 0x00-0xff.

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).

4.17.2.2 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.

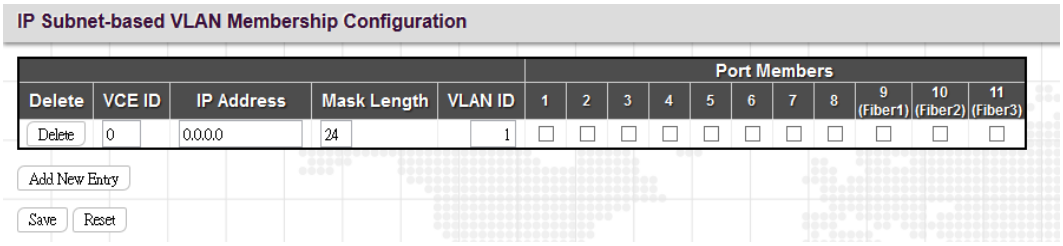
Port Members: Assign ports to this rule.

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.

4.17.3 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.

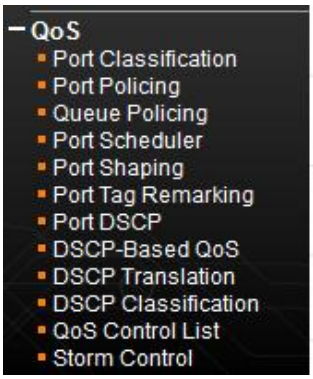
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

4.18 QoS

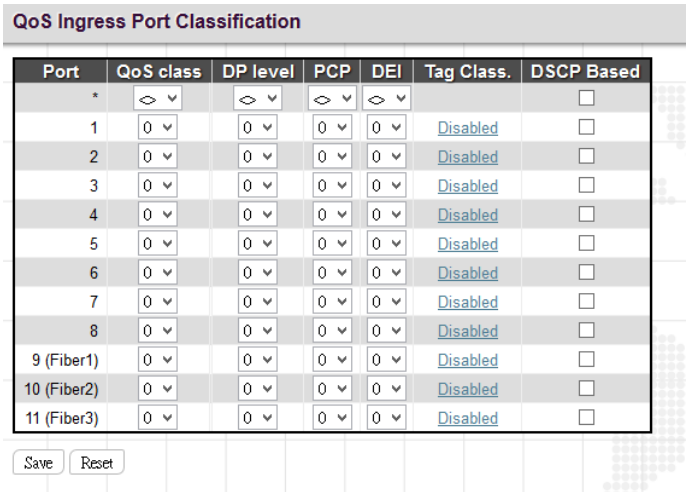
Network traffic is always unpredictable and the only basic assurance that can be offered is the best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria and receives 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.



4.18.1 Port Classification



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.

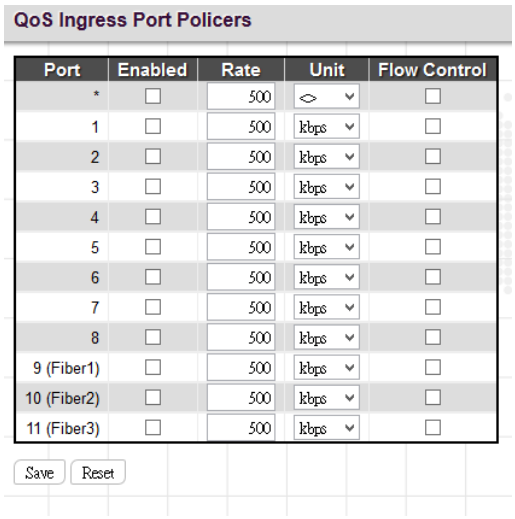
Tag Class: This field displays classification mode for tagged frames on this port:

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).

4.18.2 Port Policing



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

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

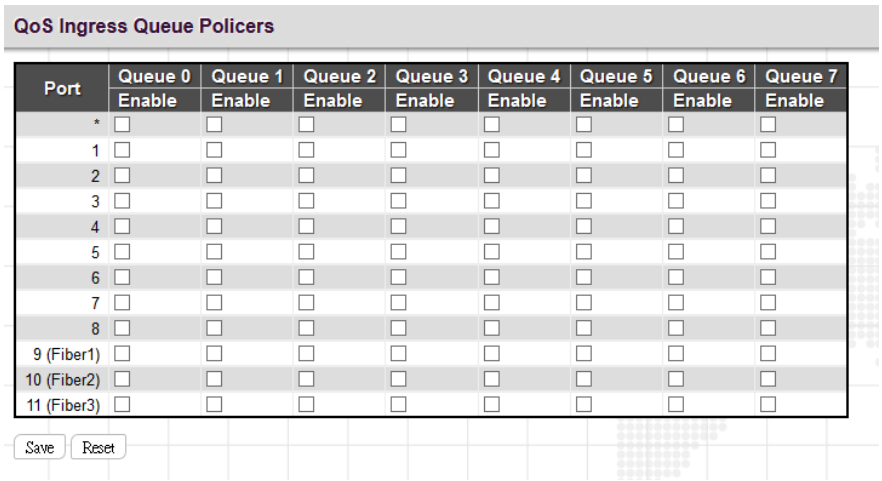
Enabled: Select the checkbox to enable port policing function on a port.

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.

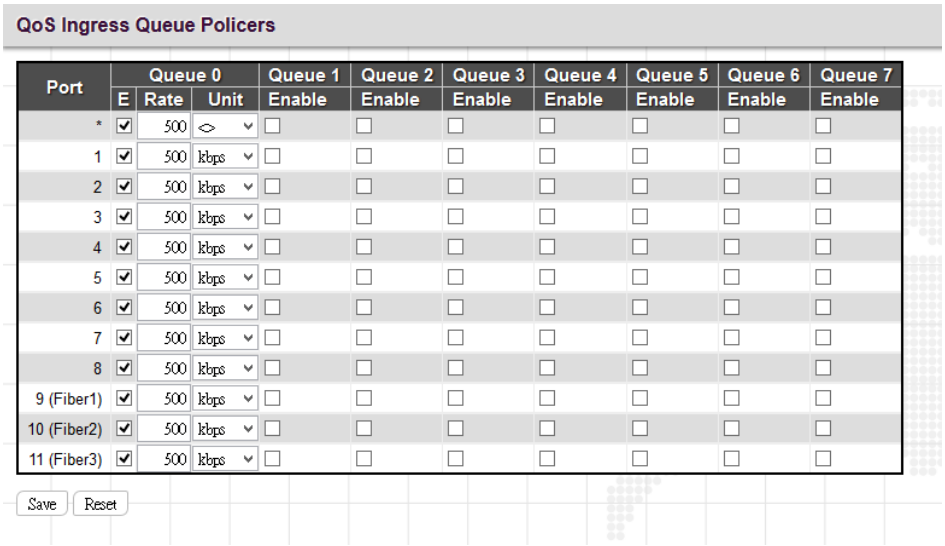
4.18.3 Queue Policing



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:



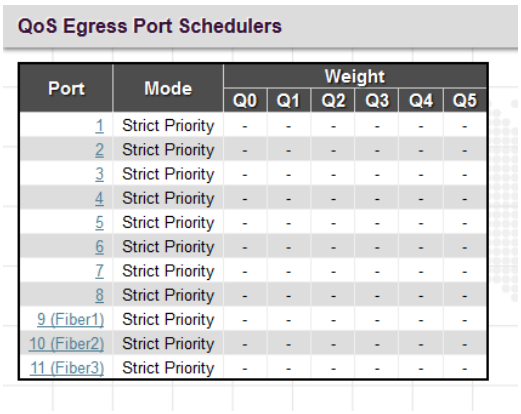
Rate: Indicate the rate for the ingress queue policer. By default, 500kbps is used. Allowed range for kbps is 100 to 1000000. Allowed range for Mbps is 1 to 3300Mbps.

Unit: Select he unit of measure for the ingress queue policer.

Save: Save the current running configurations to memory.

Reset: Clear all selected settings.

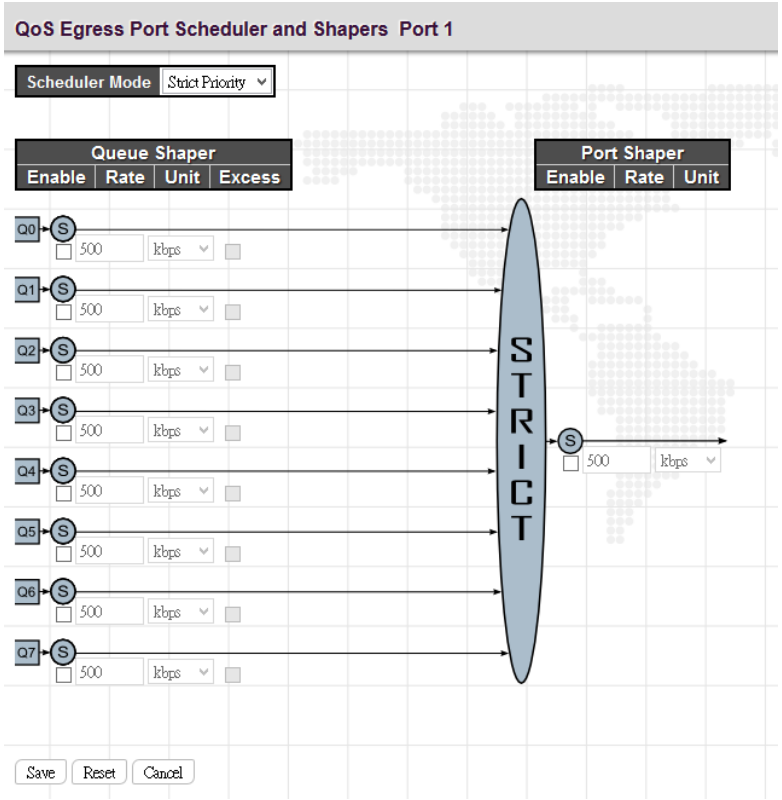
4.18.4 Port Scheduler

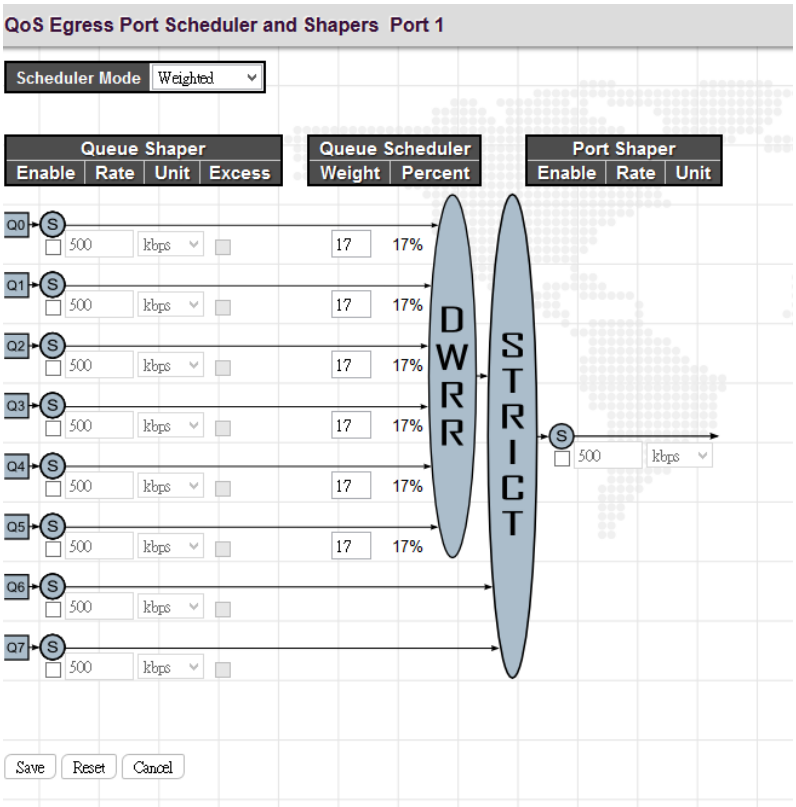


Port: Click the port to set up detailed settings for port scheduler.

Mode: Display scheduler mode selected.

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





This page allows you to set up the Schedulers and Shapers for a specific port.

Scheduler Mode: The device offers two modes to handle queues.

Strict mode: This gives egress queues with higher priority to be transmitted first before lower priority queues are serviced.

Weight mode: Deficit Weighted Round-Robin (DWRR) queuing which specifies a scheduling weight for each queue. (Options: Strict, Weighted; Default: Strict) DWRR services the queues in a manner similar to WRR, but the next queue is serviced only when the queue's Deficit Counter becomes smaller than the packet size to be transmitted.

Queue Shaper/Port Shaper/Queue Shaper

Enable: Select the checkbox to enable queue shaper on a certain queue for this selected port.

Rate: Indicate the rate for the queue shaper. By default, 500kbps is used. Allowed range for kbps is 100 to 1000000. Allowed range for Mbps is 1 to 3300Mbps.

Unit: Select he unit of measure for the queue shaper.

Excess: Select the checkbox to allow excess bandwidth.

Queue Schedule

Queue Scheduler: When Scheduler Mode is set to Weighted, the user needs to indicate a relative weight for each queue. DWRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Weight: Assign a weight to each queue. This weight sets the frequency at which each queue is polled for service and subsequently affects the response time software applications assigned a specific priority value.

Percent: The weight as a percentage for this queue.

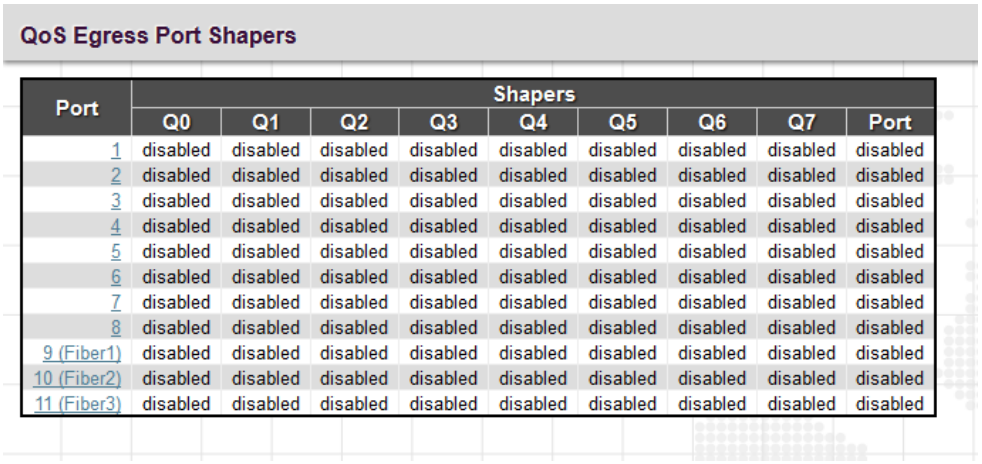
Port Shaper: Set the rate at which traffic can egress this queue.

Enable: Select the checkbox to enable Port shaper.

Rate: Indicate the rate for Port Shaper. By default, 500kbps is used. Allowed range for kbps is 100 to 1000000. Allowed range for Mbps is 1 to 3300Mbps.

Unit: Select the rate of measure

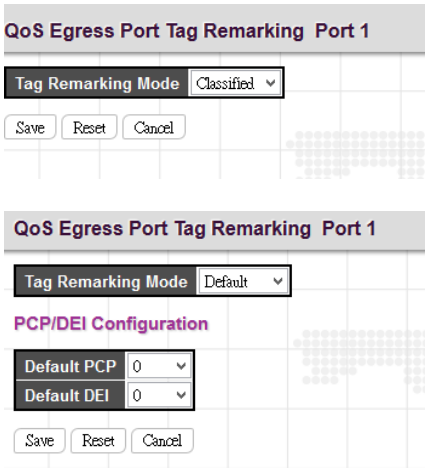
4.18.5 Port Shaping

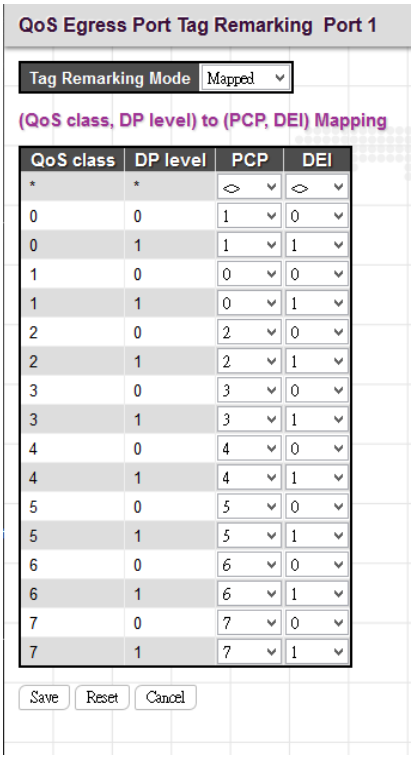


This displays each port's queue shaper and port shaper's rate.

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.

4.18.6 Port Tag Remarking





Tag Remarking Mode: Select the appropriate remarking mode used by this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values (Default PCP:0; Default DEI:0).

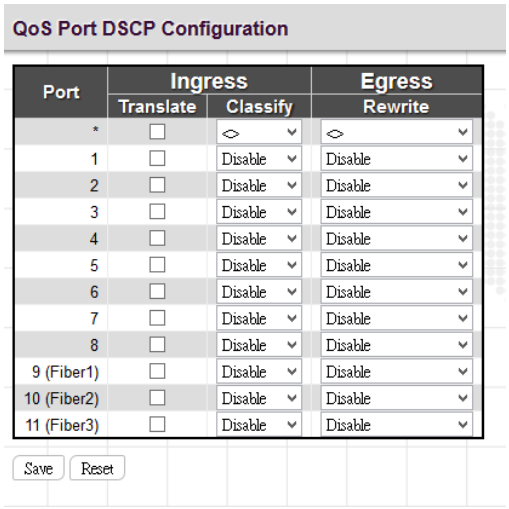
Mapped: Use the mapping of the classified QoS class values and DP levels to PCP/DEI values.

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

PCP: Remarks matching egress frames with the specified Priority Code Point (or User Priority) value. (Range: 0~7; Default: 0)

DEI: Remarks matching egress frames with the specified Drop Eligible Indicator. (Range: 0~1; Default: 0)

4.18.7 Port DSCP



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

Ingress Translate: Select the checkbox to enable ingress translation of DSCP values based on the selected classification method.

Ingress Classify: Select the appropriate classification method:

Disable: No ingress DSCP classification is performed.

DSCP=0: Classify if incoming DSCP is 0.

Selected: Classify only selected DSCP for which classification is enabled in DSCP Translation table.

All: Classify all DSCP.

Egress Rewrite: Configure port egress rewriting of DSCP values.

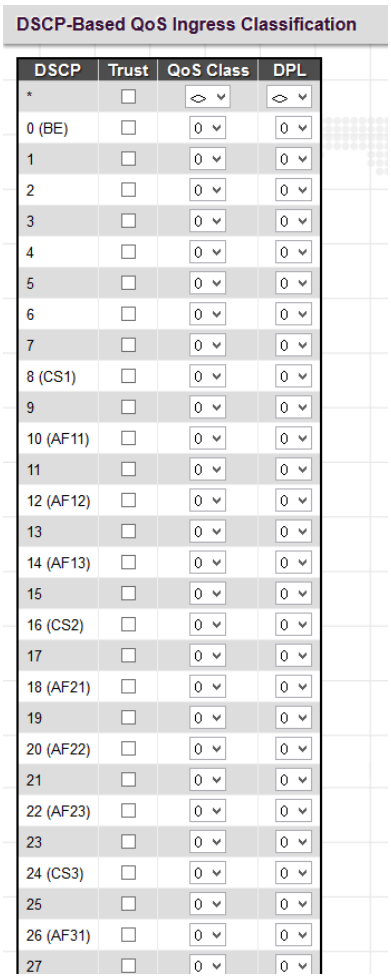
Disable: Egress rewriting is disabled.

Enable: Enable egress rewriting is enabled but with remapping.

Remap DP aware: Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. Depending on the frame's DP level, the remapped DSCP value is either taken from the DSCP Translation table, Egress Remap DP0 or DP1 field.

Remap DP unaware: Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. The remapped DSCP value is always taken from the DSCP Translation table, Egress Remap DP0 field.

4.18.8 DSCP-Based QoS



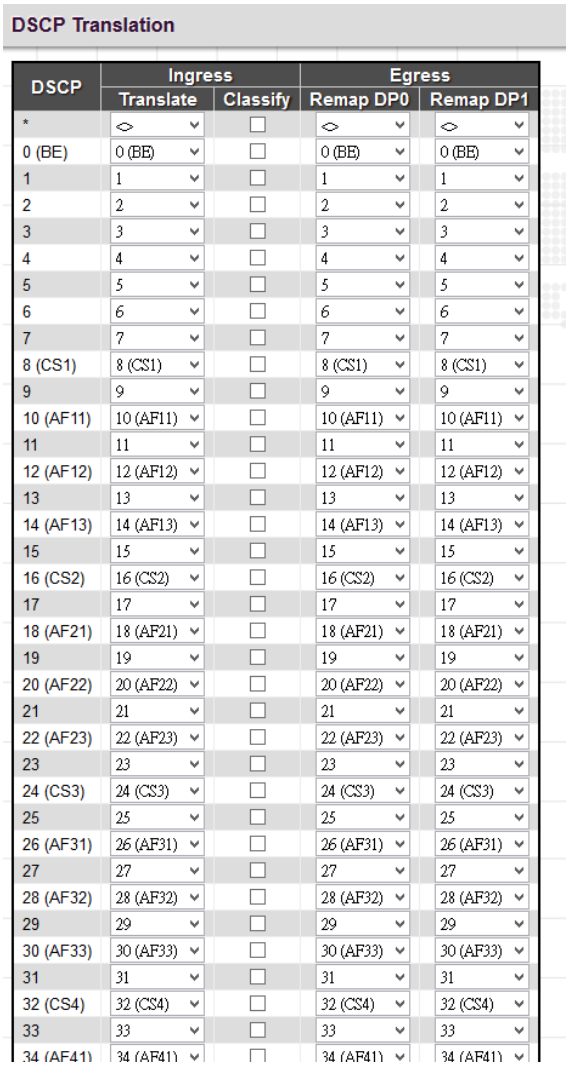
DSCP: DSCP value in ingress packet. DSCP range is from 0 to 63.

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.

4.18.9 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.

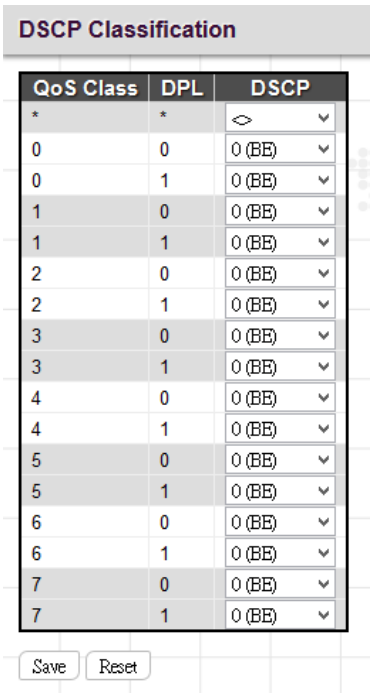
Ingress Translate: Enable Ingress Translation of DSCP values based on the specified classification method.

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.

4.18.10 DSCP Classification



Map DSCP values to QoS class and DPL value.

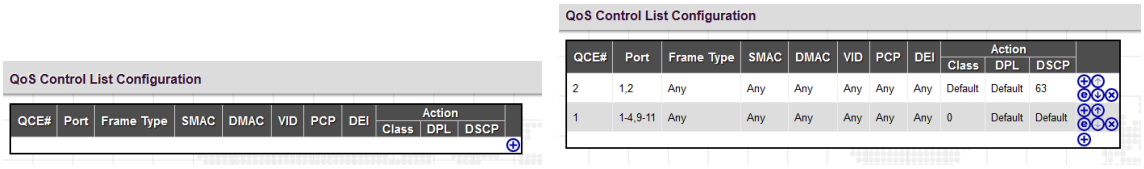
QoS Class: List of actual QoS class values.

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.

4.18.11 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.



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.

Frame Type: Display the frame type to look for in incoming frames. Possible frame types are Any, Ethernet, LLC SNAP, IPv4, IPv6.

SMAC: Source MAC address.

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

VID: Display VLAN ID (1-4095)

PCP: Display PCP value.

DEI: Display DEI value.

Action: Display the classification action taken on ingress frames when the configured parameters are matched in the frame's content. If a frame matches the QCL, the following actions will be taken.

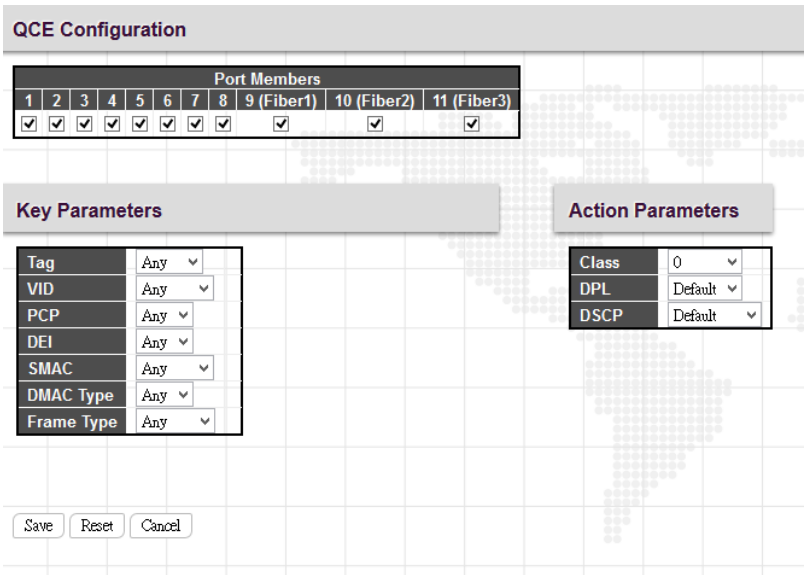
Class: If a frame matches the QCL, it will be put in the queue corresponding to the specified QoS class.

DPL: The drop precedence level will be set to the specified value.

DSCP: The DSCP value will be set to the specified value.

You can modify each QCE (QoS Control Entry) in the table using the following buttons:
: 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

Tag: Select VLAN tag type (Tag or Untag). By default, any type is used.

VID: Select VID preference. By default, any VID is used. Select "Specific", if you would like to designate a VID to this QCL entry. Or Select "Range", if you would like to map a range of VIDs to this QCL entry.

PCP: Select a PCP value (either specific value or a range of values are provided). By default, any is used.

DEI: Select a DEI value. By default, any is used.

SMAC: Select source MAC address type. By default, any is used. Select "Specific" to specify a source MAC (first three bytes of the MAC address or OUI).

DMAC Type: Select destination MAC address type. By default, any is used. Other options available are "UC" for unicast, "MC" for multicast, and "BC" for broadcast.

Frame Type: The frame types can be selected are listed below.

Any: By default, any is used which means that all types of frames are allowed.

Ethernet: This option can only be used to filter Ethernet II formatted packets (Options: Any, Specific – 600-ffff hex; Default: ffff). Note that 800 (IPv4) and 86DD (IPv6) are excluded. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

LLC: LLC refers to Link Logical Control and further provides three options.

SSAP: SSAP stands for Source Service Access Point address. By default, any is used. Select specific to indicate a value (0x00 - 0xFF).

DSAP: DSAP stands for Destination Service Access Point address. By default, any is used. Select specific to indicate a value (0x00 to 0xFF).

Control: Control field may contain command, response, or sequence information depending on whether the LLC frame type is Unnumbered, Supervisory, or Information. By default, any is used. Select specific to indicate a value (0x00 to 0xFF).

SNAP: SubNetwork Access Protocol can be distinguished by an OUI and a Protocol ID. (Options for PID: Any, Specific (0x00-0xffff); Default: Any) If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI isother than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

IPv4:

Protocol: IPv4 frame type includes Any, TCP, UDP, Other. If "TCP" or "UDP" is selected, you might further define Sport (Source port number) and Dport (Destination port number).

Source IP: Select source IP type. By default, any is used. Select "Specific" to indicate self-defined source IP and submask format. The address and mask must be in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero

IP Fragment: By default, any is used. Datagrams sometimes may be fragmented to ensure they can pass through a network device that uses a maximum transfer unit smaller than the original packet's size.

DSCP: By default, any is used. Select "Specific" to indicate a DSCP value. Select "Range" to indicate a range of DSCP value.

IPv6:

Protocol: IPv6 protocol includes Any, TCP, UDP, Other. If "TCP" or "UDP" is selected, you may need to further define Sport (Source port number) and Dport (Destination port number).

Source IP: Select source IP type. By default, any is used. Select "Specific" to indicate self-defined source IP and submask format.

DSCP: By default, any is used. Select "Specific" to indicate a DSCP value. Select "Range" to indicate a range of DSCP value.

Action Parameters

Specify the classification action taken on ingress frame if the parameters match the frame's content. The actions taken include the following:

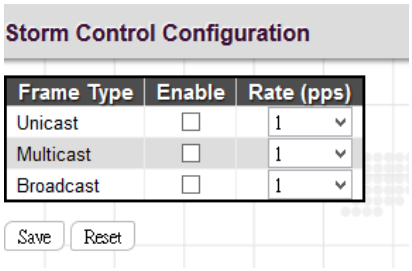
Class: If a frame matches the QCE, it will be put in the queue corresponding to the specified QoS class or placed in a queue based on basic classification rules.

DPL: If a frame matches the QCE, the drop precedence level will be set to the selected value or left unchanged.

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

4.18.12 Storm Control

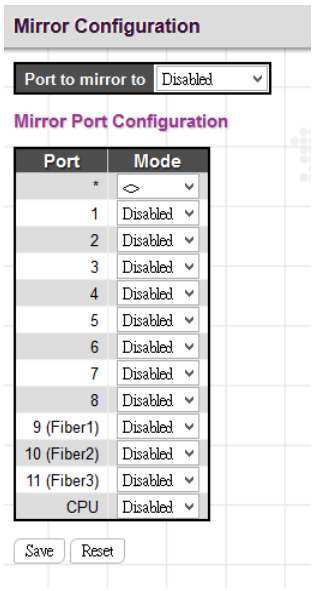
Storm Control is used to keep a network from downgraded performance or a complete halt by setting up a threshold for traffic like broadcast, unicast and multicast. When a device on the network is malfunctioning or application programs are not well designed or properly configured, storms may occur and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

4.19 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.

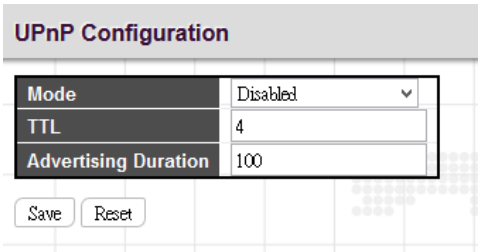
Disabled: Disable the port mirroring function on a given port.

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.

4.20 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.

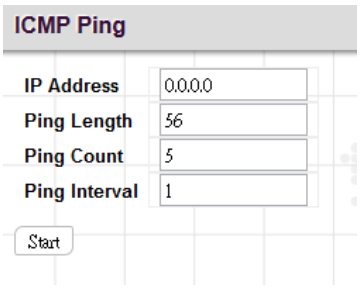
Advertising Duration: This defines how often an UPnP advertisement is sent. The duration is carried in Simple Service Discover Protocol (SSDP) packets which informs a control point how often it should receive a SSDP advertisement message from the switch. By default, the advertising duration is set to 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.

4.21 Diagnostics

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

4.21.1 Ping

This Ping function is for ICMPv4 packets.



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

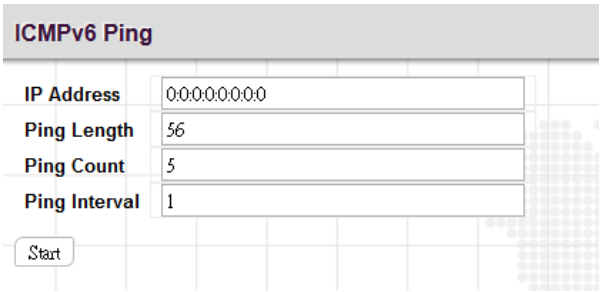
Ping Length: The size or length of echo packets.

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

Ping Interval: The time interval between each ping request.

4.21.2 Ping6

This Ping function is for ICMPv6 packets.



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

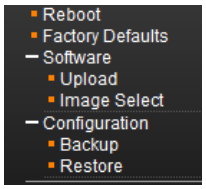
Ping Length: The size or length of echo packets.

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

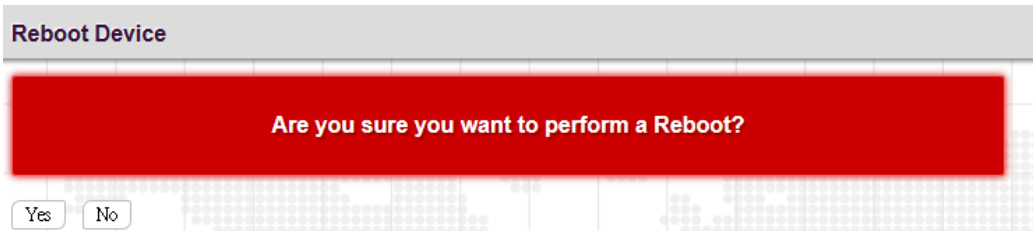
Ping Interval: The time interval between each ping request.

4.22 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.

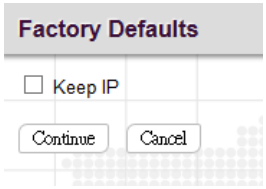


4.22.1 Reboot



Click “Yes” button to reboot the switch.

4.22.2 Factory Defaults

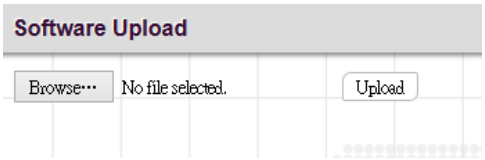


Keep IP: Check the “Keep IP” box if you want to use the current IP settings after restoring to factory default settings.

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.

4.22.3 Software

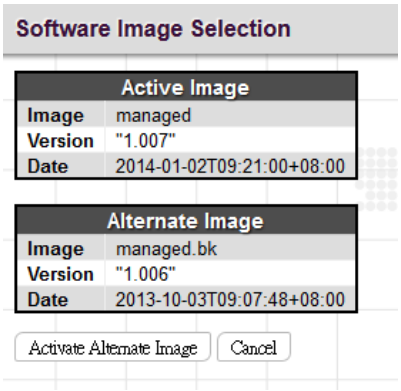
4.22.3.1 Upload



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.

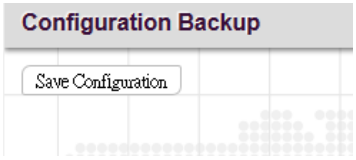
4.22.3.2 Image Select



Select the image file to be used in this device.

4.22.4 Configuration

4.22.4.1 Backup



Save a copy of current running configurations in XML format in your local device.

4.22.4.2 Restore

Restore With IP: Check the “Restore With IP” box if you want to use the IP settings saved in the Configuration file that you want to restore.

Select a configuration file and then click “Upload” to restore the previously saved settings. Once uploading is successful, the settings saved in the uploaded configuration file will take effect immediately.

APPENDIX A. u-Ring CONFIGURATION PROCEDURE

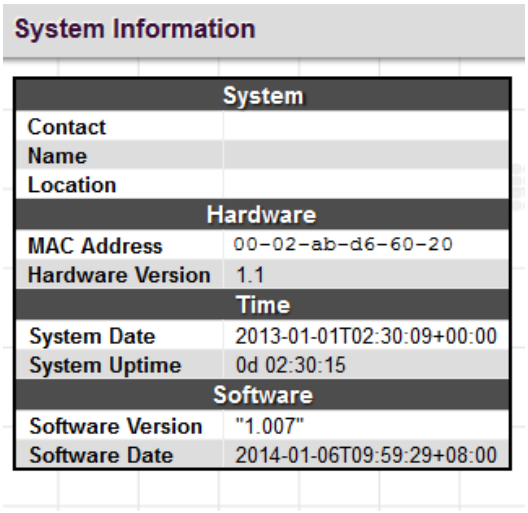
Introduction

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.

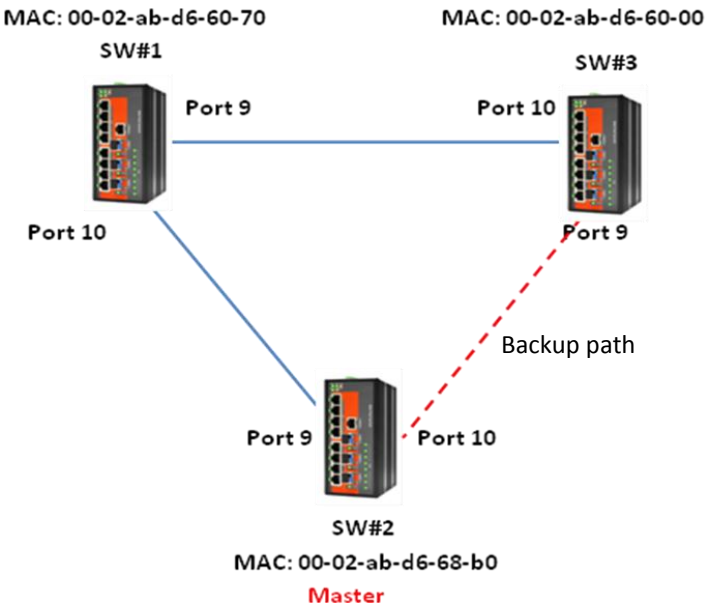
The purpose of this document is to give valuable aid to a network engineer in topology design, deployment and configuration of Industrial Grade Ethernet Switches for ring protection. The example uses a ring of three units and performs all configurations via the web GUI management interface.

Equipment Used in this Example:

1. The Industrial Grade Ethernet Switches with u-Ring redundancy protocol * 3
2. Laptop * 1



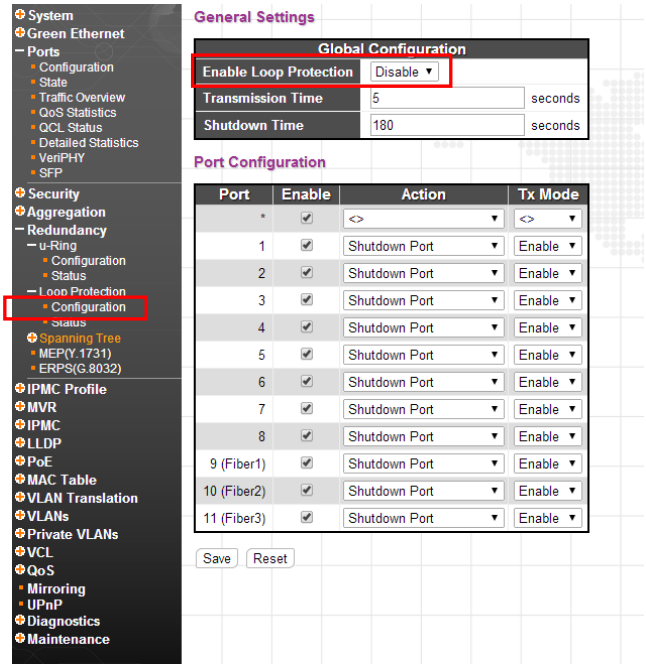
Testing Topology:

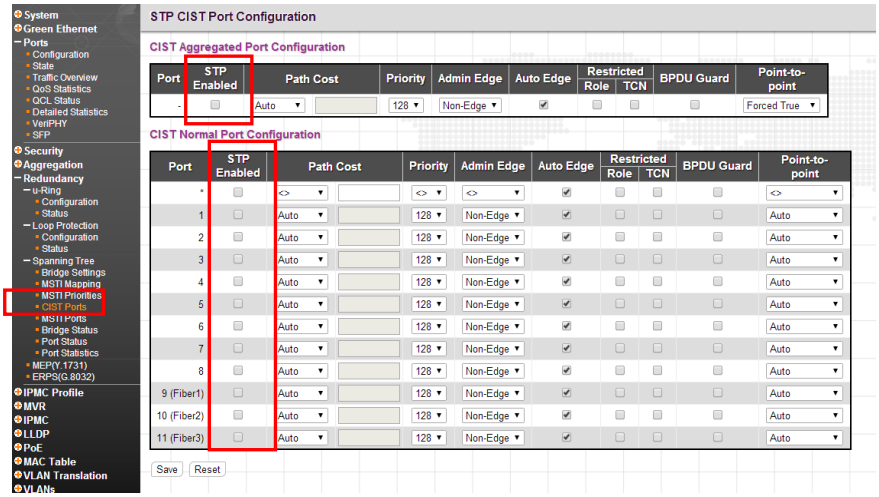


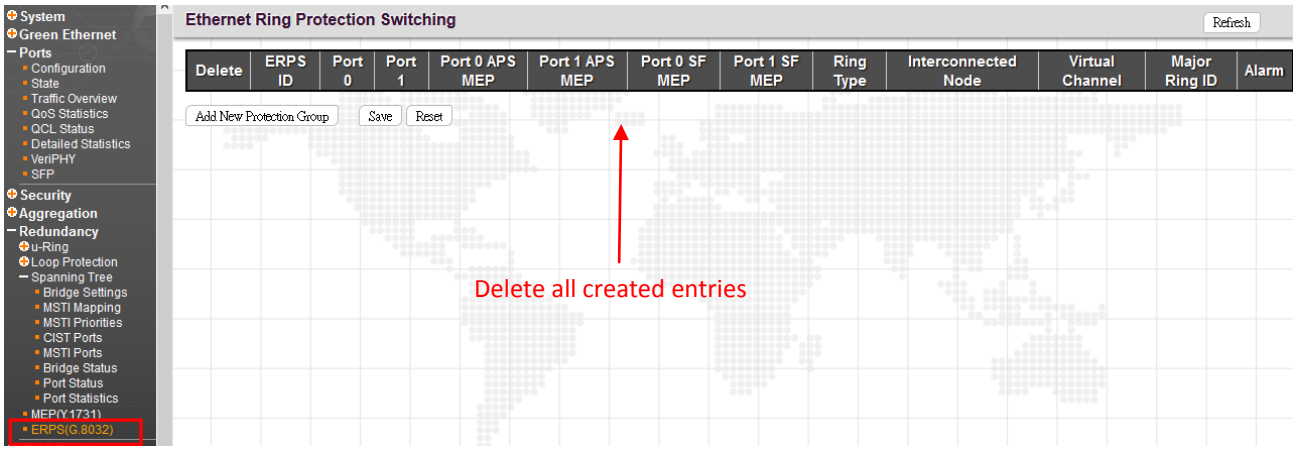
Warning: During initial configuration and in order to avoid an Ethernet "Loop" condition, please do not connect the physical Ring prior to completion of the u-Ring configuration.

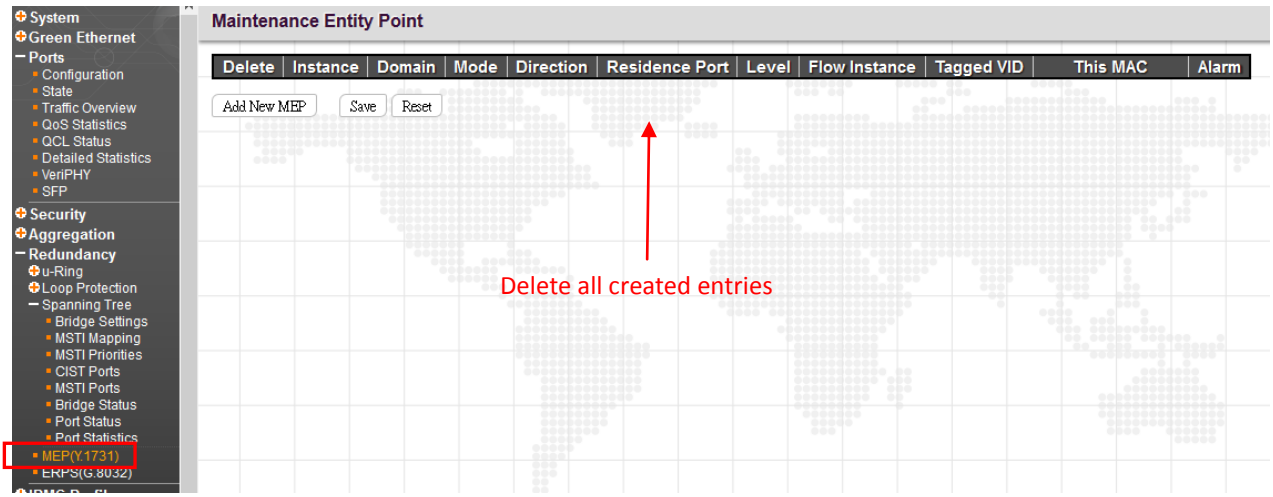
Configuration:

A. Make sure SW#1, SW#2, SW#3's Loop Protection, STP, ERPS and MEP configurations are all disabled.



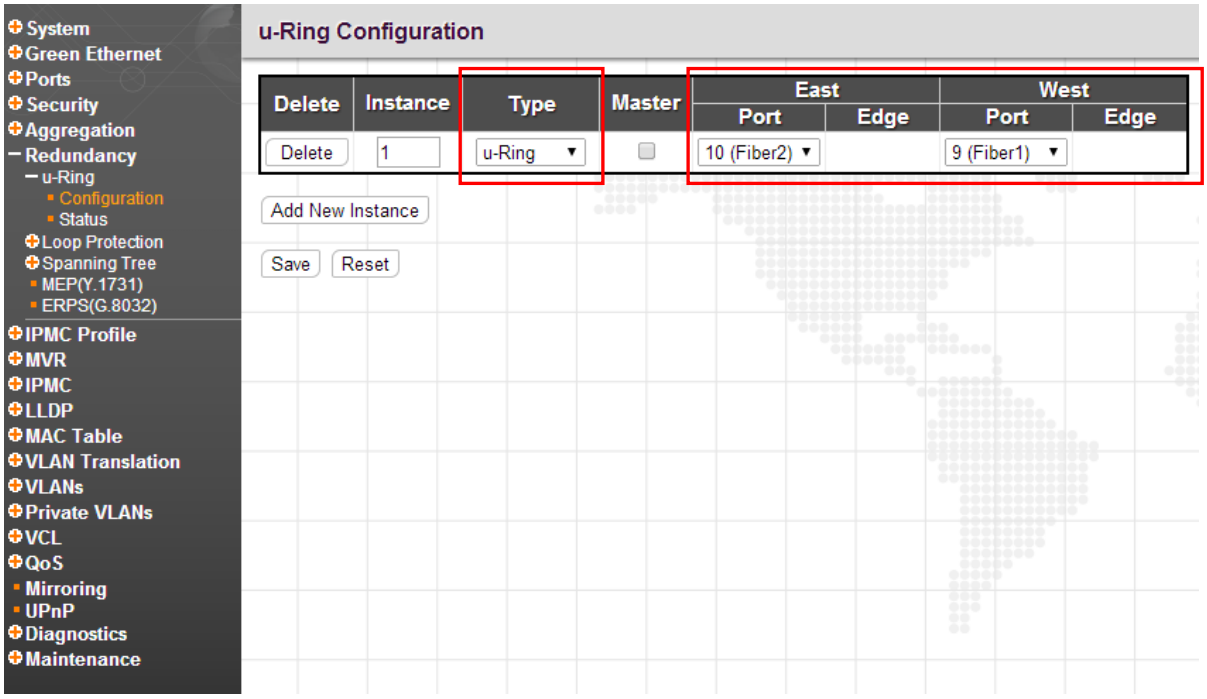




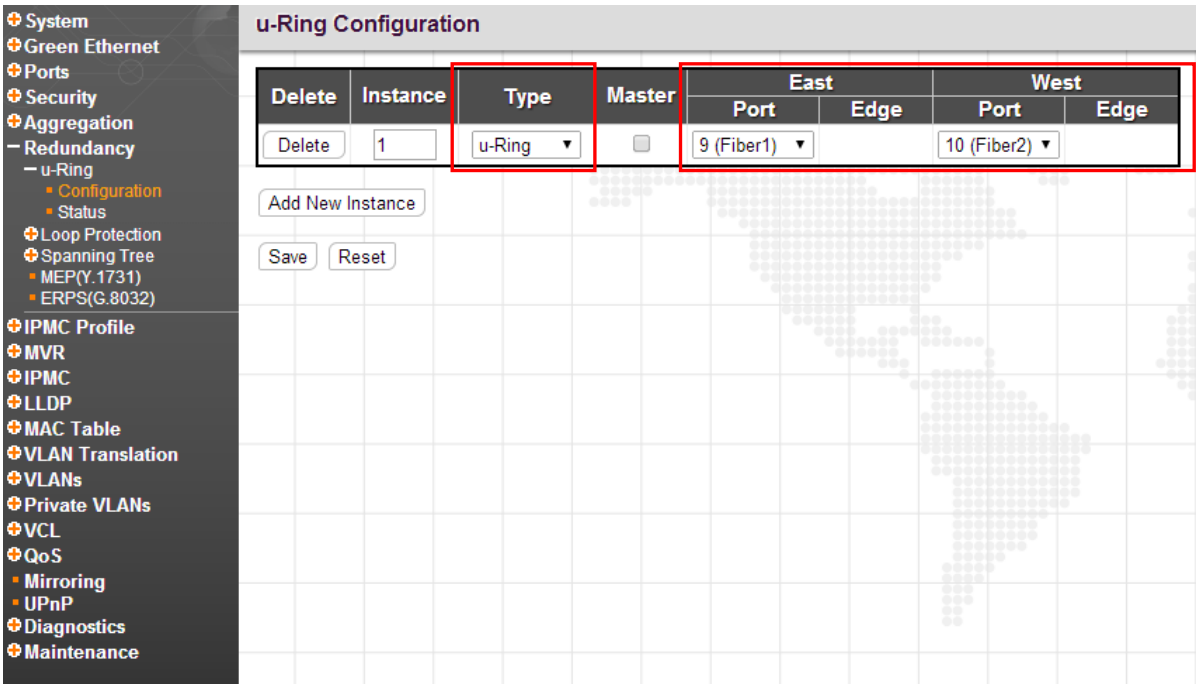


B. Add a new Instance in Redundancy>u-Ring>Configuration page

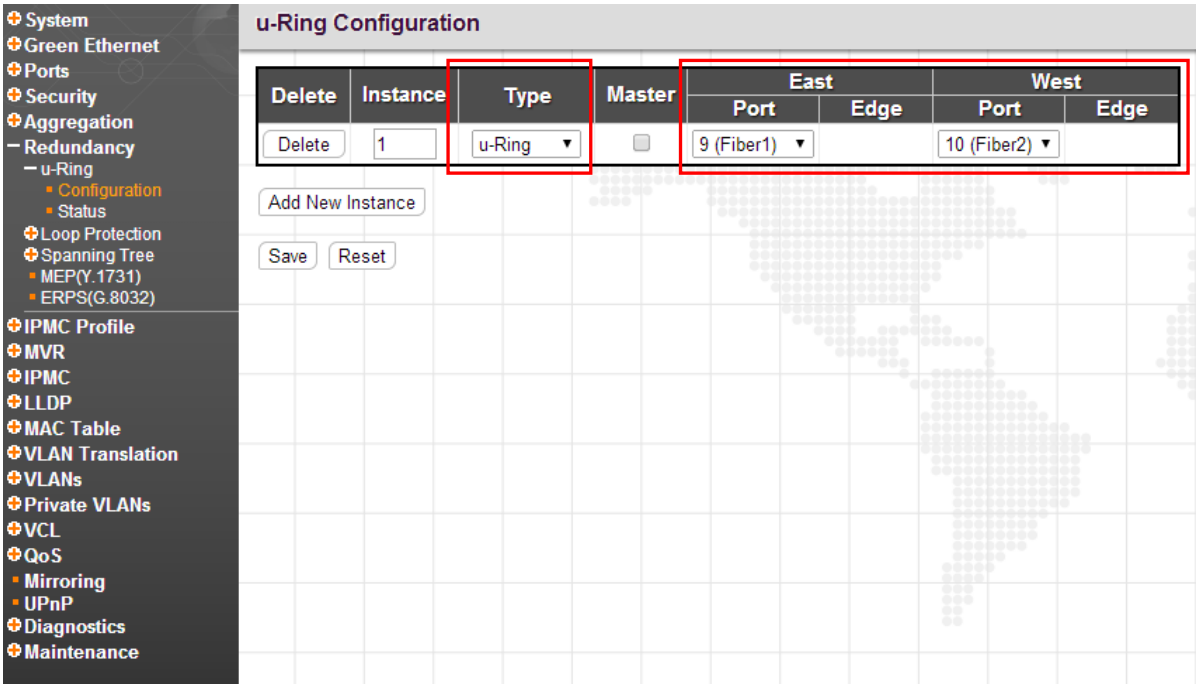
SW#1: Select “u-Ring” type and select East port (10 Fiber 2) and West port (9 Fiber1) from the pull-down menu. Then click “Save” button.



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.



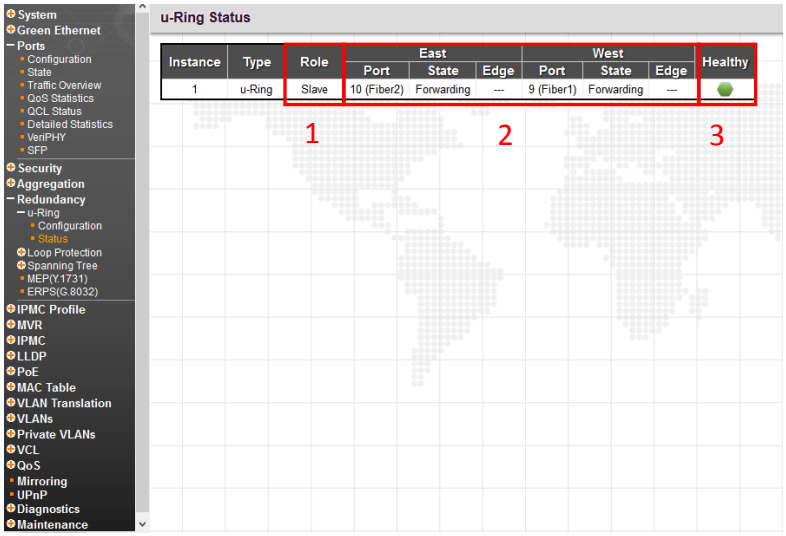
C. Connect the physical ring. Once cabling is connected correctly, u-Ring starts working.

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.

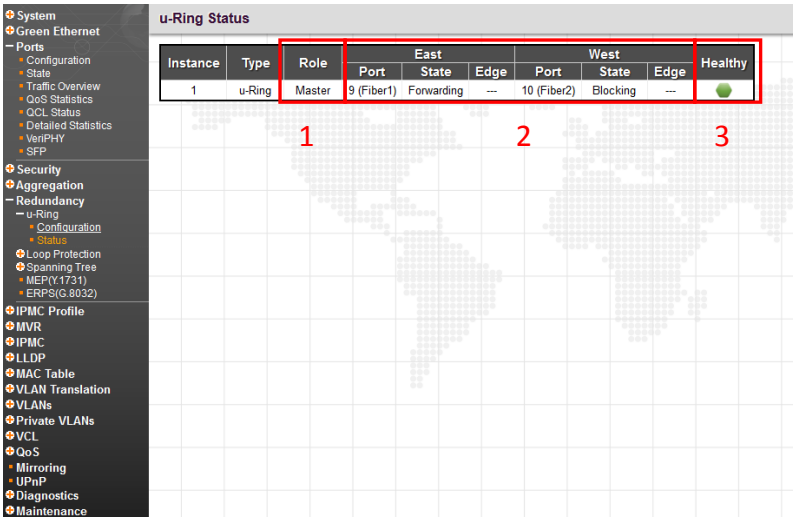
A. Check the Redundancy>u-Ring>status page of each device.

SW#1



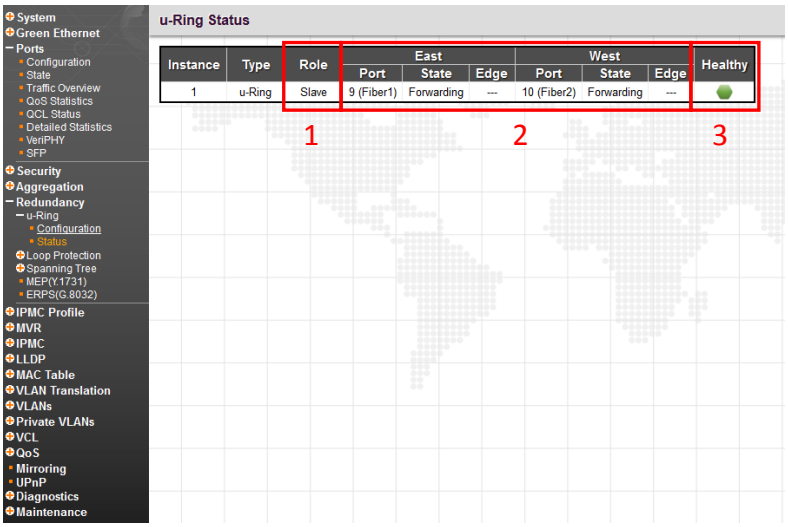
1. The role of SW#1 is “Slave” which means that East and West port will not be blocked (forward data).
2. East and West port are “Forwarding” data.
3. The “Green” color means that the ring connection is good.

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.

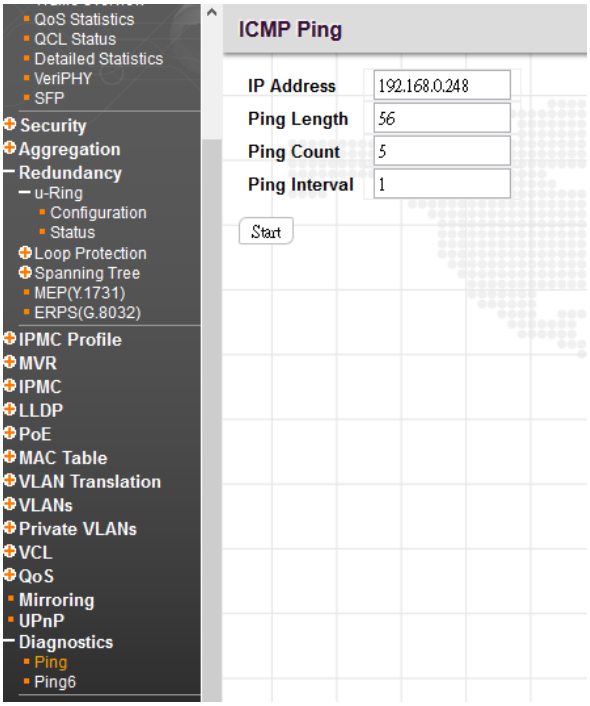
SW#3

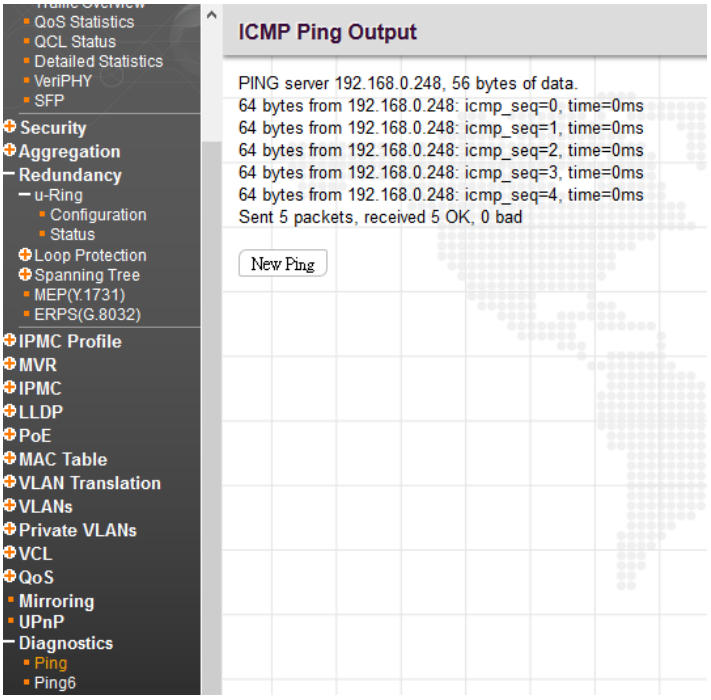


1. The role of SW#3 is "Slave" which means that East and West port will not be blocked (forward data).
2. East and West port are "Forwarding" data.
3. The "Green" color means that the ring connection is good.

B. Using Ping to test the connectivity between Switches.

Go to Diagnostics>Ping page.



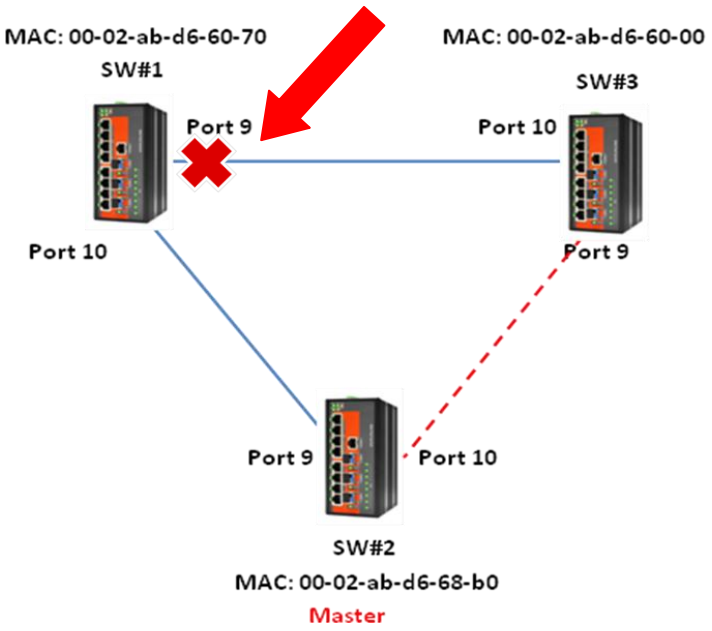


If one of the switches cannot ping the other switch, please check that you have correct cabling and configurations including IP assignment, u-Ring configuration.

C. Disconnect a port to see whether the status of blocked port in SW#2 (Port 10) changes to "Forwarding" or not.

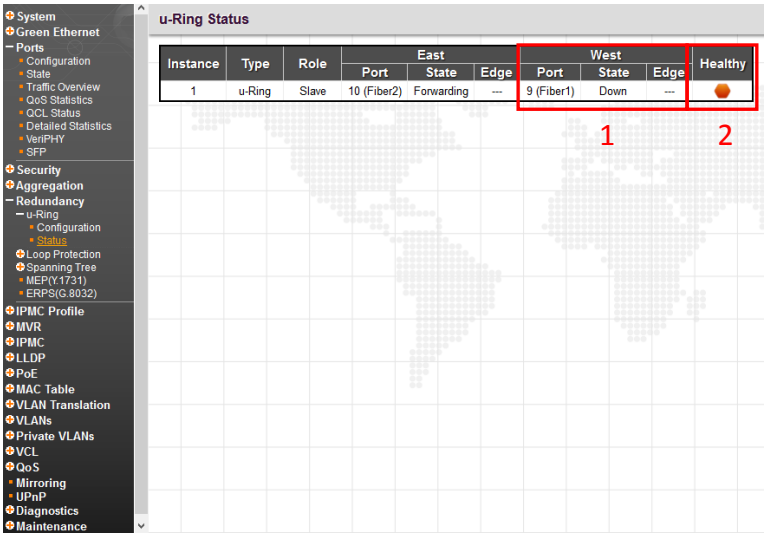
1. Manually disconnect Port 9 in SW#1.

Manually disconnect Port 9 in SW#1.



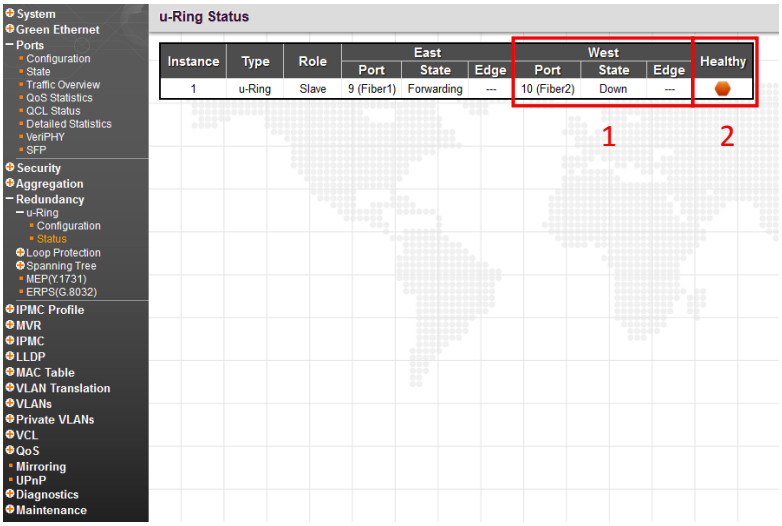
2. The status of SW#1 Port 9 and SW#3 Port 10 is down.

SW#1



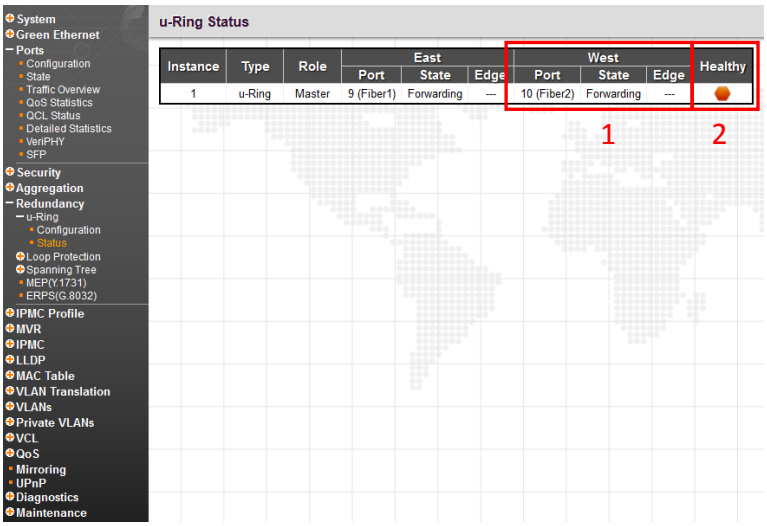
1. The status of port 9 is down.
2. The “Red” alarm color means that there is something wrong with the ring (This may result from physical disconnection).

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.

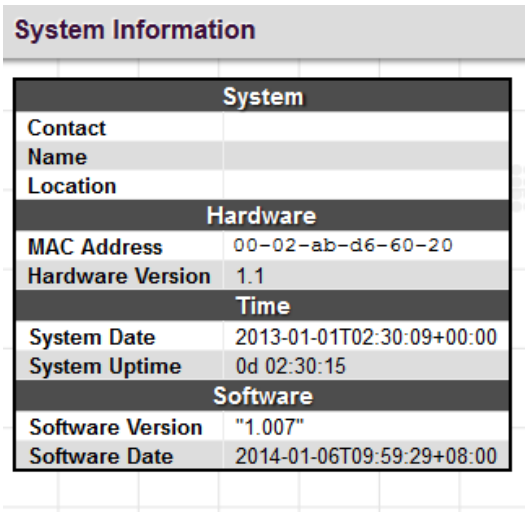
Any failure along the ring triggers a R-APS(SF) (R-APS signal fail) message along both directions from the nodes adjacent to the failed link after these nodes have blocked the port facing the failed link. On obtaining this message, RPL owner unblocks the RPL port.

Introduction:

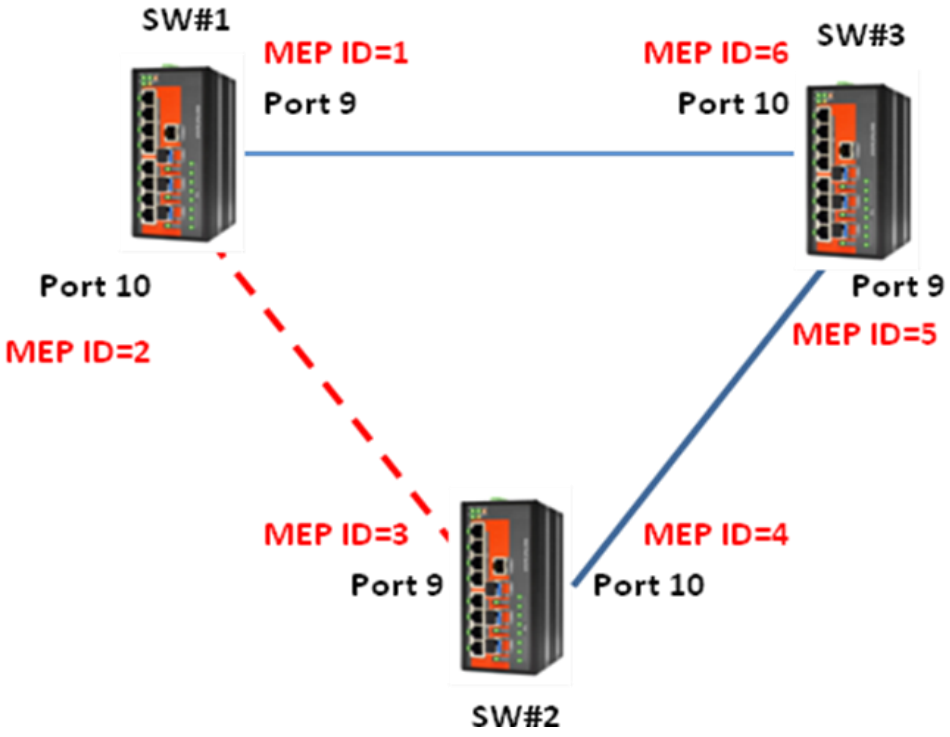
The purpose of this document is to give valuable aid to a network engineer in topology design, deployment and configuration of Industrial Grade Ethernet Switches for ring protection with sub-50ms recovery time. The example uses a ring of three units and performs all configurations via the web GUI management interface.

Equipment Used in this Example:

1. The Industrial Grade Ethernet Switches with G.8032 function * 3
2. Laptop * 1



Testing Topology:



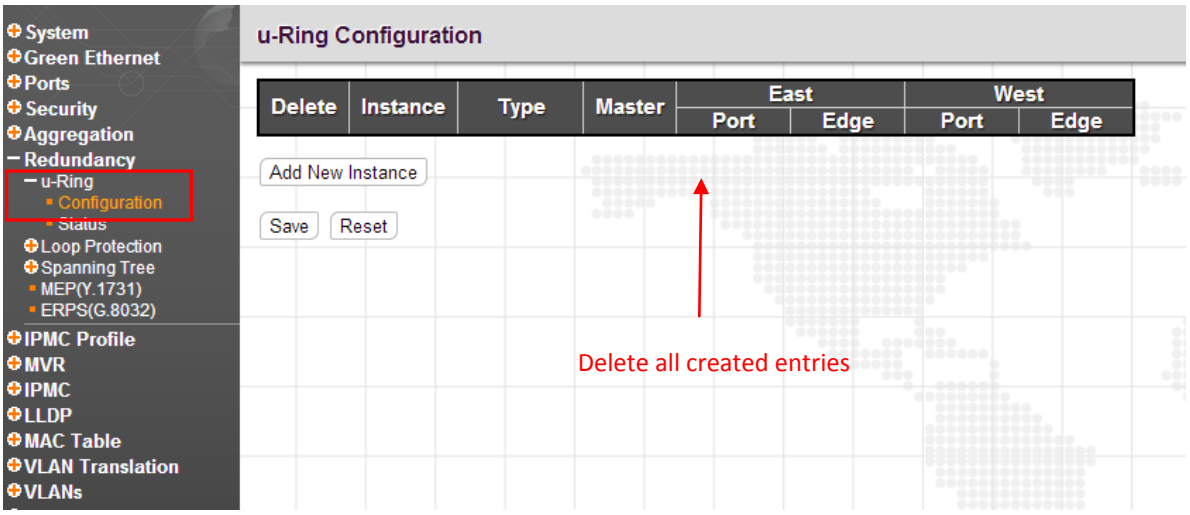
<Figure 1>

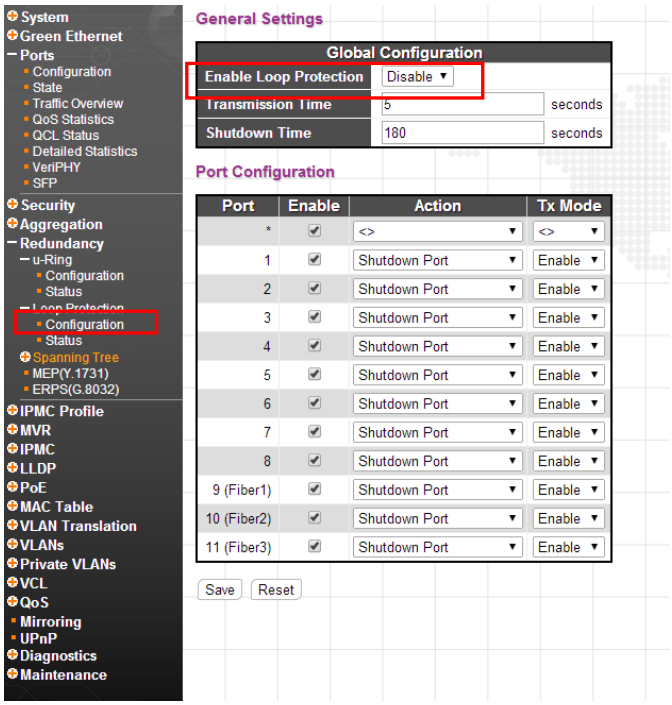
Warning:

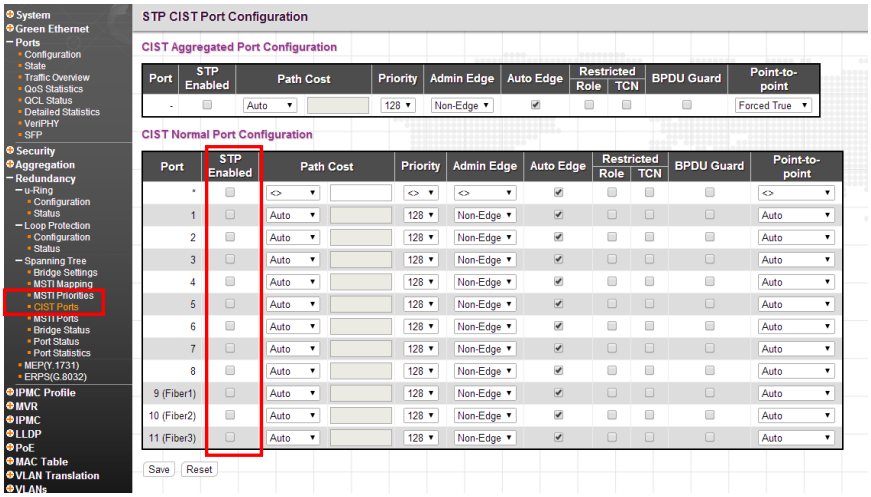
1. ***Please design your network topology and physical links first. Since G.8032 syncs with neighbor switch's MAC address (Peer to peer), it is important to make sure your physical connections are in correct locations and that they are not arbitrarily changed.***
2. ***During initial configuration and in order to avoid an Ethernet "Loop" condition, please do not connect the physical Ring prior to completion of the G.8032 configuration.***

Configuration of SW#1:

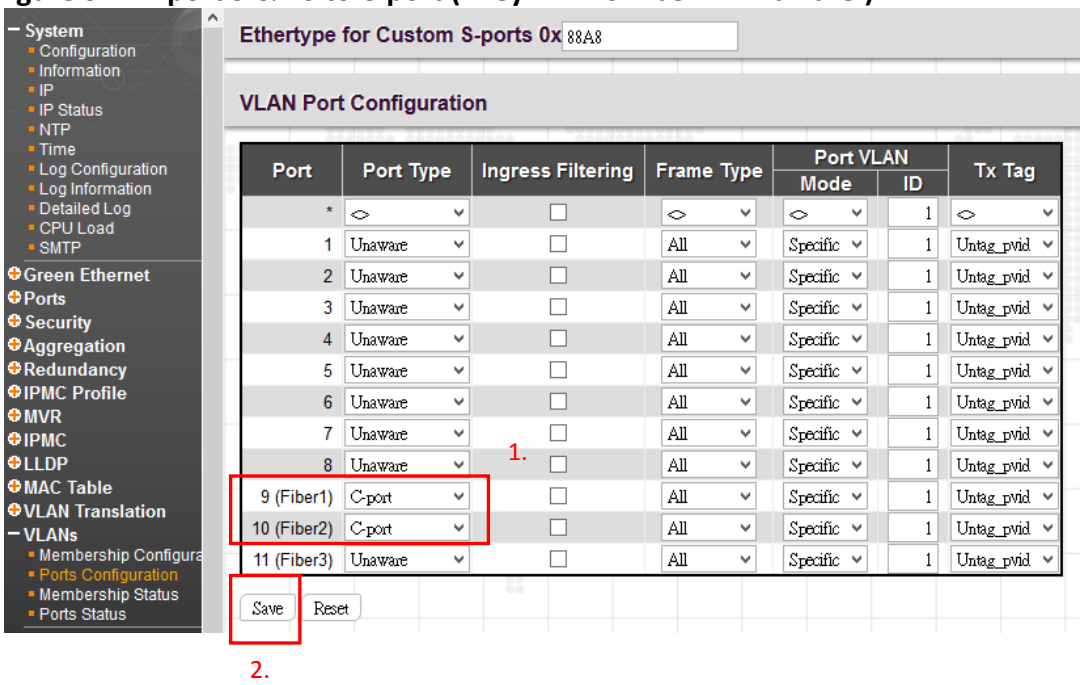
A. Make sure SW#1's u-Ring, Loop Protection and STP configurations are all disabled.





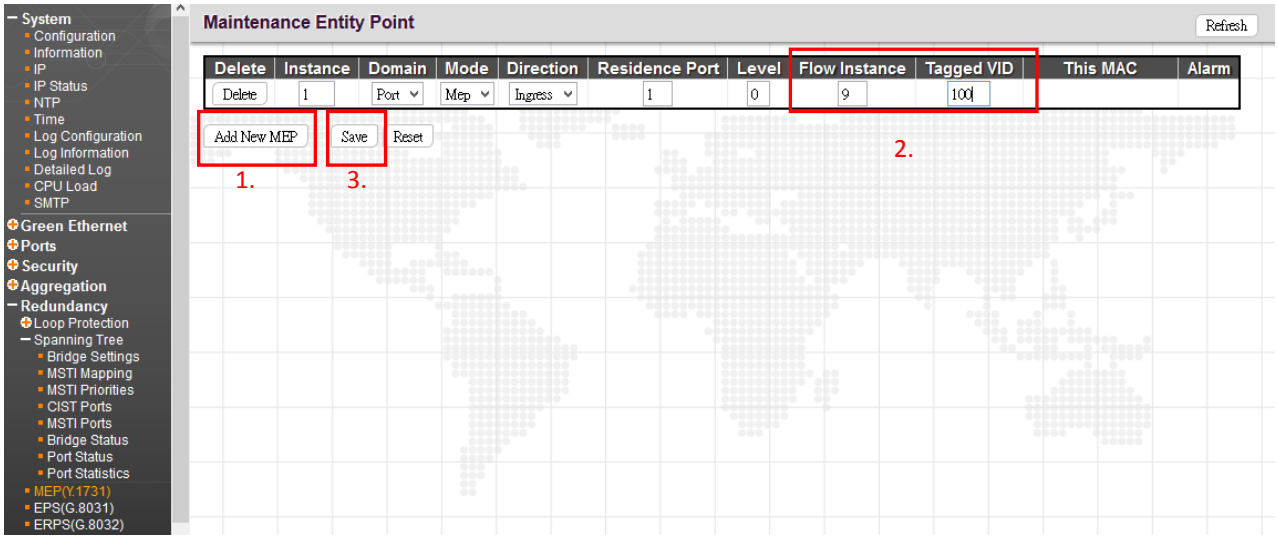


B. Configure SW#1 port 9 & 10 to C-port (They will now be VLAN aware.)

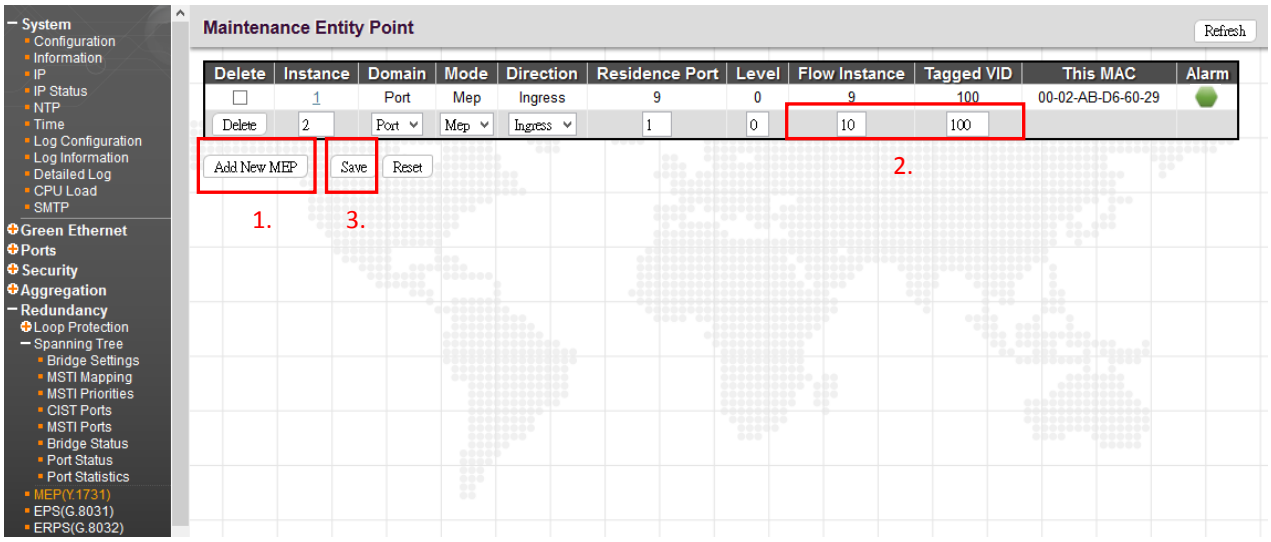


1. Pull-down and select C-port ("C" for customer tag, inner tag or 802.1Q tag)
2. Click "Save".

C. Configure MEP (Maintenance associated End Point) on SW#1



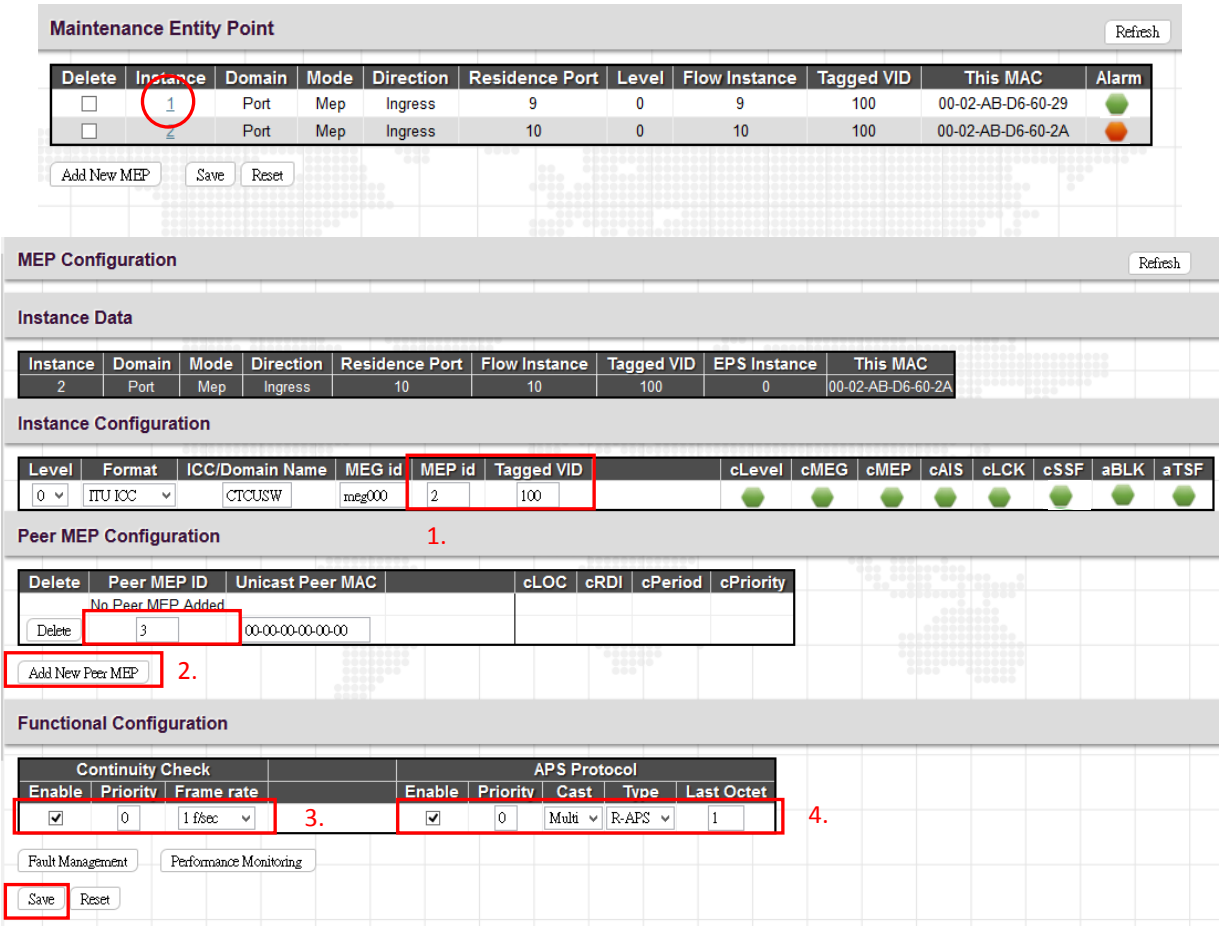
1. Click "Add New MEP"
2. Enter port 9 (Fiber 1) into "Flow Instance" and set VID (user defined, we will use 100 here and throughout)
3. Click "Save"



1. Click "Add New MEP"
2. Enter port 10 (Fiber 2) into "Flow Instance" and set VID (user defined, 100 here)
3. Click "Save"

NOTE: *All switches must use the same VID.*

D. Click "Instance 1 " to configure detailed setting of MEP

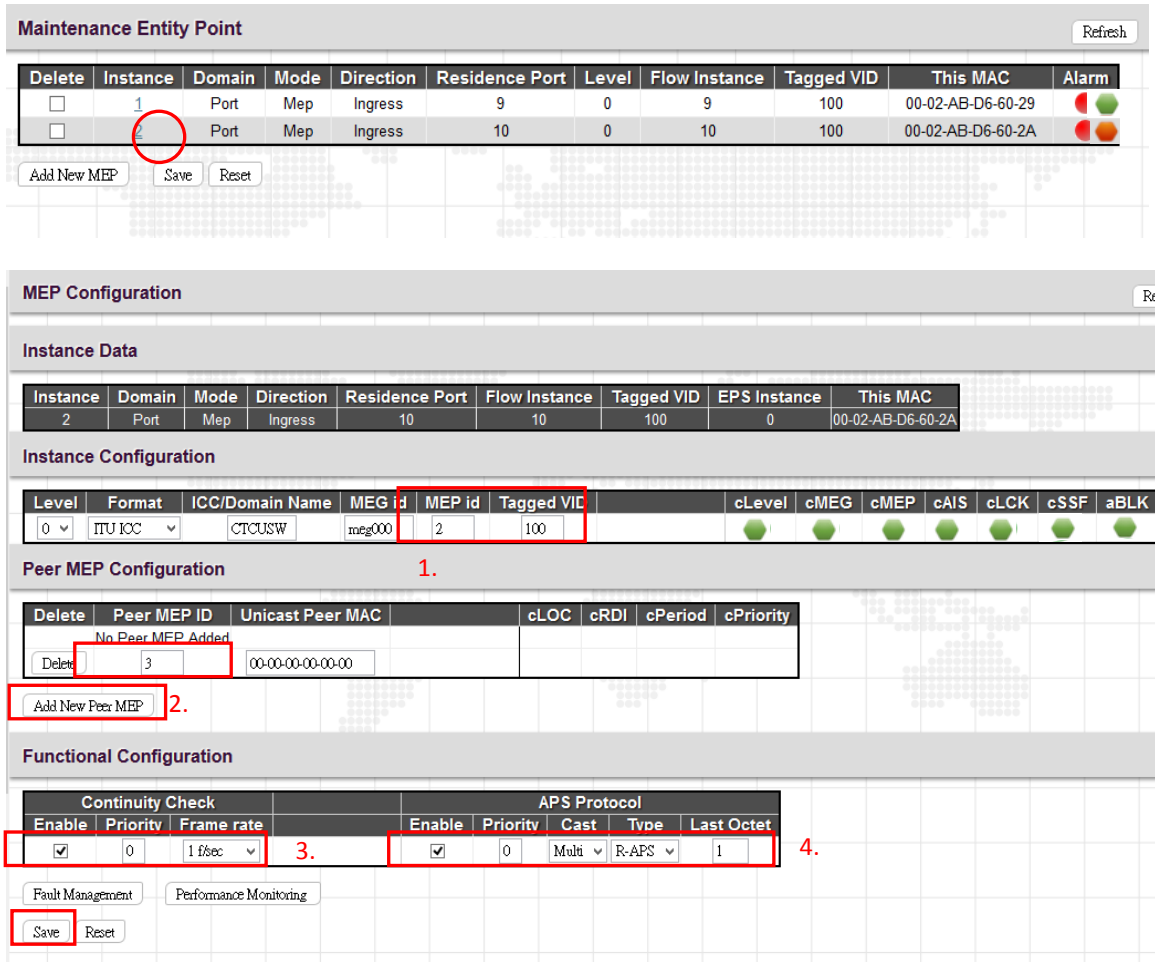


1. Set the first MEP ID to "1" and make sure Tagged VID matches our set VID (100 here)
2. Click "Add New Peer MEP" and enter the peer's ID which is "6" in our topology example
3. Enable Continuity Check and leave "Frame rate" at 1 f/sec
4. Enable the APS Protocol, with "Multicasting" and type "R-APS"
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>.

E. Click “Instance 2 “ to configure further setting of MEP for port 10



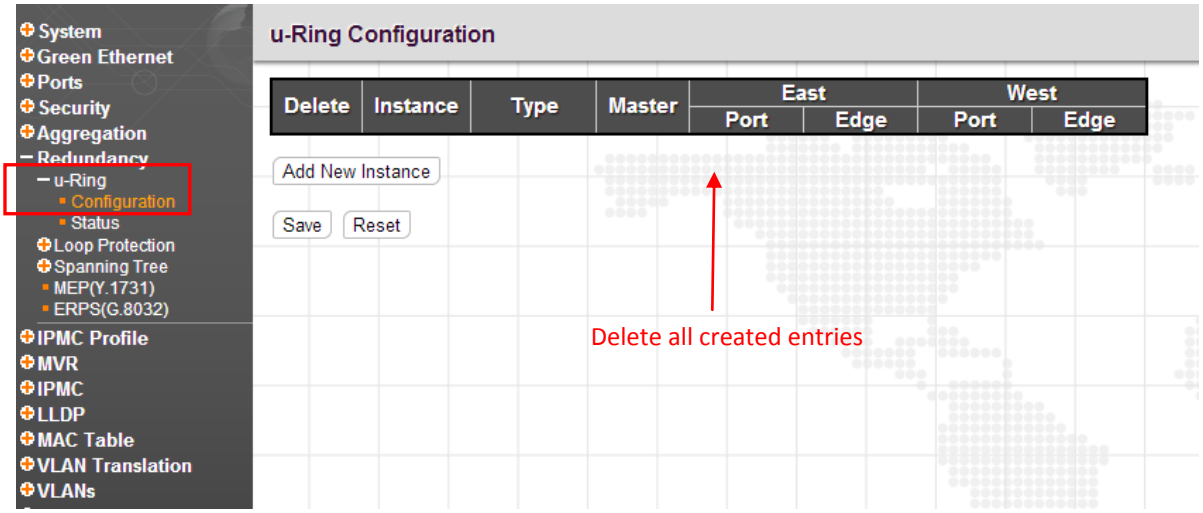
1. Set the second port MEP ID to "2" and make sure Tagged VID matches our set VID (100 here)
2. Click "Add New Peer MEP" and enter the peer's ID which is "3" in our topology example
3. Enable Continuity Check and leave "Frame rate" at 1 f/sec
4. Enable the APS Protocol, with "Multicasting" and type "R-APS"
5. Click "Save"

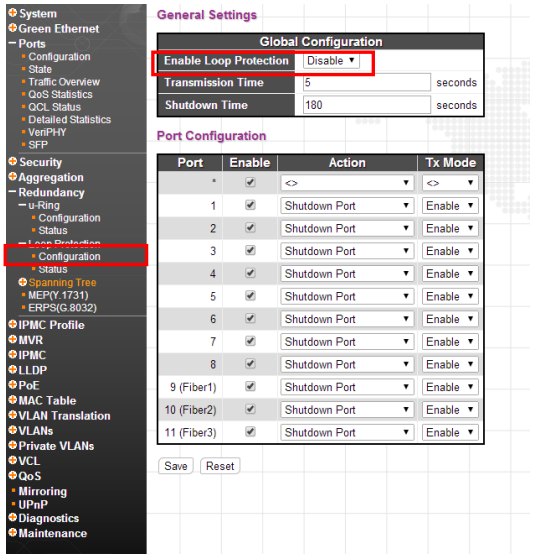
NOTE:

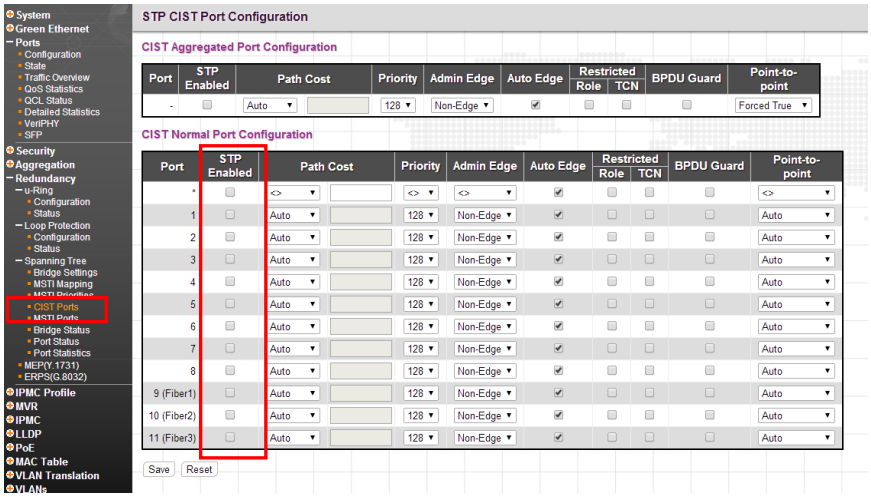
The MEP ID (2) here is for Port 10 of SW#1
And Peer MEP ID (3) is the neighbor port 9 of SW#2.
Always refer back to your design topology as in < Figure 1>.

Configuration of SW#2

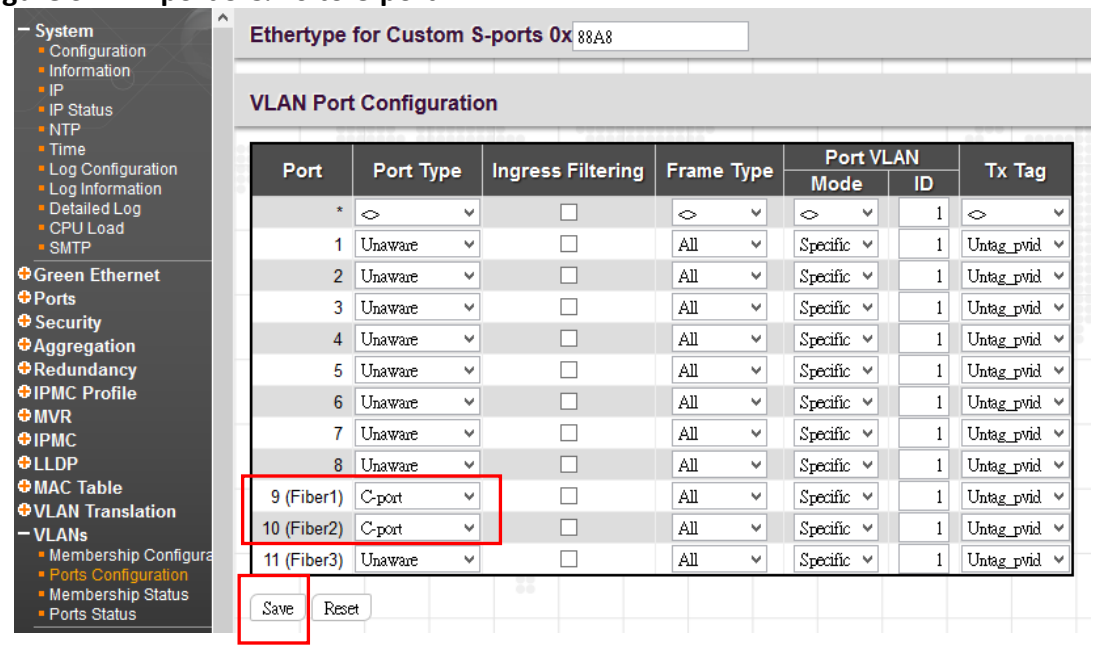
A. Use the same configuration process as SW#1, make sure SW#2's u-Ring, Loop Protection and STP configurations are all disabled.



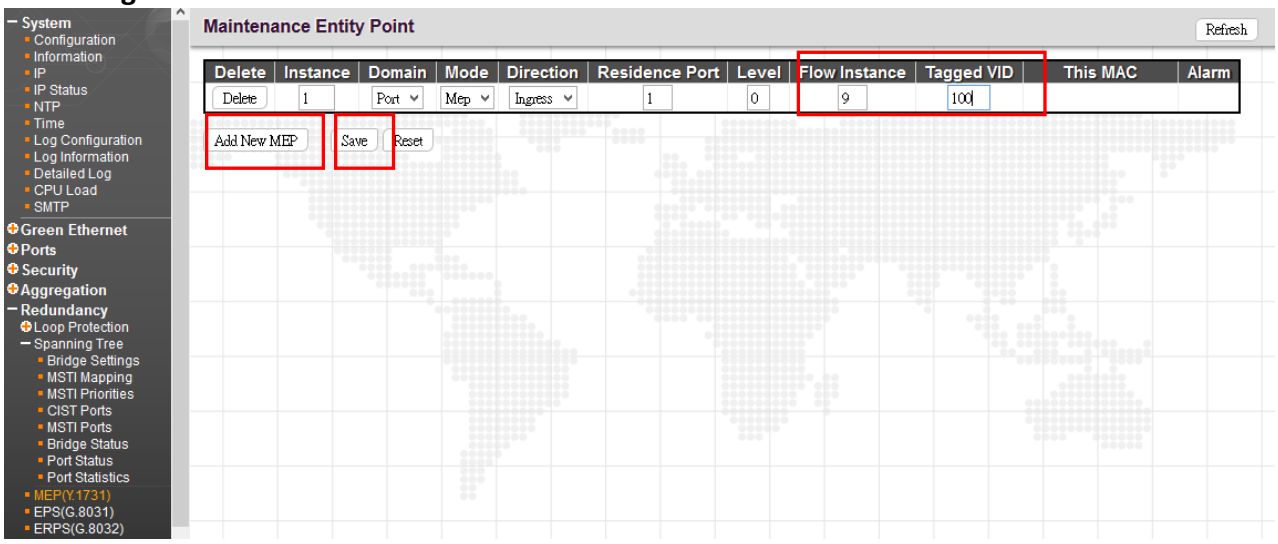


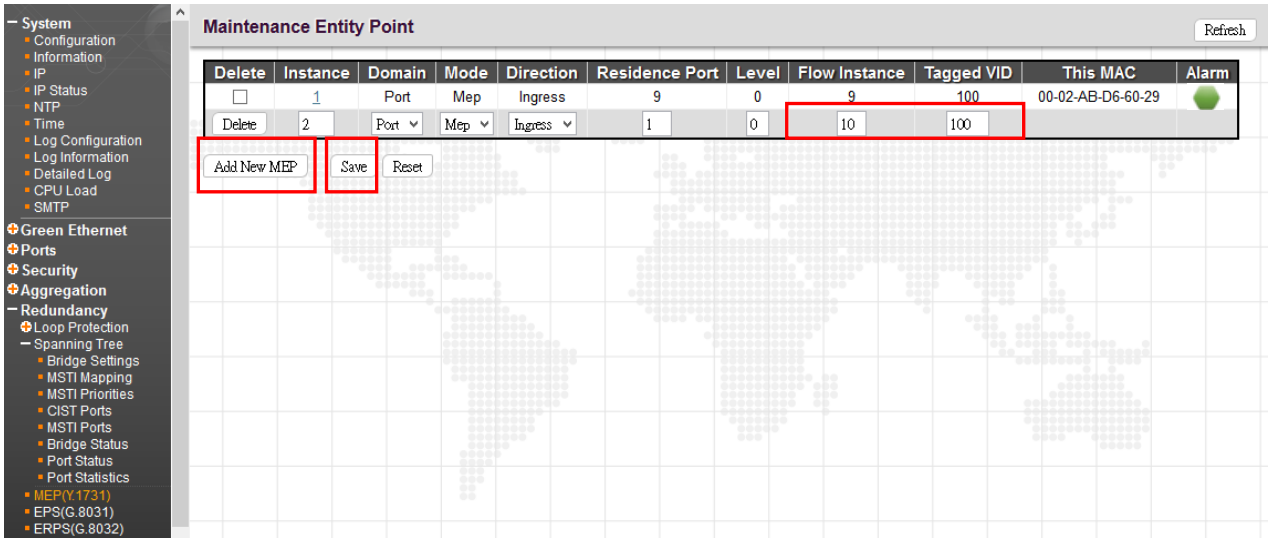


B. Configure SW#2 port 9 & 10 to C-port

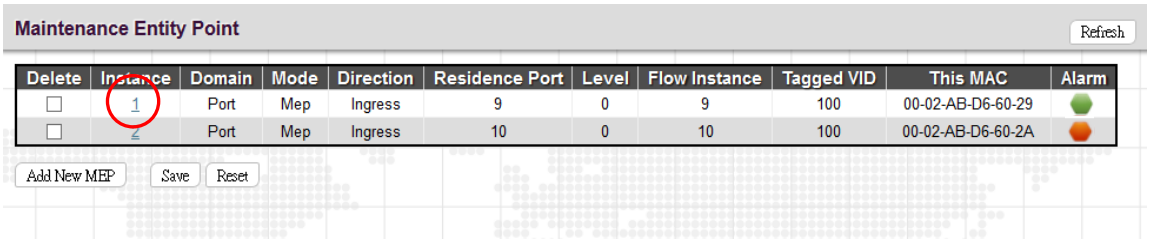


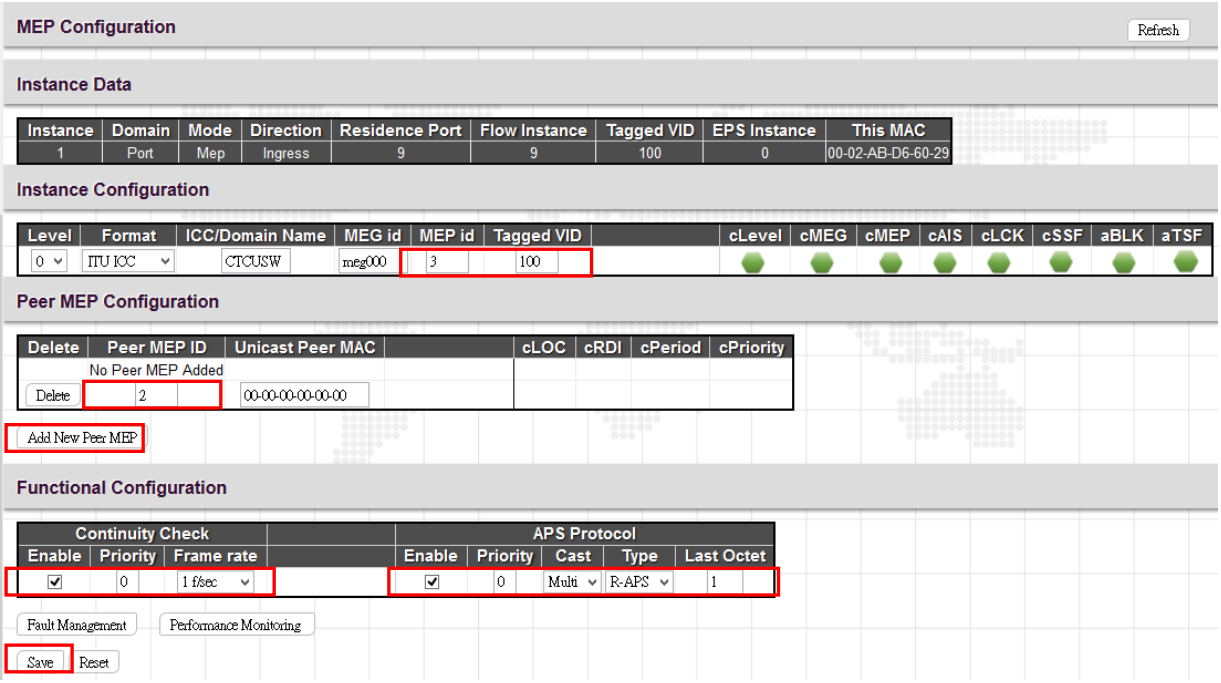
C. Configure MEP on SW#2





D. Click “Instance 1 “ to configure further setting of MEP

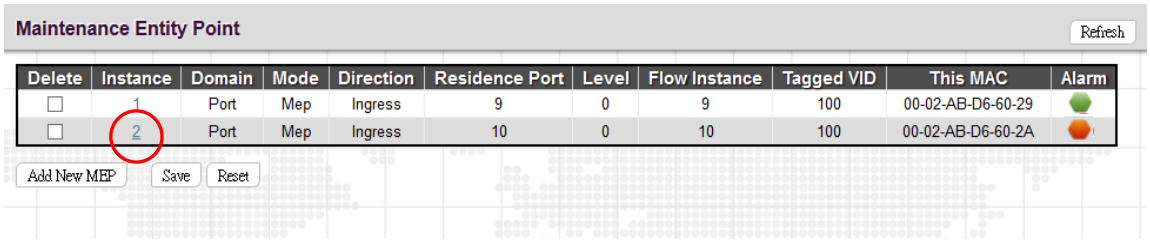


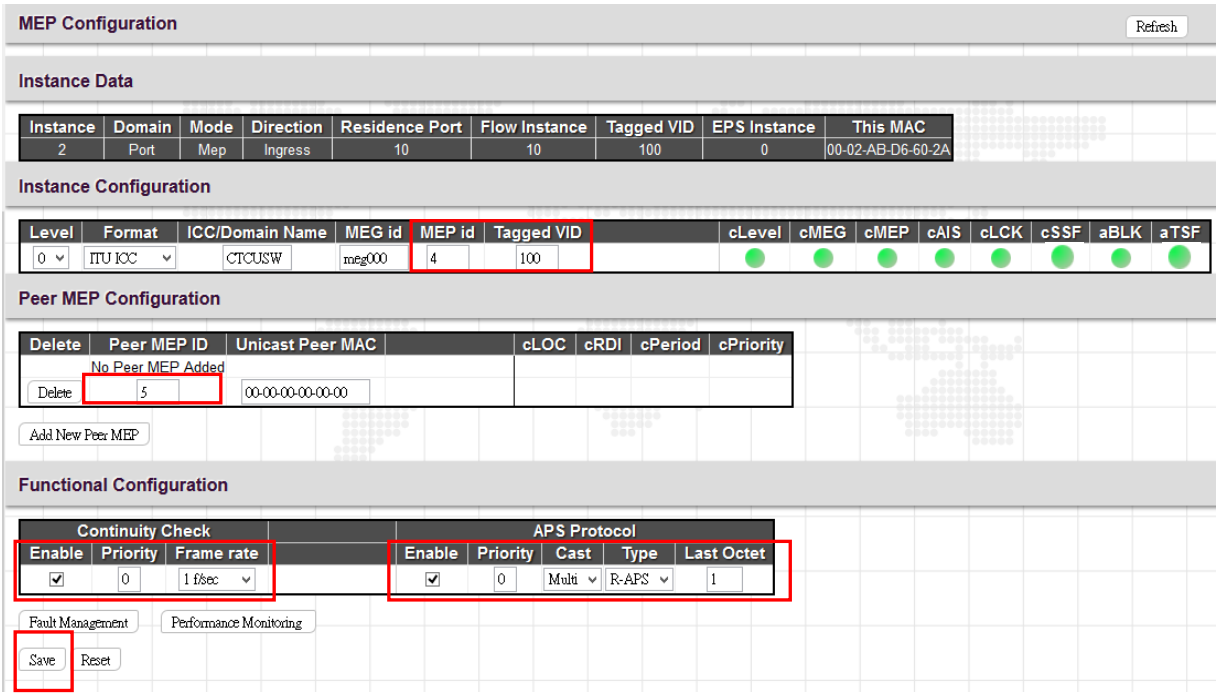


NOTE:

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>.

E. Click "Instance 2 " to configure further setting of MEP



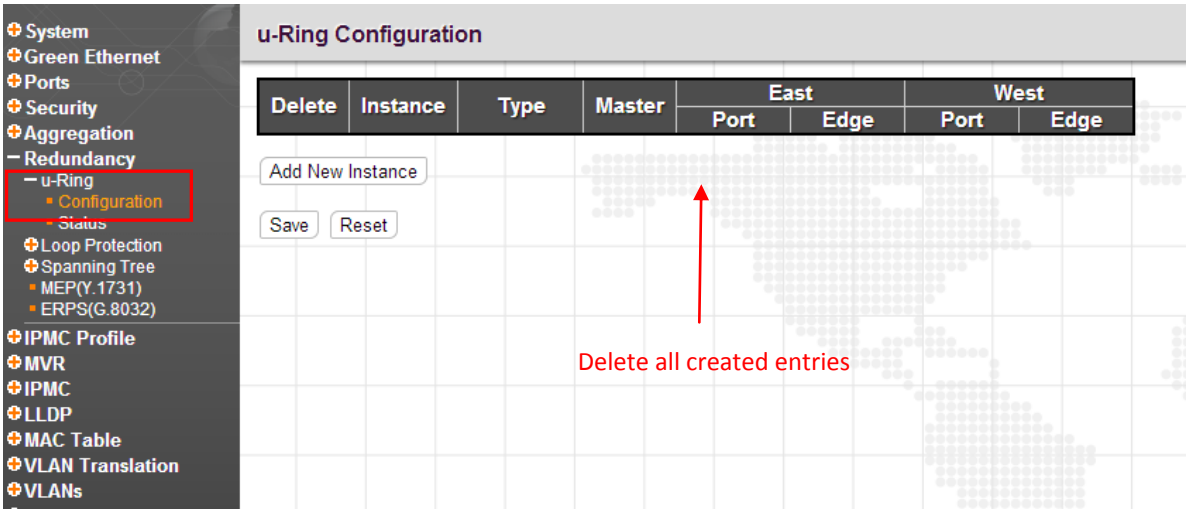


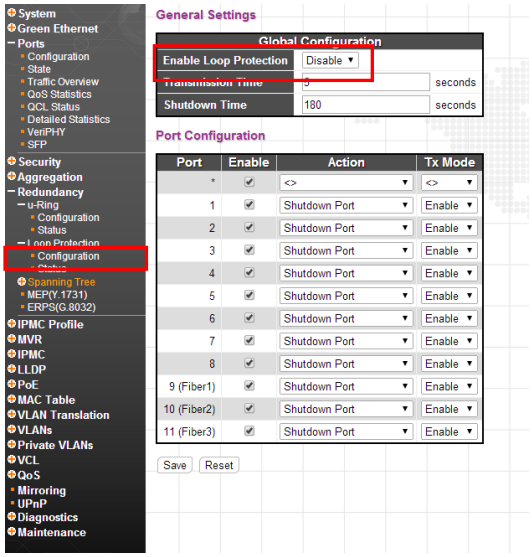
NOTE:

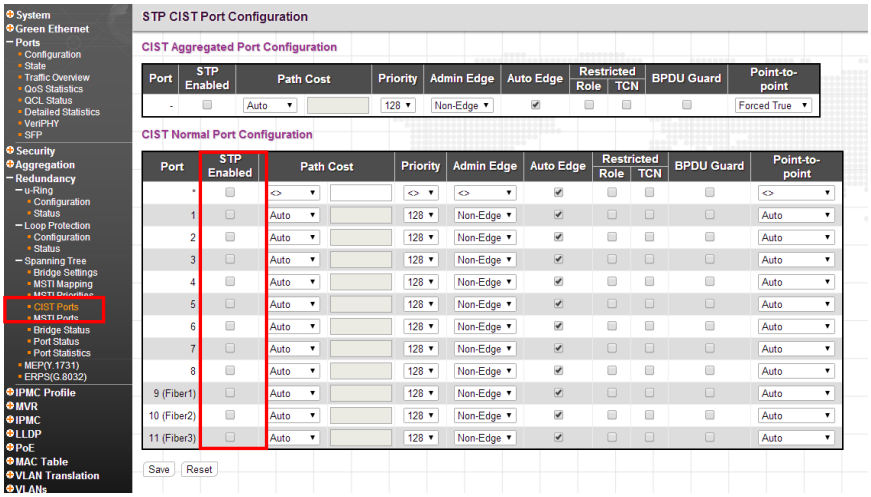
The MEP ID (4) here is for Port 10 of SW#2
And Peer MEP ID (5) is the neighbor port 9 of SW#3.
Always refer back to your design topology as in < Figure 1>.

Configuration of SW#3

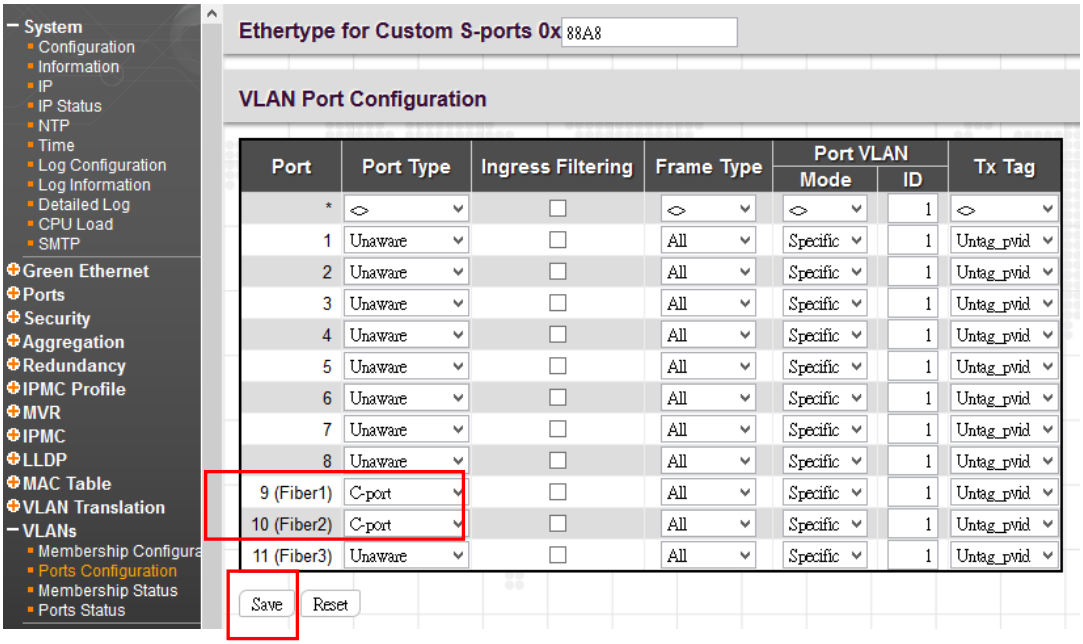
A. Same configuration process as SW#1 & SW#2, make sure SW#3's u-Ring, Loop Protection and STP configurations are all disabled.



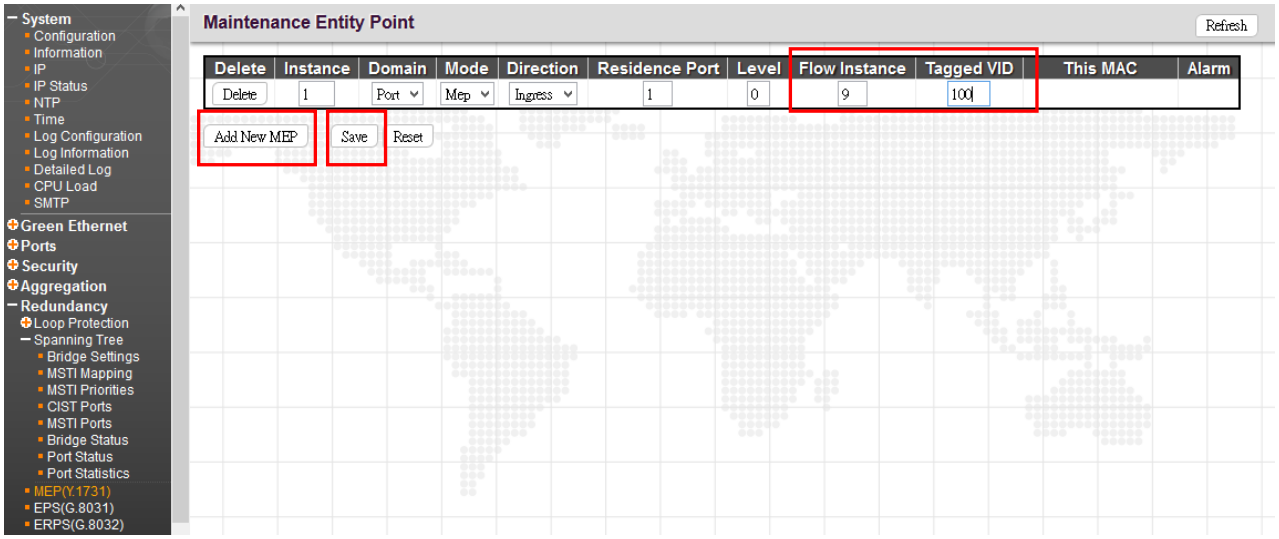


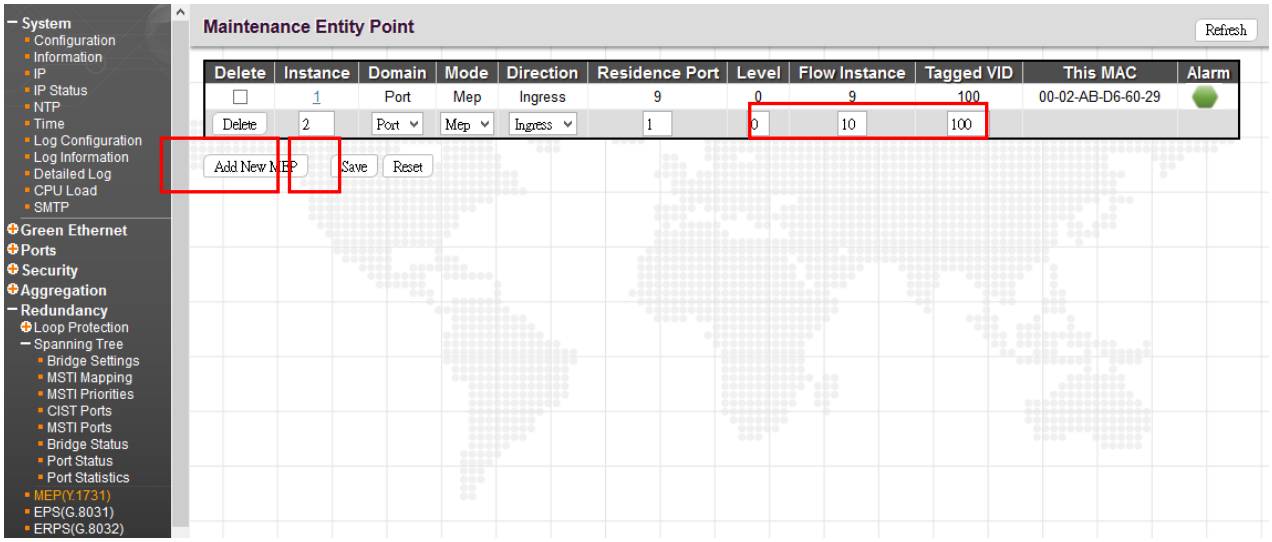


B. Configure SW#3 port 9 & 10 to C-port

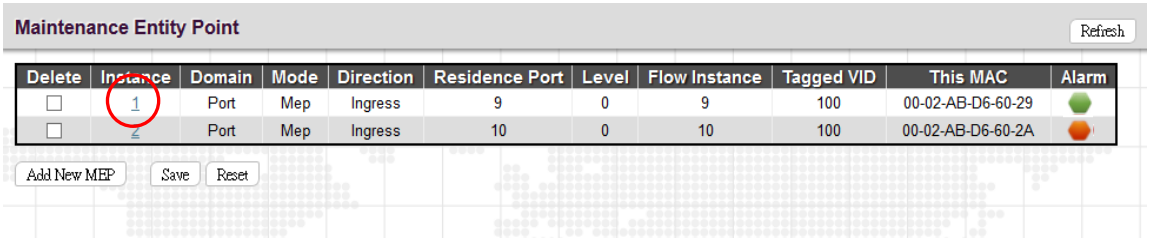


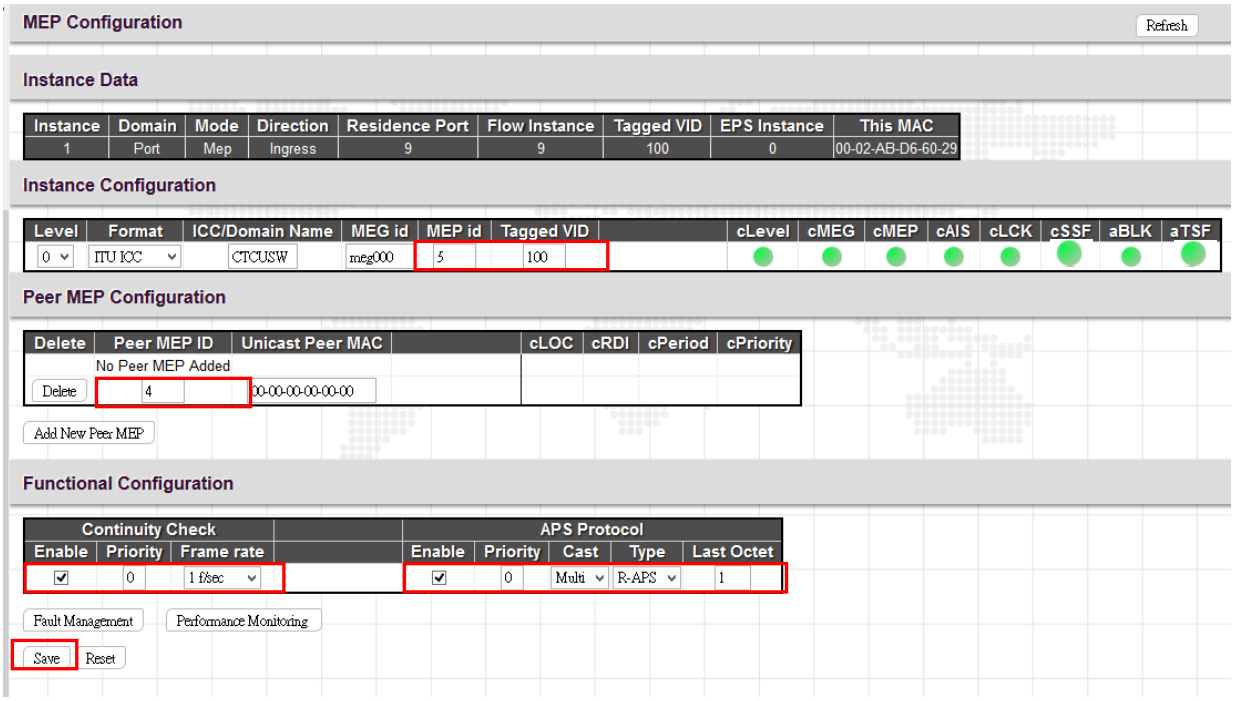
C. Configure MEP on SW#3





D. Click “Instance 1 “ to configure further setting of MEP

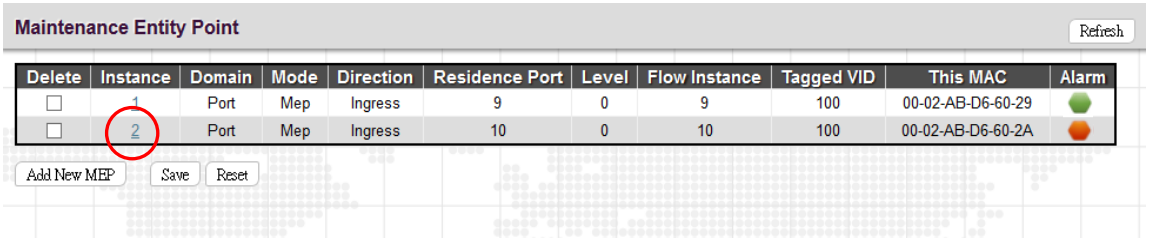


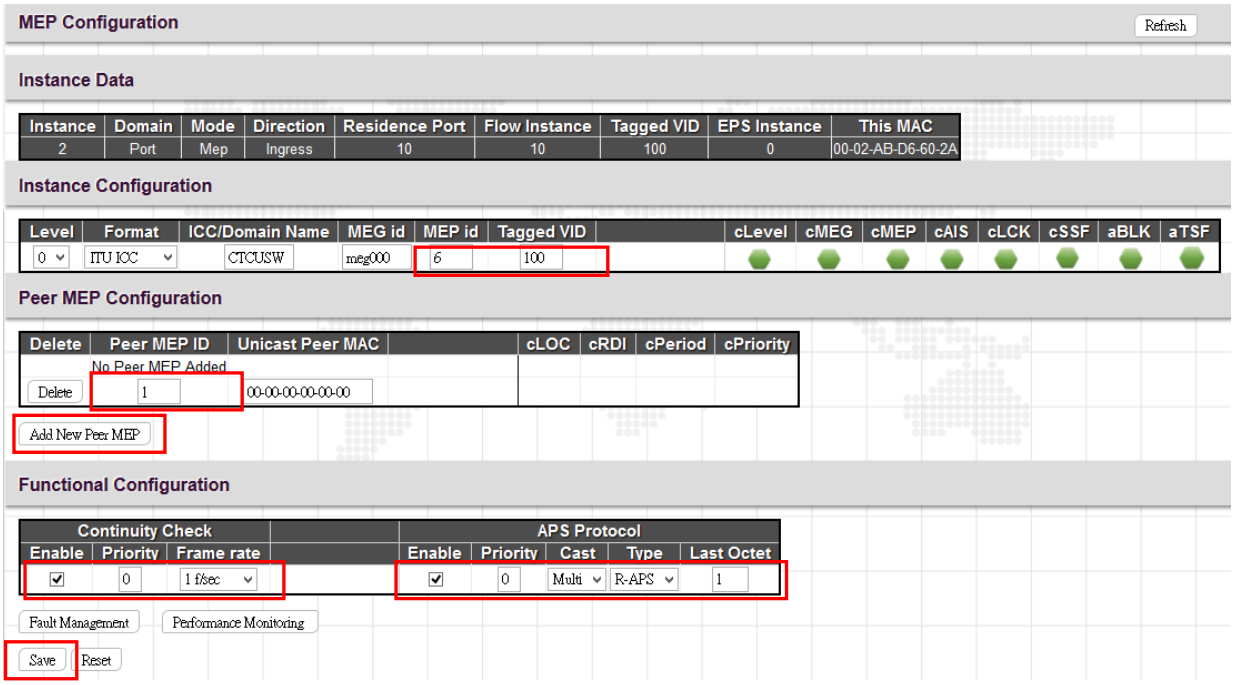


NOTE:

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>.

E. Click "Instance 2 " to configure further setting of MEP

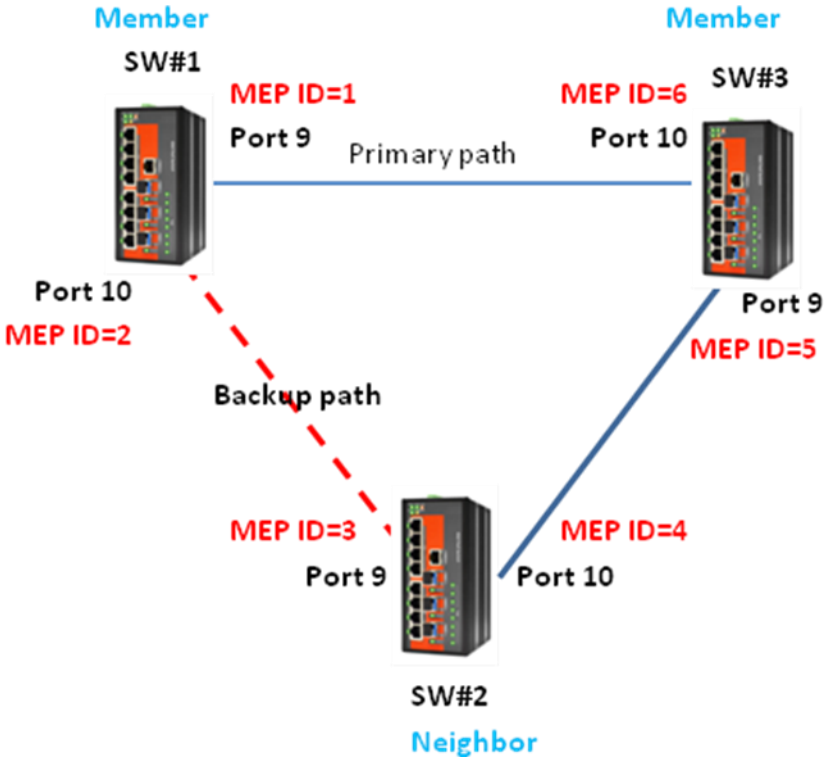




NOTE:

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>.

ERPS configuration

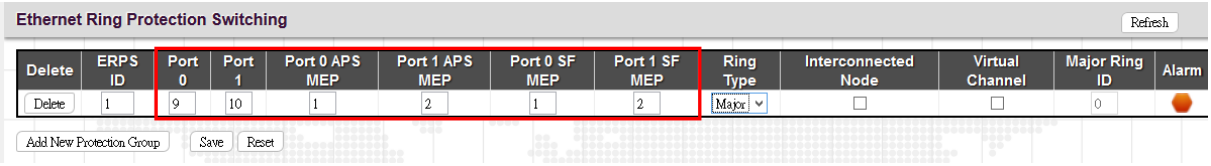


We need to assign one switch as Master, one as Neighbor, and all others as Member switches. The function of Master switch is to decide which path is active (unblocked) and which one is backup path (blocked). Neighbor switch is connecting to Master switch directly by backup path (or standby path).

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

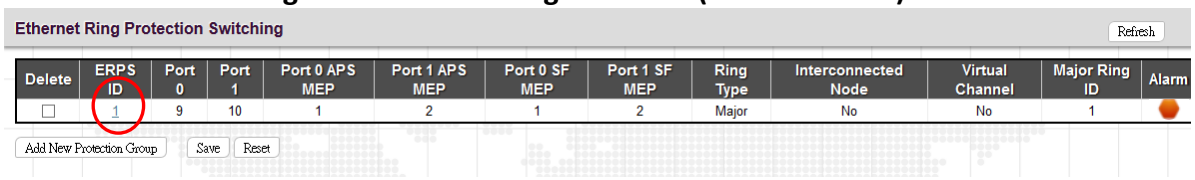


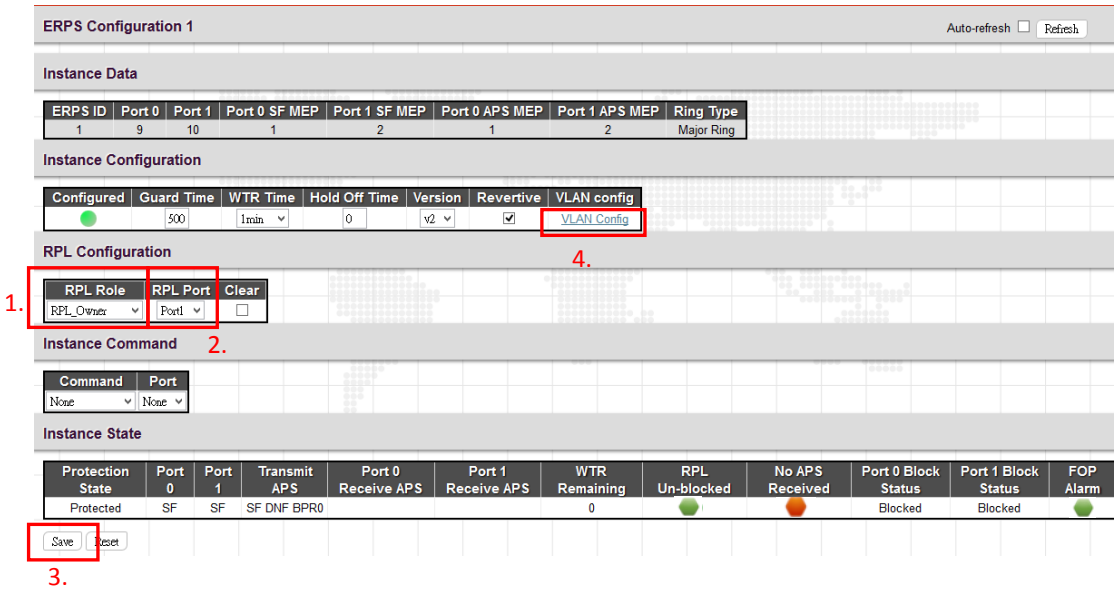
1. From ERPS Click "Add New Protection Group" and follow the setting logic described below
2. Click "Save"

NOTE:

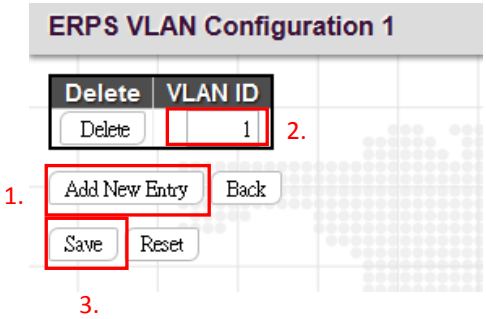
The Port 0 and 1 send the CCM (Continuity Check Message) packets of Y.1731 out from switch physical interfaces. We use Port 9 and 10 for the ERPS example here.
"Port 0 APS MEP" "Port 1 APS MEP" "Port 0 SF MEP" Port 1 SF MEP" columns will follow the MEP ID we assigned for Port 9 & 10 earlier, so interface 9 = port 0 = 1 , interface 10 = port 1= 2.

B. Click ERPS ID to configure advance setting of ERPS – (Master switch)





1. For Master switch, please make 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"

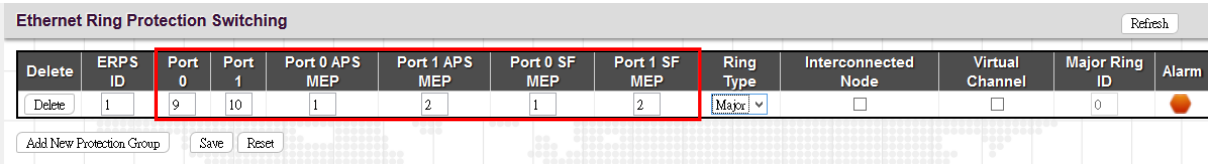
NOTE: RPL Role

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

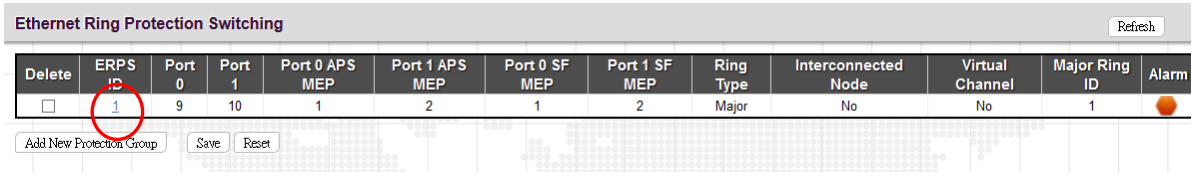
ERPS configuration of SW#2 (Neighbor switch)

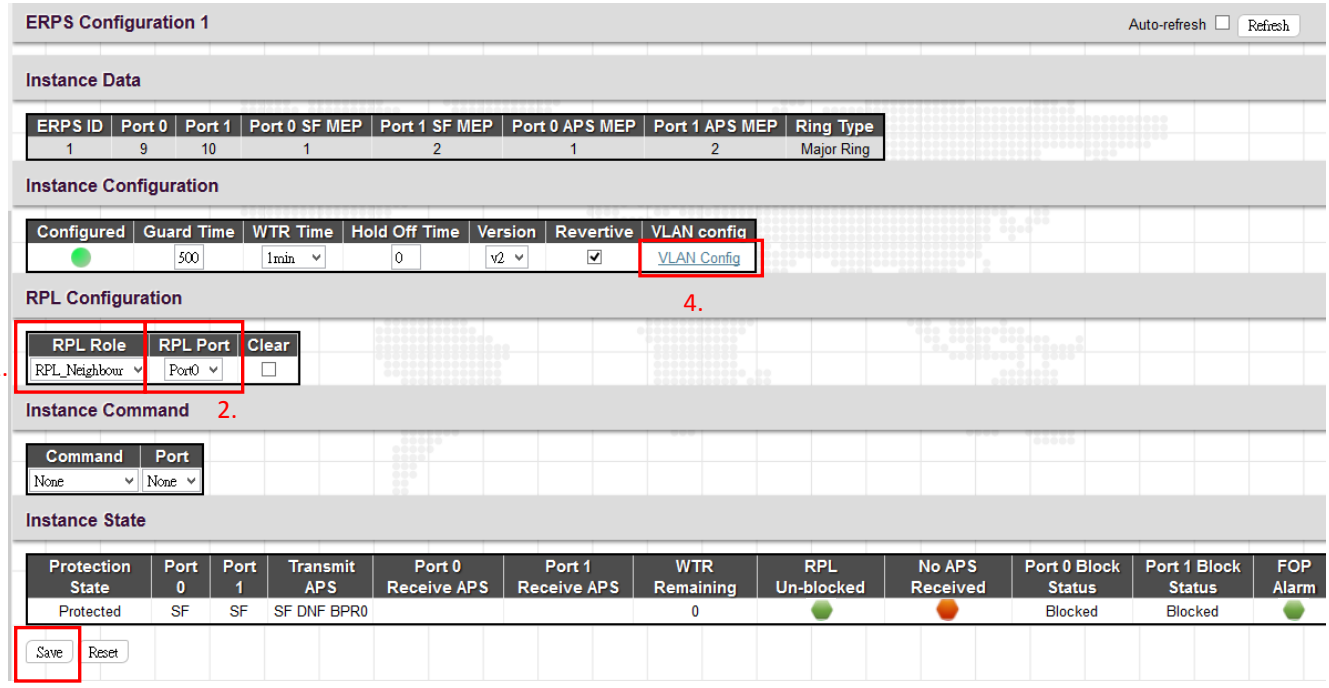
A. Create 1 ERPS protection Group



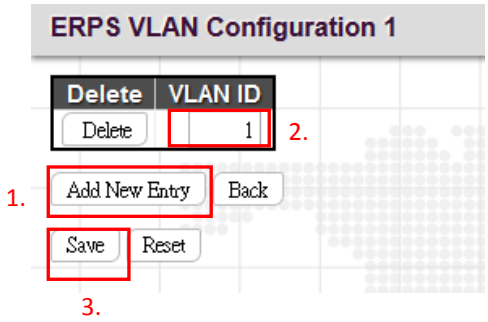
1. Click "Add New Protection Group", configure Ports, APS and SF
2. Click "Save"

B. Click ERPS ID to configure advance setting of ERPS – (Neighbor switch)





1. For Neighbor switch, please make RPL role "RPL_Neighbour"
2. Set the "RPL Port" to Port0
3. Click "Save"
4. Click "VLAN Config" and follow the settings below

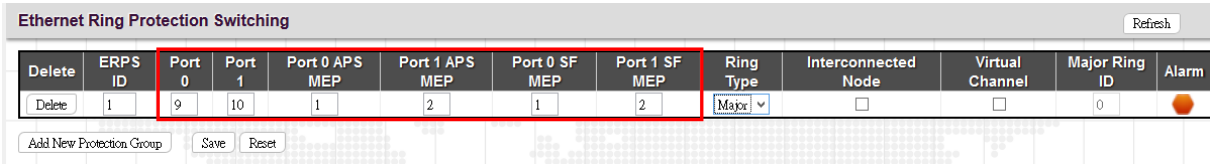


1. Click "Add New Entry"
2. Set VLAN ID to "1"
3. Click "Save"

NOTE: *RPL Port = Port 0 (Interface 9 of SW#2)*

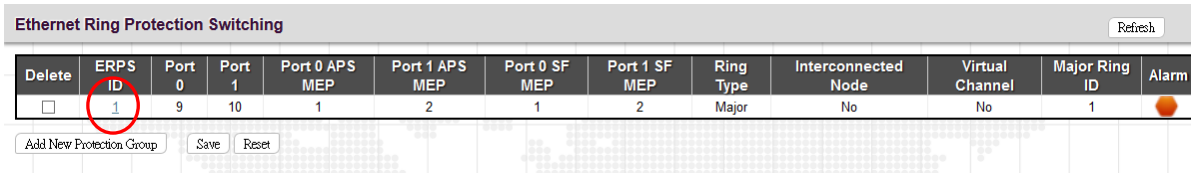
ERPS configuration of SW#3 (Member switch)

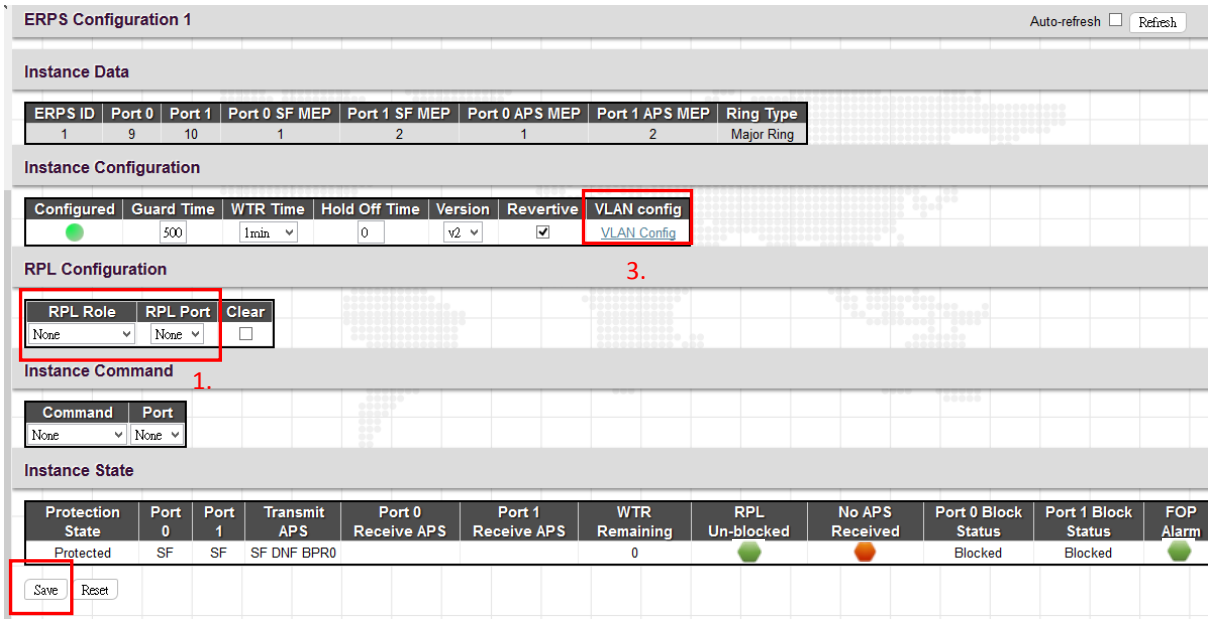
A. Create 1 ERPS protection Group



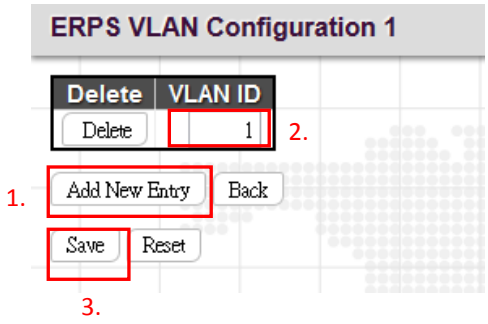
1. Click "Add New Protection Group", configure Ports, APS and SF
2. Click "Save"

B. Click ERPS ID to configure advance setting of ERPS – (Member switch)





1. For Member switches, please make sure RPL role and port are "None"
2. Click "Save"
3. Click "VLAN Config"

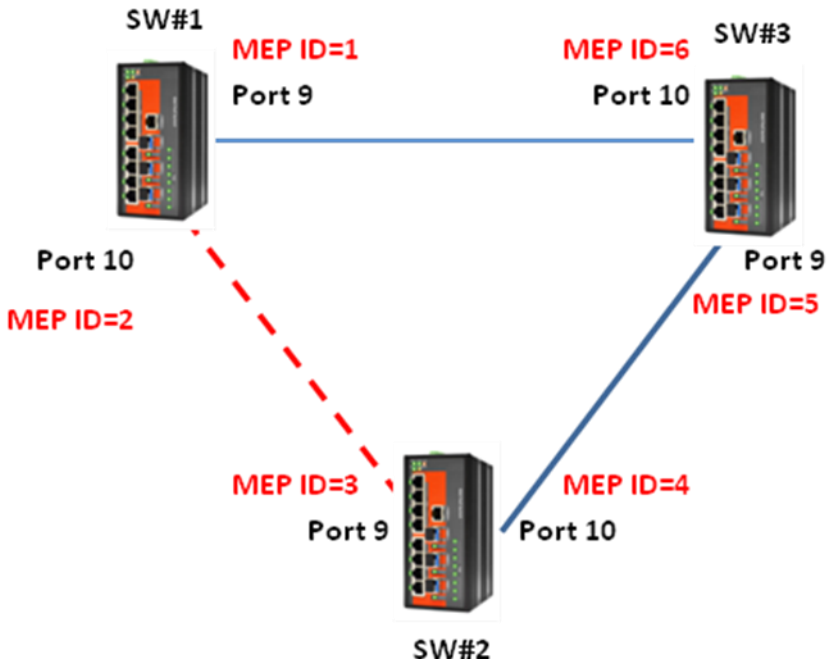


1. Click "Add New Entry"
2. Set VLAN ID to "1"
3. Click "Save"

NOTE: *RPL Role => None = Member switch.*

Verification and Testing

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	Ingress	9	0	9	100	00-02-AB-D6-60-09	
☐	2	Port	Mep	Ingress	10	0	10	100	00-02-AB-D6-60-0A	

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	Ingress	9	0	9	100	00-02-AB-D6-68-B9	
☐	2	Port	Mep	Ingress	10	0	10	100	00-02-AB-D6-68-BA	

Add New MEP | Save | Reset

<SW#3>

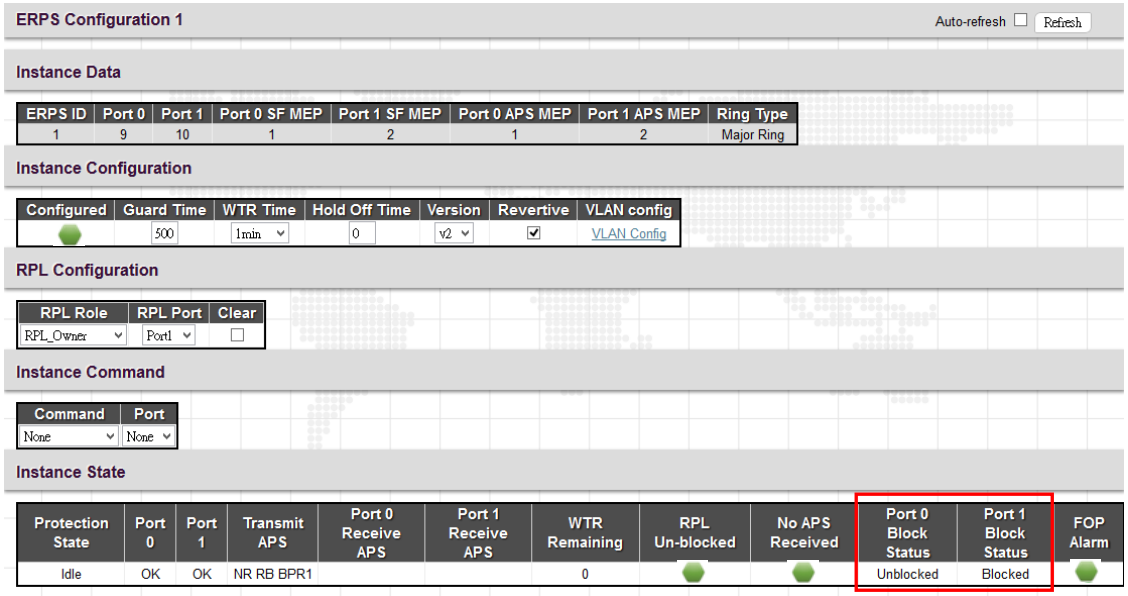
Maintenance Entity Point

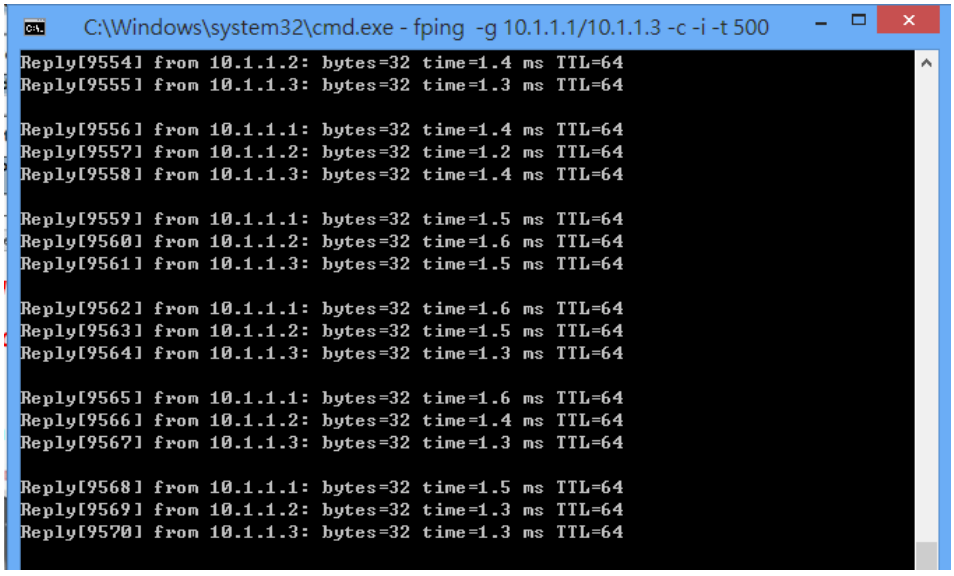
Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
☐	1	Port	Mep	Ingress	9	0	9	100	00-02-AB-D6-60-79	
☐	2	Port	Mep	Ingress	10	0	10	100	00-02-AB-D6-60-7A	

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.

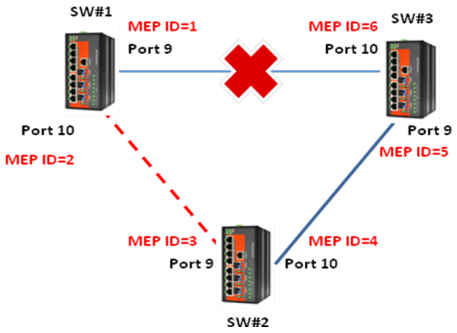


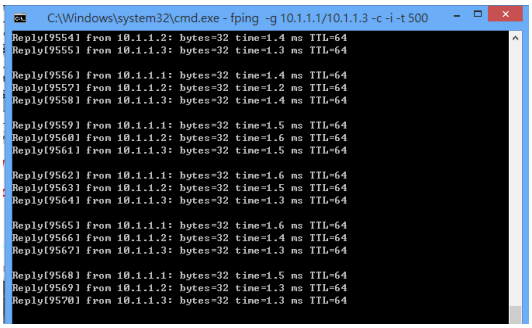


NOTE:

In normal status, Port 0 (Interface 9) is primary path (Unblock)
Port 1 (Interface 10) is standby path, so it is blocked.

Disconnect path between SW#1 and SW#3, like in the below figure. The standby path should now be active and still can ping all switches.





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	☐

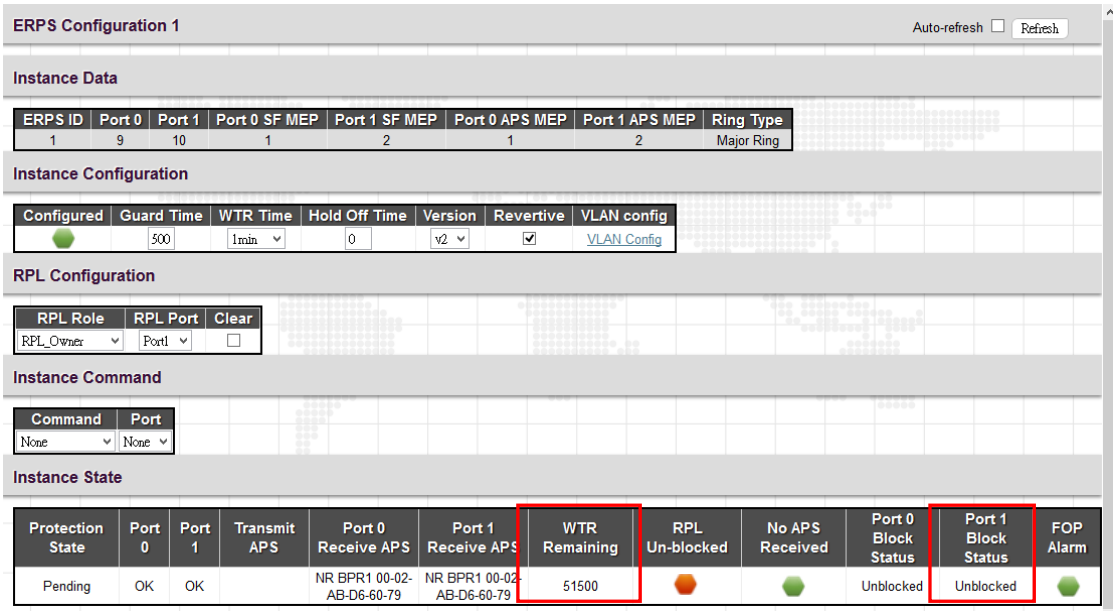
Instance Command

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-D6-60-79	0			Blocked	Unblocked	

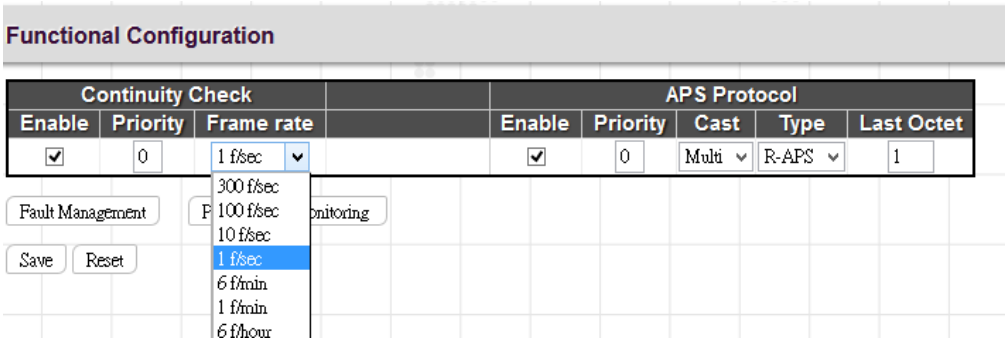
NOTE: *When you put the primary path back, the WTR Remaining will start to count down for 1 min before changing primary and standby paths back to normal status.*



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. VLAN BASIC CONFIGURATIONS

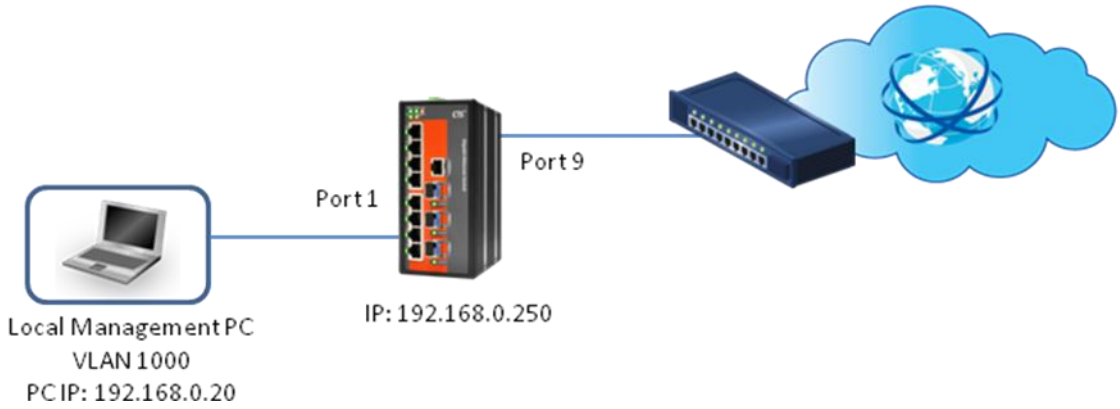
This Appendix will cover the following VLAN related configurations:

A. Management VLAN (Local management)
B. Management VLAN (Remote management)
C. 802.1Q VLAN
D. Q IN Q VLAN

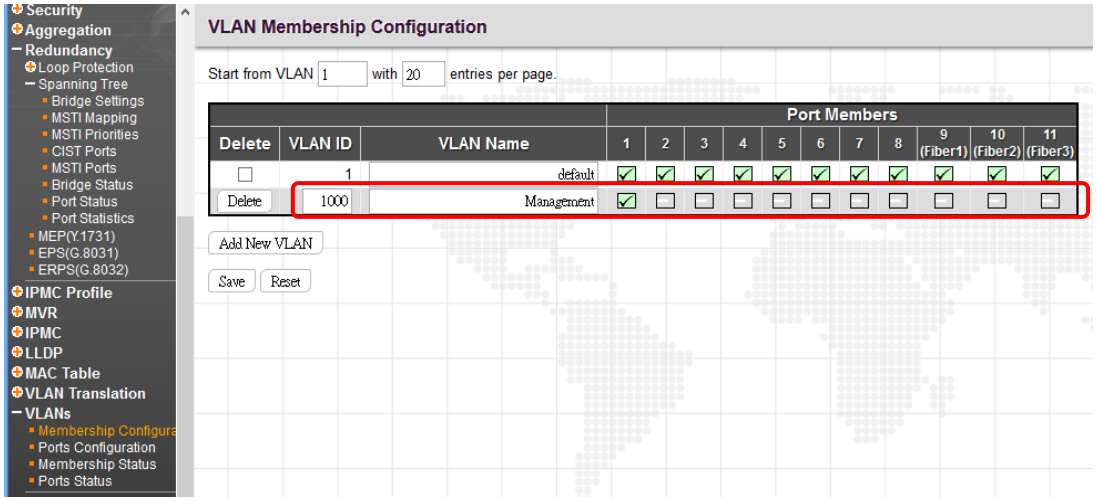
By default, the IP address is 10.0.0.1. For the first-time user, you can use the CONSOLE port to change the IP address via CLI to the desired one. Please refer to "Introduction to CLI" for more information on changing IP address of this device using the CONSOLE port.

VLAN configuration examples provided here are for easy and quick reference. The user can use their own IP address and VLAN requirements to set up their VLAN configurations. For detailed explanations of each VLAN options, please see VLAN section.

A. Local Management VLAN

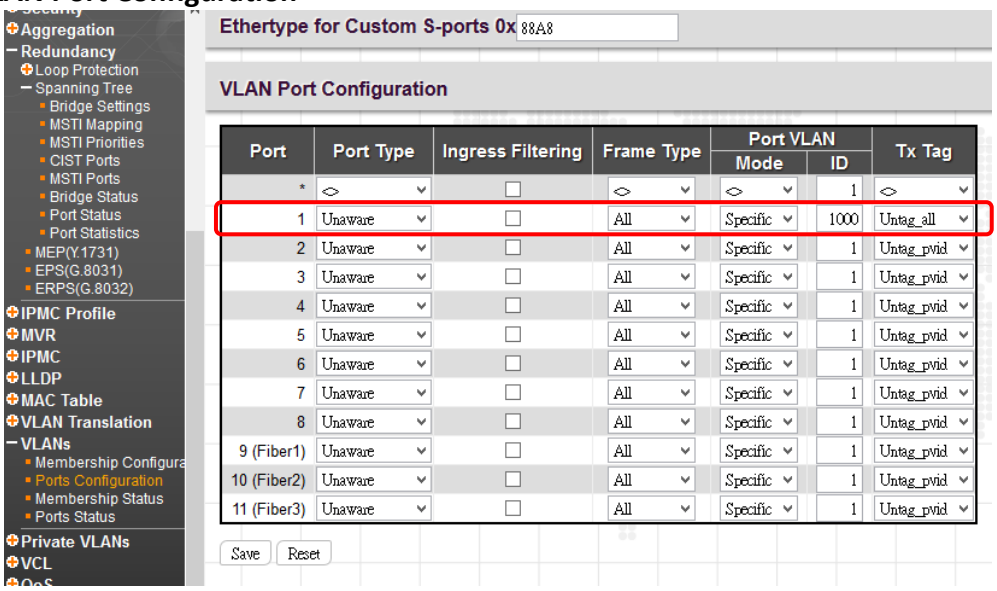


VLANs > VLAN Membership Configuration



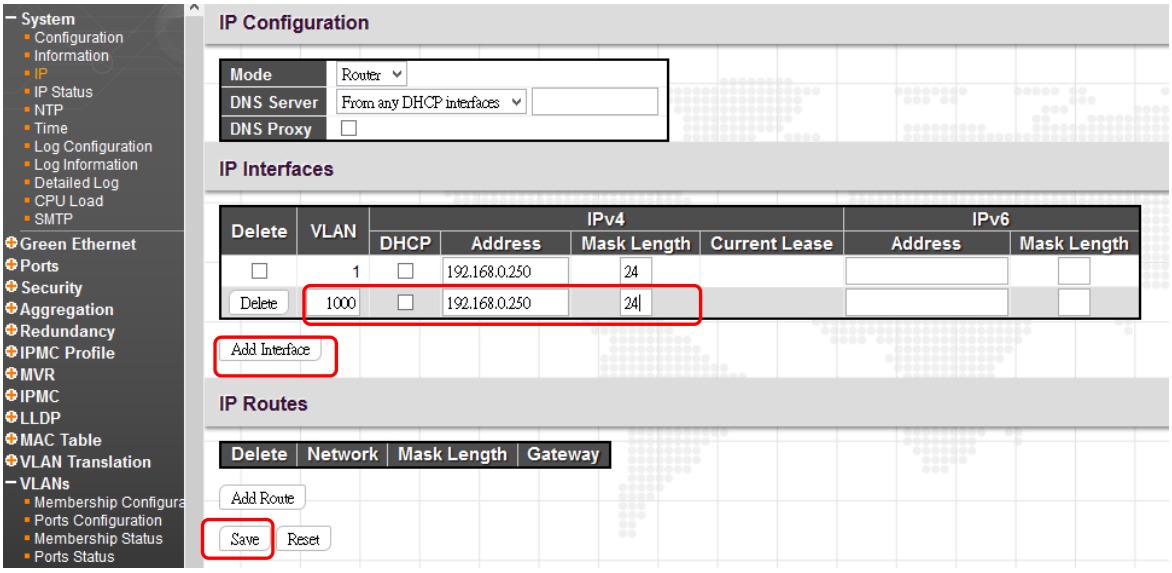
1. Connect your PC to a LAN port instead of the management port that you want to configure.
2. Click “Add New VLAN” button to insert a new entry.
3. Enter “1000” for VLAN ID, “Management” for VLAN Name and select port 1 as a port member.
4. Click “Save” button.

VLANs > VLAN Port Configuration



5. Set Port 1’s port type to “Unaware”, Frame Type to “All”, Port VLAN ID to “1000”, Tx Tag to “Untag All”.
6. Click “Save” button.

System > IP > IP Interfaces

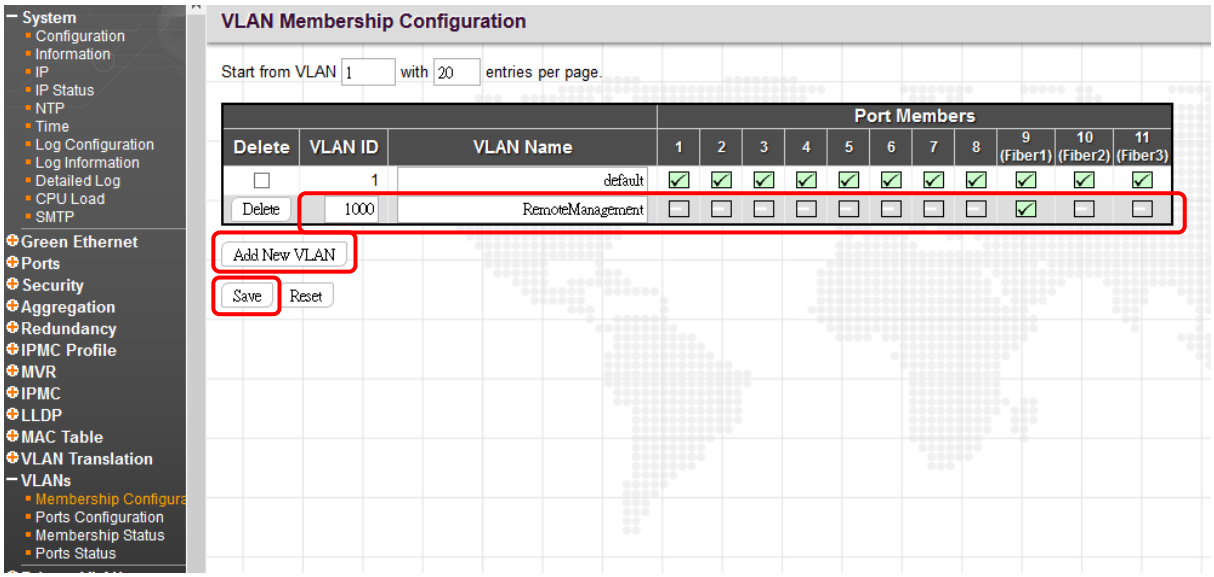


7. Click “Add Interface” button to insert a new entry.
8. Input management VLAN information. Set VLAN field to “1000” and IP address to “192.168.0.250”.
9. Click “Save” button to change management VLAN from 1 to 1000. Once you click “Save” button, your management PC is immediately disconnected from this device.
10. Connect your management PC to Port 1 (the management port) to access this device.
11. Delete VLAN 1 entry.

NOTE: *Make sure you have correct IP and VLAN settings before deleting the original management VLAN. Incorrect settings or cabling will disconnect you from this device. If you are unable to manage this device due to incorrect settings, use the CONSOLE port and CLI to reset the IP and VLAN settings to the defaults. Then, use the default IP address to reconfigure this device.*

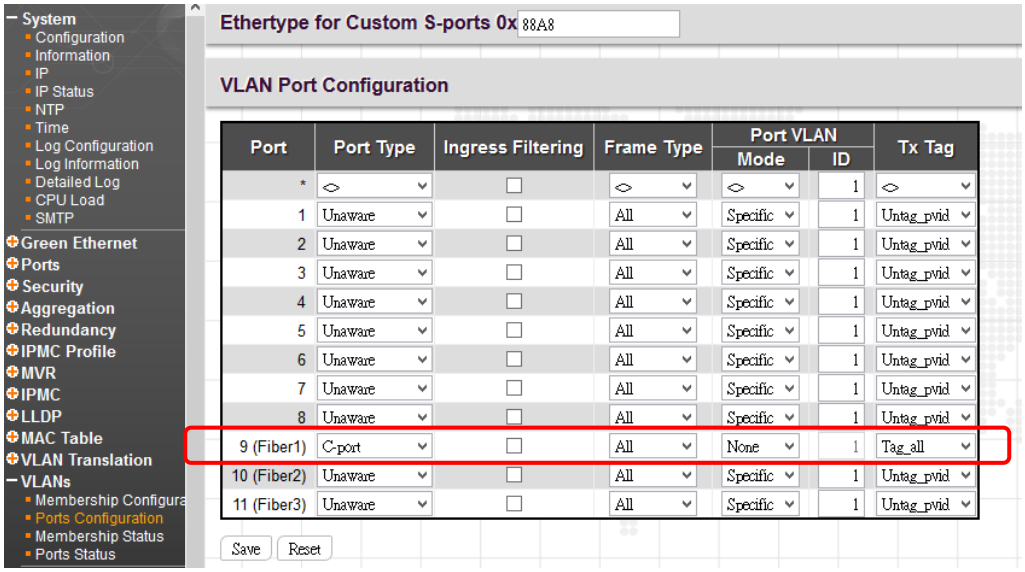
B. Remote Management VLAN

VLANs > VLAN Membership Configuration



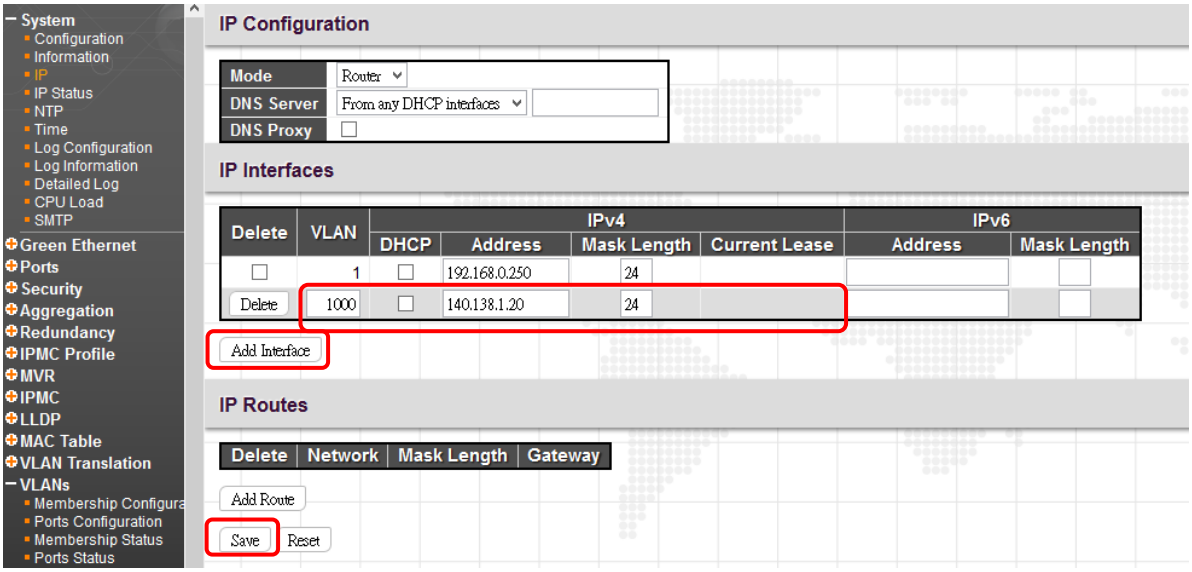
1. Click “Add New VLAN” button to insert a new entry.
2. Enter “1000” for VLAN ID, “Management” for VLAN Name and select port 9 as a port member.
3. Click “Save” button.

VLANs > VLAN Port Configuration



4. Set Port 9's Port Type to "C-port", Frame Type to "All", Port VLAN Mode to "None", Tx Tag to "Tag_all".
5. Click "Save" button.

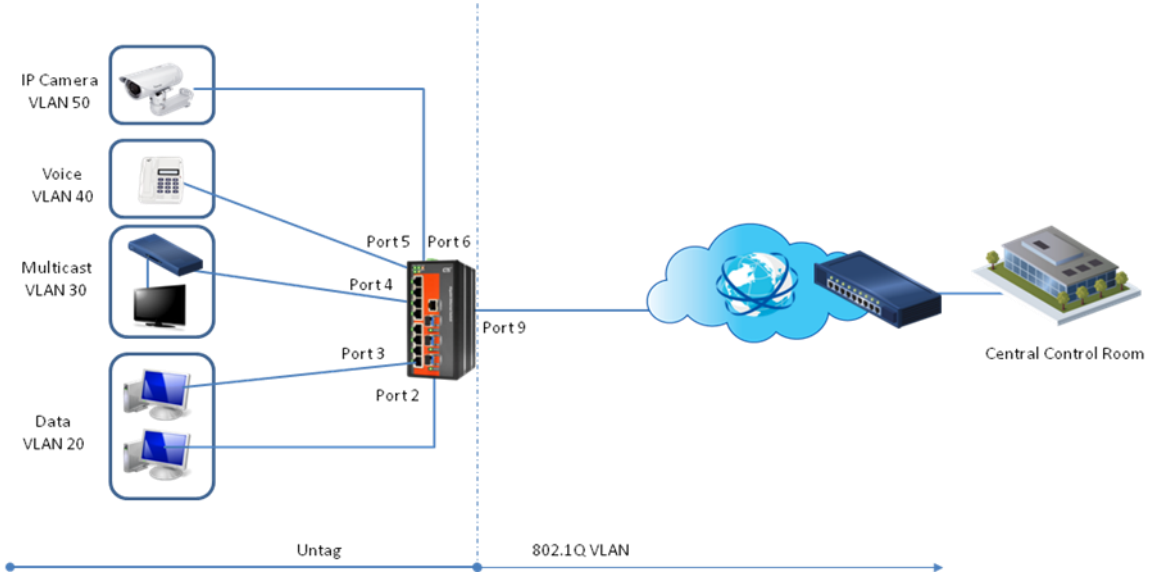
System > IP > IP Interfaces



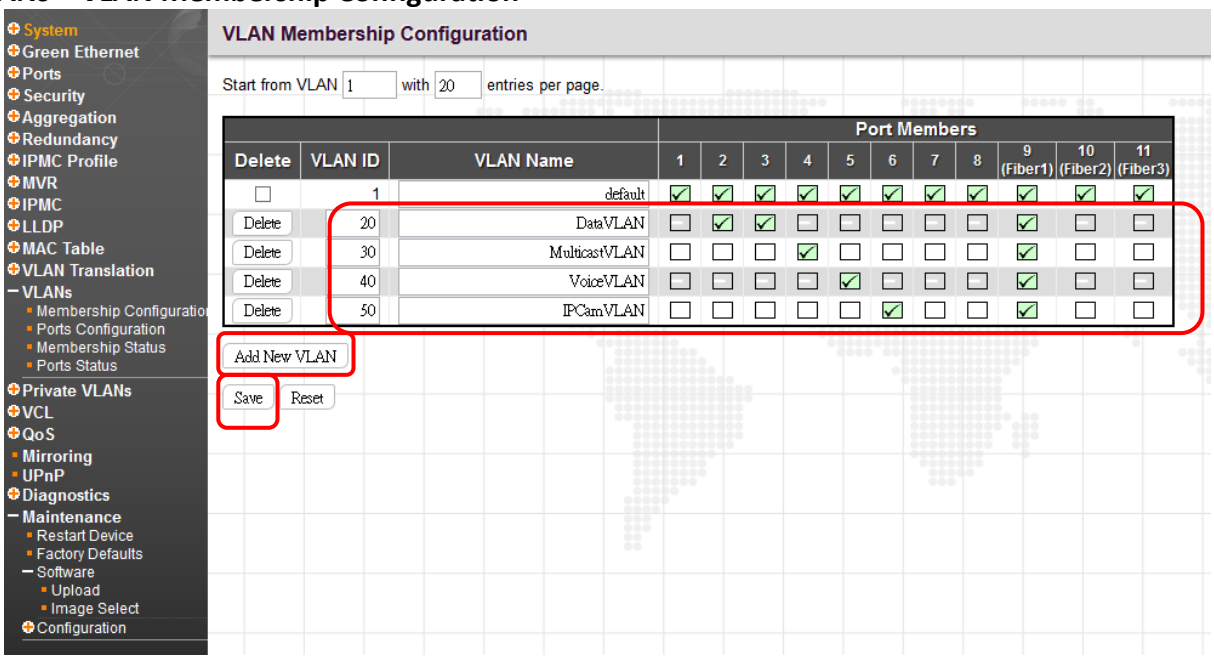
6. Click "Add Interface" button to insert a new entry.
7. Input management VLAN information. Set VLAN field to "1000" and IP address to "140.138.1.20".
8. Click "Save" button to change management VLAN from 1 to 1000. Once you click "Save" button, your local management PC is immediately disconnected from this device.
9. Now you are able to manage the device via Port 9.
10. Delete VLAN 1.

NOTE: *Make sure you have correct IP and VLAN settings before deleting the original management VLAN. Incorrect settings or cabling will disconnect you from this device. If you are unable to manage this device due to incorrect settings, use the CONSOLE port and CLI to reset the IP and VLAN settings to the defaults. Then, use the default IP address to reconfigure this device.*

C. 802.1Q VLAN



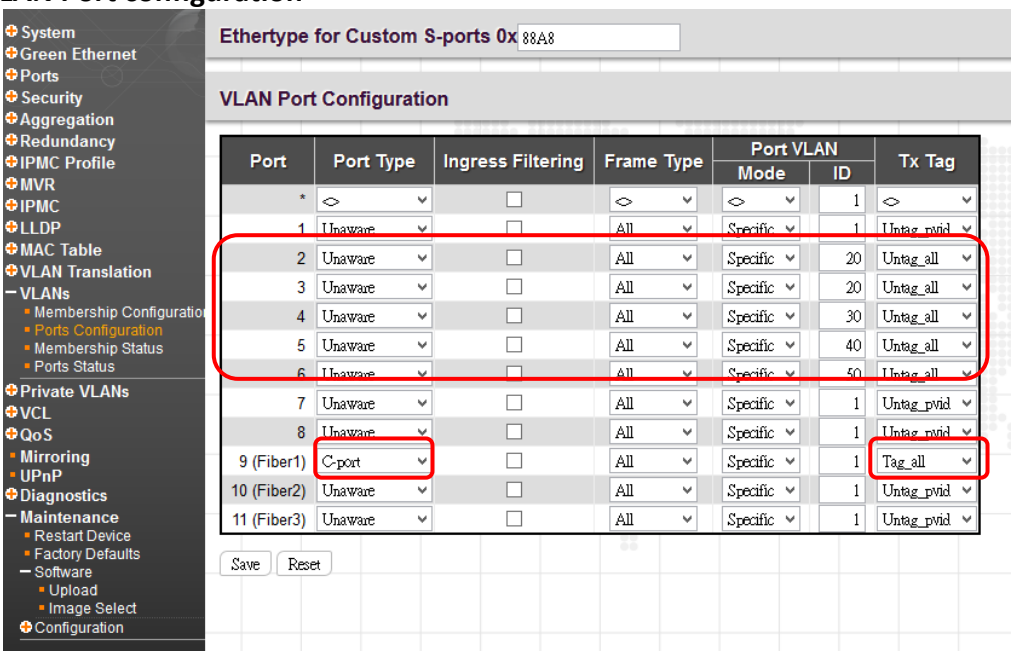
VLANs > VLAN Membership Configuration



1. Click “Add New VLAN” to insert new entries.
2. Enter VLAN 20 settings (20, DataVLAN, port 2 & 3 & 9).
3. Enter VLAN 30 settings (30, MulticastVLAN, port 4 & 9).
4. Enter VLAN 40 settings (40, VoiceVLAN, port 5 & 9).

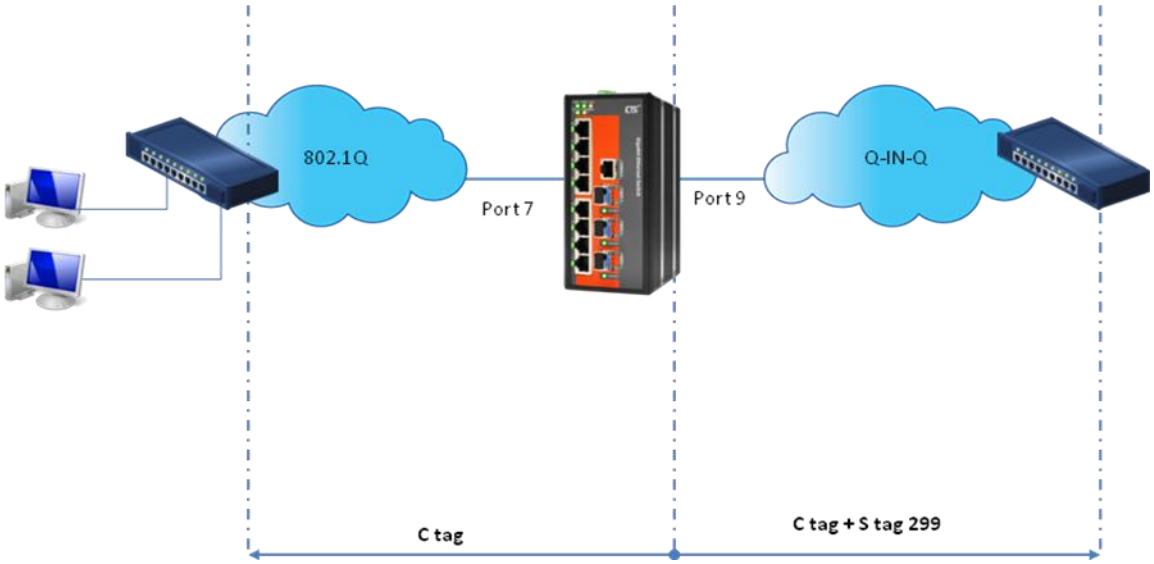
5. Enter VLAN 50 settings (50, IPCamVLAN, port 6 & 9).
6. Click “Save” button.

VLANs > VLAN Port configuration

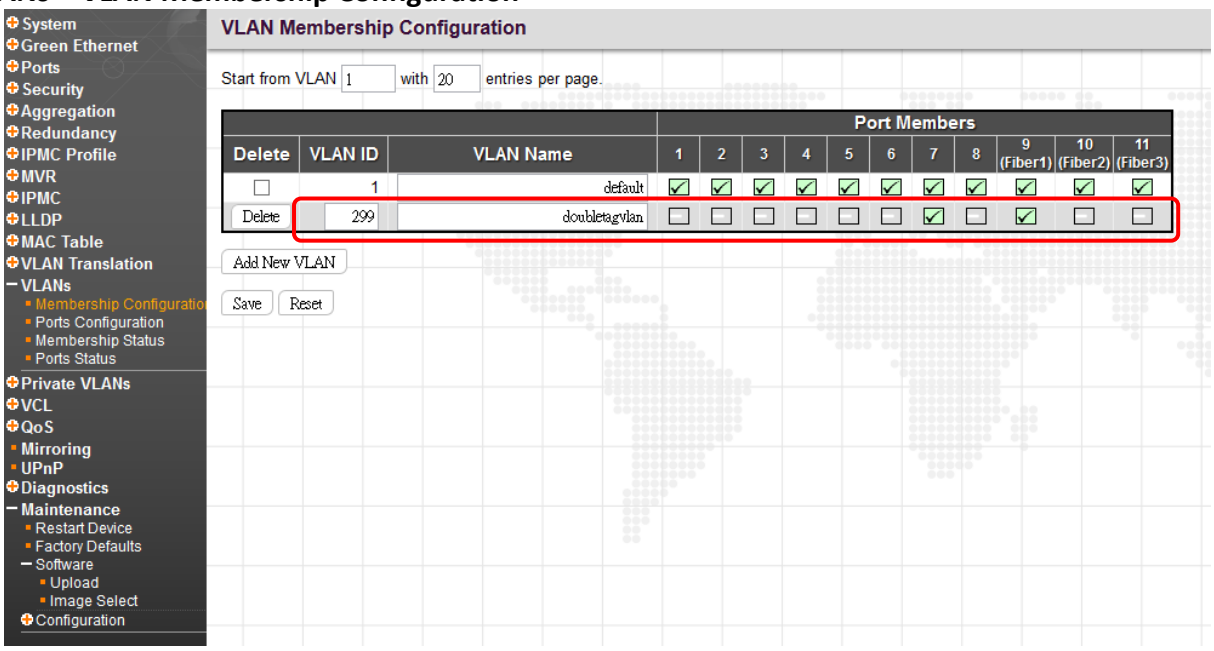


7. Set Port 2, 3, 4, 5, 6’s Port Type to “Unaware”, Frame Type to “All”
8. Set Port 2, 3, 4, 5, 6’s Port Port VLAN ID to “20”, “20”, “30”, “40”, “50”, respectively.
9. Set Port 2, 3, 4, 5, 6’s Tx Tag to “Untag_all” or “Untag_pvid”.
10. Set Port 9’s Port Type to “C-port” and Tx Tag to “Tag_all” or “Untag_pvid”.
11. Click “Save” button.

D. QinQ VLAN

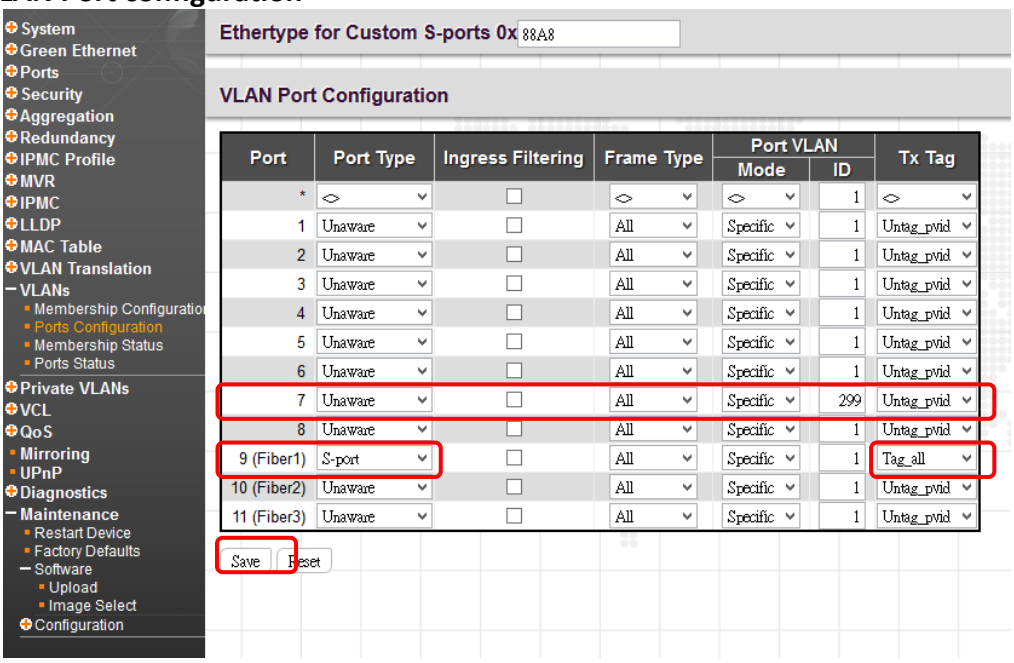


VLANs > VLAN Membership Configuration



1. Click “Add New VLAN” to insert a new entry.
2. Enter VLAN ID 299 settings (299, doubletagvlan, Port 7 & 9).
3. Click “Save” button.

VLANs > VLAN Port configuration



4. Set Port 7's Port Type to "Unaware", Frame Type to "All", Port VLAN ID to "299", Tx Tag to "Untag_pvid".
5. Set Port 9's Port Type to "S-port", Frame Type to "All", Tx Tag to "Tag_all" or "Untag_pvid".
6. Click "Save" button.

APPENDIX D. 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.

CTC union®

www.ctcu.com

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

ISO 9001 Quality System Certified CTC Union Technologies Co.,LTD.
All trademarks are the property of their repective owners. Technical information in this document is subject to change without notice.