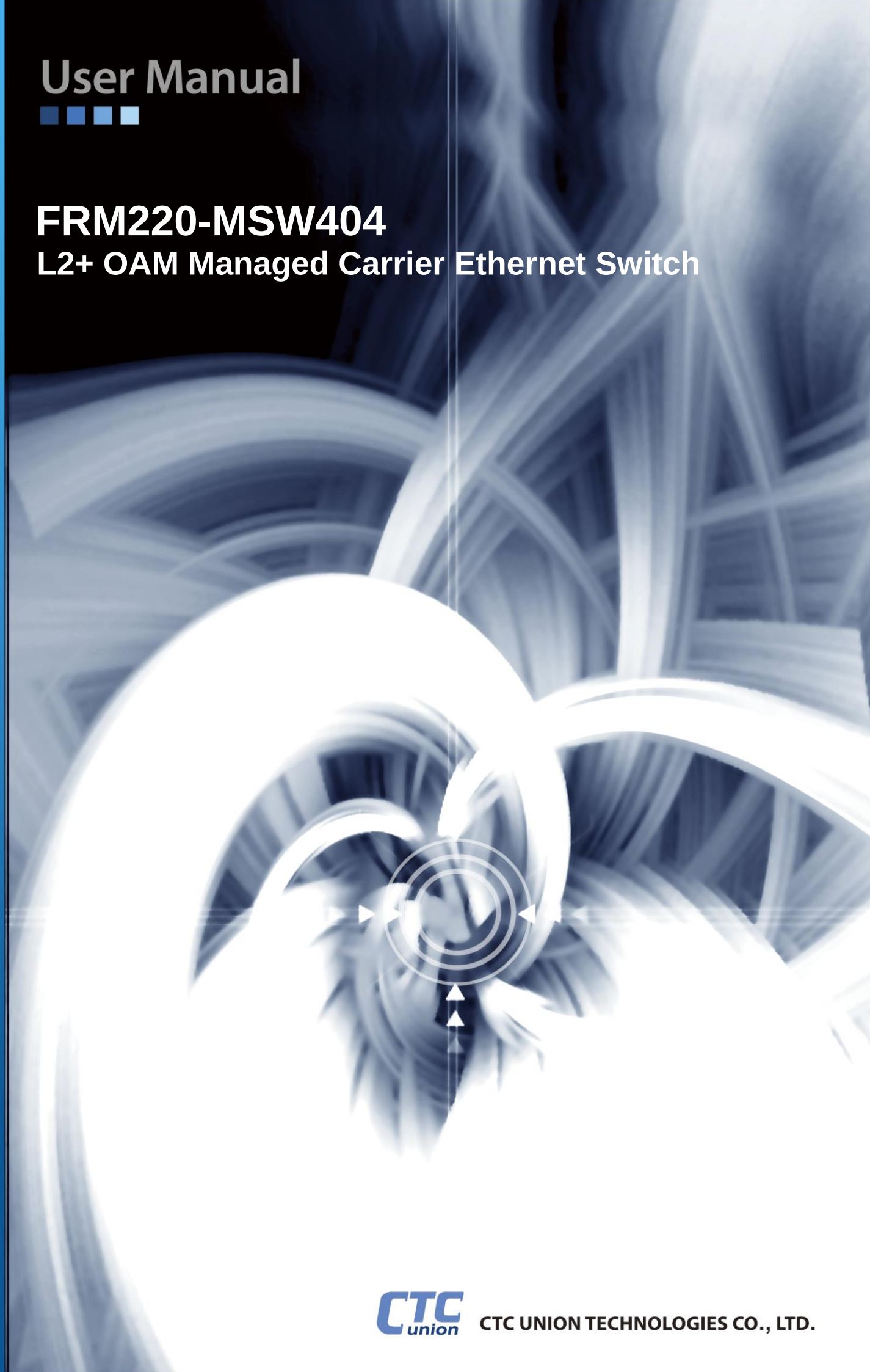
User Manual

FRM220-MSW404

L2+ OAM Managed Carrier Ethernet Switch



CTC UNION TECHNOLOGIES CO., LTD.

LEGAL

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

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

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

TRADEMARKS

Microsoft is a registered trademark of Microsoft Corp.
HyperTerminal™ is a registered trademark of Hilgraeve Inc.

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.

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

FRM220-MSW404
L2+ OAM Managed Carrier Ethernet Switch

User Manual
Version 0.9b (Preliminary) July 2015

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

CHAPTER 1. INTRODUCTION 9

1.1 WELCOME 9
1.2 PRODUCT DESCRIPTION 9
1.3 PRODUCT SPECIFICATIONS 9
1.4 PANEL 10
1.4.1 LED 10
1.4.2 Default Push Button 11

CHAPTER 2. INSTALLATION 12

2.1 CHASSIS OPTION 12
2.2 ELECTRICAL INSTALLATION FOR CHASSIS 13
2.3 INSTALLATION OF SFP MODULES 13
2.3.1 Inserting a Bale Clasp SFP Module into the Cage 13
2.3.2 Removing a Bale Clasp SFP Module 13

CHAPTER 3. WEB OPERATION & CONFIGURATION 14

3.1 HOME PAGE 14
3.1.1 Login 14
3.1.2 Port Status 15
3.1.3 Refresh 15
3.1.4 Help System 15
3.1.5 Logout 15
3.2 SYSTEM 16
3.2.1 System Configuration 16
3.2.2 System Information 17
3.2.3 System IP 17
3.2.4 System IP Status 19
3.2.5 System NTP 19
3.2.6 System Time 20
3.2.7 System Log Configuration 21
3.2.8 System Log Information 21
3.2.9 System Detailed Log 22
3.2.10 System CPU Load 22
3.3 PORTS 23
3.3.1 Ports Configuration 23
3.3.2 Ports State 25
3.3.3 Ports Traffic Overview 25
3.3.4 Ports QoS Statistics 26
3.3.5 Ports QCL Status 26
3.3.6 Ports Detailed Statistics 27
3.3.7 Ports SFP 29
3.4 SECURITY 30
3.4.1 Switch 30
3.4.1.1 Users 30
3.4.1.2 Privilege Levels 31
3.4.1.3 Auth Method 32
3.4.1.4 SSH 33
3.4.1.5 HTTPS 33
3.4.2 Access Management 34
3.4.2.1 Access Management Configuration 34
3.4.2.2 Access Management Statistics 34
3.4.3 SNMP 35
3.4.3.1 SNMP System Configuration 35
3.4.3.2 Trap Configuration 36
3.4.3.3 SNMPv3 Community Configuration 38
3.4.3.4 SNMPv3 User Configuration 39

3.4.3.5 SNMPv3 Group Configuration 40
3.4.3.6 SNMPv3 View Configuration 40
3.4.3.7 SNMPv3 Access Configuration 41
3.4.4 RMON 42
3.4.4.1 RMON Statistics Configuration 42
3.4.4.2 RMON History Configuration 42
3.4.4.3 RMON Alarm Configuration 43
3.4.4.4 RMON Event Configuration 44
3.4.4.5 RMON Statistics Overview 44
3.4.4.6 History Overview 45
3.4.4.7 Alarm Overview 46
3.4.4.8 Event Overview 47
3.4.5 Network 47
3.5.5.1 Port Security 47
3.4.5.1.1 Limit Control 47
3.4.5.1.2 Switch Status 49
3.4.5.1.3 Port Status 50
3.4.5.2 NAS 50
3.4.5.2.1 Configuration 51
3.4.5.2.2 Switch Status 53
3.4.5.2.3 Port Statistics 54
3.4.5.3 ACL 55
3.4.5.3.1 Ports 55
3.4.5.3.2 Rate Limiters 57
3.4.5.3.3 Access Control List 57
3.4.5.3.4 ACL Status 61
3.4.5.4 DHCP 62
3.4.5.4.1 Snooping Configuration 63
3.4.5.4.2 Relay Configuration 63
3.4.5.4.3 Relay Statistics 64
3.4.5.5 IP Source Guard 65
3.4.5.5.1 Configuration 65
3.4.5.5.2 Static Table 65
3.4.5.5.3 Dynamic Table 66
3.4.5.6 ARP inspection 66
3.4.5.6.1 Port Configuration 66
3.4.5.6.2 VLAN Configuration 67
3.4.5.6.3 Static Table 68
3.4.5.6.4 Dynamic Table Configuration 68
3.4.5.6.5 Dynamic Table Status 69
3.4.6 RADIUS 69
3.4.6.1 Configuration 69
3.4.6.2 RADIUS Overview 70
3.4.6.3 RADIUS Details 71
3.4.6.4 TACACS+ 73
3.5 AGGREGATION 74
3.5.1 Static 74
3.5.2 LACP 75
3.5.2.1 Port Configuration 75
3.5.2.2 System Status 76
3.5.2.3 Port Status 76
3.5.2.4 Port Statistics 77
3.6 LINK OAM 77
3.6.1 Port Settings 78
3.6.2 Event Settings 78
3.6.3 Port Statistics 79
3.6.4 Port Status 80
3.6.5 Event Status 81

3.6.6 Remote Device 83
3.7 LOOP PROTECTION 84
3.7.1 Configuration 84
3.7.2 Status 85
3.8 SPANNING TREE 85
3.8.1 Bridge Settings 86
3.8.2 MSTI Mapping 88
3.8.3 MSTI Priorities 89
3.8.4 CIST Ports 90
3.8.5 MSTI Ports 91
3.8.6 Bridge Status 91
3.8.7 Port Status 93
3.8.8 Port Statistics 94
3.9 IPMC PROFILE 94
3.9.1 Profile Table 94
3.9.2 Address Entry 96
3.10 MVR 96
3.10.1 Configurations 97
3.10.2 Statistics 98
3.10.3 MVR Channel Groups 98
3.10.4 MVR SFM Information 99
3.11 IPMC 99
3.11.1 IGMP Snooping 100
3.11.1.1 Basic Configuration 101
3.11.1.2 VLAN Configuration 102
3.11.1.3 Port Filtering Profile 103
3.11.1.4 Status 103
3.11.1.5 Groups Information 104
3.11.1.6 IPv4 SFM Information 104
3.11.2 MLD Snooping 105
3.11.2.1 Basic Configuration 105
3.11.2.2 VLAN Configuration 106
3.11.2.3 Port Filtering Profile 107
3.11.2.4 Status 108
3.11.2.5 Groups Information 108
3.11.2.6 IPv6 SFM Information 109
3.12 LLDP 109
3.12.1 Configuration 110
3.12.2 LLDP-MED 111
3.12.3 Neighbours 113
3.12.4 LLDP-MED Neighbours 114
3.12.5 LLDP Global Counters 114
3.13 EPS 115
3.14 MEP 117
3.15 ERPS 127
3.16 MAC TABLE 128
3.16.1 Configuration 128
3.16.2 MAC Address Table 129
3.17 VLAN TRANSLATION 129
3.17.1 Port to Group Mapping 130
3.17.2 VID Translation Mapping 130
3.18 VLANS 131
3.18.1 Membership Configuration 131
3.18.2 Membership Status 134
3.18.3 Port Status 134
3.19 PRIVATE VLANS 135
3.19.1 PVLAN Membership 135
3.19.2 Port Isolation 135

3.20 VCL 136
3.20.1 MAC-based 136
3.20.1.1 Membership Configuration 136
3.20.1.2 Membership Status 137
3.20.2 Protocol-based VLAN 137
3.20.2.1 Protocol to Group 137
3.20.2.2 Group to VLAN 138
3.20.3 IP Subnet-based VLAN 139
3.21 VOICE VLAN 139
3.21.1 Configuration 140
3.21.2 OUI 141
3.22 ETHERNET SERVICES 142
3.22.1 Port Configuration 142
3.22.2 L2CP 143
3.22.3 Bandwidth Profiles 143
3.22.4 EVCs 145
3.22.5 ECEs 146
3.22.6 EVC Statistics 148
3.22.7 ECE Statistics 149
3.23 QOS 149
3.23.1 Port Classification 150
3.23.2 Port Policing 151
3.23.3 Queue Policing 151
3.23.4 Port Scheduler 152
3.23.5 Port Shaping 154
3.23.6 Port Tag Remarking 155
3.23.7 Port DSCP 156
3.23.8 DSCP-Based QoS 157
3.23.9 DSCP Translation 158
3.23.10 DSCP Classification 159
3.23.11 QoS Control List 159
3.23.12 Storm Control 162
3.24 MIRRORING 163
3.25 UPNP 163
3.26 GVRP 164
3.26.1 Global Config 164
3.26.2 Port Config 165
3.27 SFLOW 165
3.27.1 Configuration 165
3.27.2 Statistics 167
3.28 RFC2544 168
3.28.1 Profiles 168
3.28.2 Report 170
3.29 DIAGNOSTICS 172
3.29.1 Ping 172
3.29.2 Link OAM 172
3.29.2.1 MIB Retrieval 172
3.29.3 Ping6 173
3.29.4 VeriPHY 173
3.30 MAINTENANCE 174
3.30.1 Restart Device 174
3.30.2 Factory Defaults 175
3.30.3 Software 175
3.30.3.1 Upload 175
3.30.3.2 Image Select 175
3.30.3.3 Upgrade boot code 175
3.30.4 Configuration 176
3.30.4.1 Save 176

3.30.4.2 Download 176
3.30.4.3 Upload 176
3.30.4.4 Activate 177
3.30.4.5 Delete 177

CHAPTER 1. INTRODUCTION

1.1 Welcome

Thank you for choosing FRM220-MSW404 L2 OAM Managed Switch. This manual is used to explain the hardware installation procedures and operation of FRM220-MSW404, and to present its capabilities and specifications. This manual is divided into 3 chapters, the Introduction, Installation and Web Based Provisioning chapters. Installers should carefully read Chapter 1 & 2, Introduction and Installation. For Operating Personnel who would like to use Web Based Management, go to Chapter 3 for detailed descriptions.

1.2 Product Description

FRM220-MSW404 is a carrier class Ethernet Demarcation Device with 4 x 10/100/1000Base-T Ethernet ports and 4 x 100/1000Base-X dual rate SFP fiber ports which enables E-Line, E-LAN and E-Tree services (Carrier Ethernet 2.0 Compliant) for Metro Ethernet network deployments. By supporting link and service Ethernet OAM schemes, the FRM220-MSW404 also provides RFC2544 features and extensive fault detection and diagnostic capabilities to ensure that actual network use complies with pre-agreed SLA (Service Level Agreement).

1.3 Product Specifications

- **Optical Interface**
  - Connector: SFP cage x 4
  - Data rate: 100M/1000M (Manual setting)
  - Duplex mode: Full duplex
- **Electrical Interface**
  - Connector: UTP port x 4
  - Data rate: UTP 10M/100M/1000M (auto or forced)
  - Duplex mode: Full or Half Duplex (RJ-45)
  - Cable: 10Base-T Cat. 3,4,5,5e UTP
100Base-TX Cat. 5, 5e or higher
1000Base-T Cat 5, 5e, 6 or higher
- **Standards**: IEEE802.3, 802.3u, 802.3z, 802.3ab, 802.3x, 802.1W, 802.1p, 802.1Q, RFC 4330 (SNTP)
- **Maximum MTU**: 10K bytes
- **Packet Buffer**: 8M bits
- **MAC Table Size**: 8K
- **Indicators**: Power, T1, T2, ALM, Speed, Link/ACT
- **Power**
  - **Input**: 12VDC
  - **Consumption**: <20W
- **Dimensions**: 140mm (D) x 88mm (W) x 42mm (H)
- **Weight**: 180g
- **Operating Temperature**: 0°C ~50°C
- **Humidity**: 5%~90% non-condensing
- **Certification**: CE, FCC, RoHS Compliant

1.4 Panel

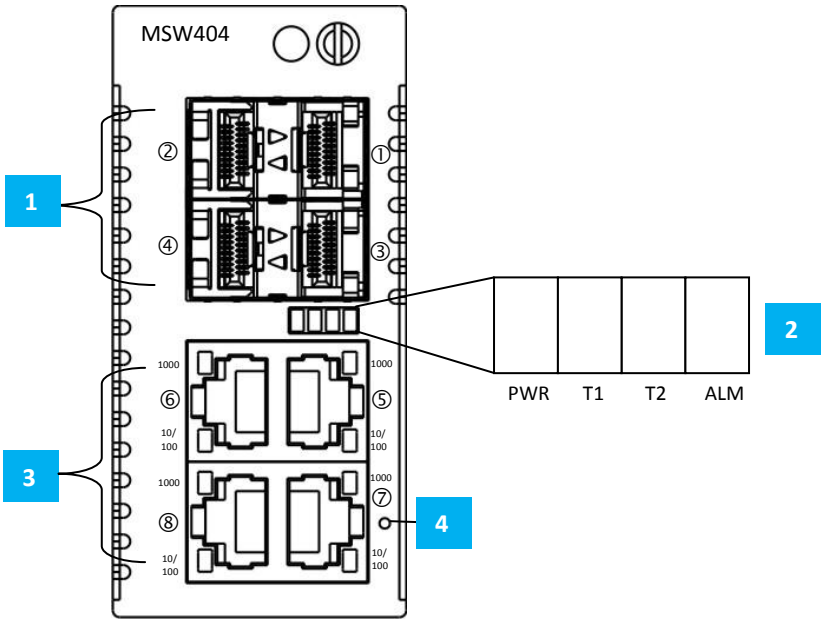


Figure1. FRM220-MSW404 Front Panel

1 SFP Slots

2 PWR, T1, T2, ALM LED indicators

3 RJ-45 UTP Ports

4 Default push button

1.4.1 LED

LED	Color	Status	Definition
PWR	Green	ON	Power is on.
	OFF		Power is not connected.
T1	Green	ON	Under loopback testing.
	OFF		Normal operation.
T2	Green	ON	Under RFC2544 testing.
	OFF		Normal operation.
ALM	Red	ON	Alarm events occur.
	OFF		Normal operation.
Port 1~4 SFP Fiber LED	Green	ON	Port link is up and works in 100Mbps.
		Blink	Traffic is present.
	OFF		No fiber link or fiber link works in 1000Mbps.
	Yellow	ON	Port link is up and works in 1000Mbps.
		Blink	Traffic is present.
	OFF		No fiber link or fiber link works in 100Mbps.
RJ-45 Port 5~8 10/100 LED	Yellow	ON	Port link is up and works in 10/100Mbps.
		Blink	Traffic is present.
	OFF		No Ethernet link or port link works in 1000Mbps.
RJ-45 Port 5~8 1000 LED	Orange	ON	Port link is up and works in 1000Mbps.
		Blink	Traffic is present.
	OFF		No Ethernet link or port link works in 10/100Mbps.

1.4.2 Default Push Button

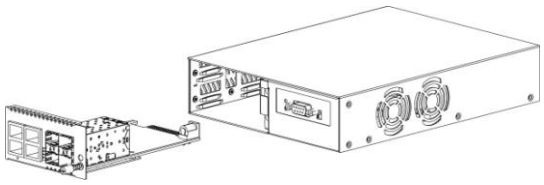
The "Default" push button is located next to RJ-45 UTP port. It is used to recover lost password or to return TCP/IP settings to factory default values. Use a pencil or blue-point pen and then press the button for 3 seconds then release to reset the device to the factory default settings. DO NOT POWER OFF. Allow the device to again fully reboot.

Default values:
Login Username: admin
Password: None (Leave this field blank)
IP: 10.1.1.1
Netmask: 255.255.255.0
Gateway: 0.0.0.0

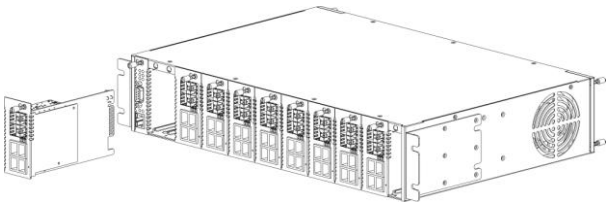
CHAPTER 2. INSTALLATION

2.1 Chassis Option

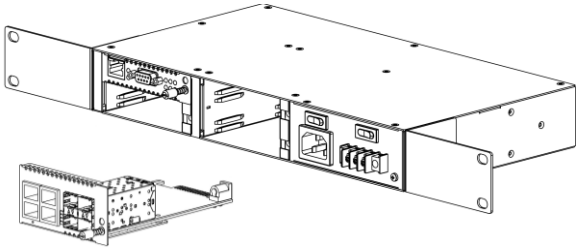
FRM220-MSW404 card can be placed in **FRM220** series chassis, including the two-slot CH02M, CH02-NMC, CH04A, CH08 or the full twenty-slot CH-20 chassis. Chassis with built-in power are available with single AC (100~240VAC), single DC (18~75VDC), dual AC, dual DC or AC plus DC combo.



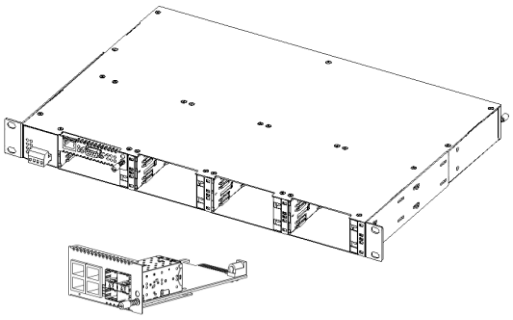
CH02M or CH02-NMC-XX Chassis (XX= AC, DC, AA, DD or AD)



FRM220-CH20



CH04A-XX Chassis (XX= AC, DC, AA, DD or AD)



CH08-XX Chassis (XX= AC, DC, AA, DD or AD)

Figure 2. Chassis options for FRM220-MSW404 card

2.2 Electrical Installation for Chassis

With a built-in AC power chassis, AC power is supplied to the chassis through a standard IEC C14 3-prong receptacle, located on the rear of the chassis. Any detachable nationally approved power cord with IEC C13 line plug may be used to connect AC power to the chassis unit. With a built-in DC power chassis, DC-48V is connected to the terminal block located on the rear of the chassis, observing the proper polarity. The chassis should always be grounded through the protective earth lead of the power cable in AC installations, or via the frame ground connection for DC installations.

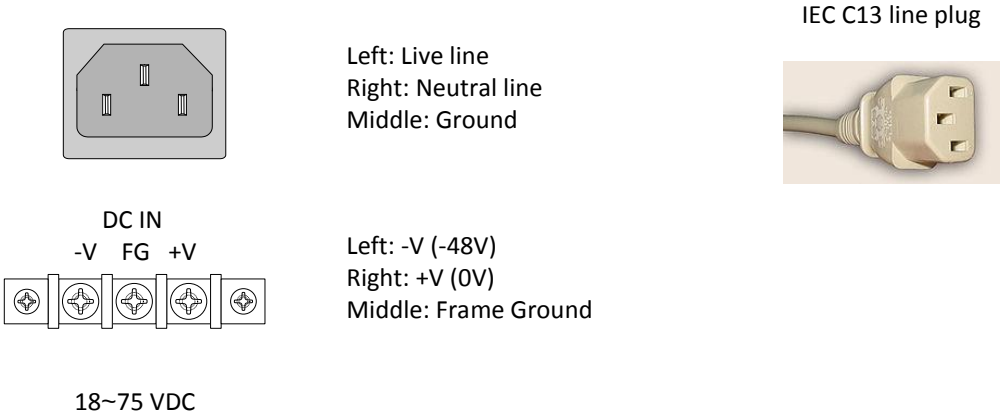


Figure 3. IEC (AC) & terminal block (DC) power connector pin assignment

2.3 Installation of SFP Modules

This device supports SFP modules that are of the Bale Clasp type. The bale clasp pluggable module has a bale clasp that secures the module into the SFP cage.

2.3.1 Inserting a Bale Clasp SFP Module into the Cage

Step 1. Close the bale clasp upward before inserting the pluggable module.
Step 2. Line up the SFP module with the port, and slide it into the cage.

2.3.2 Removing a Bale Clasp SFP Module

Step 1. Open the bale clasp on the SFP module. Press the clasp downward with your index finger.
Step 2. Grasp the SFP module between your thumb and index finger and carefully remove it from the SFP cage.

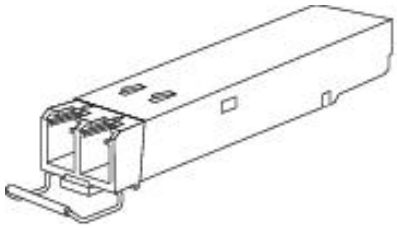


Figure 4. Bale Clasp type SFP with bale open

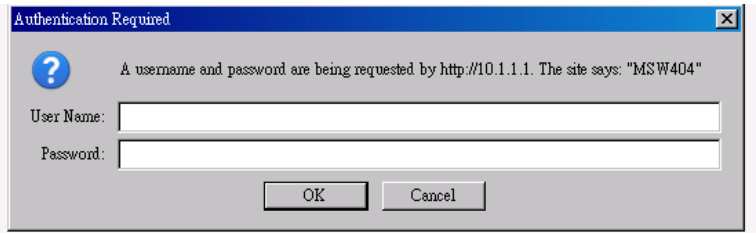
CHAPTER 3. WEB OPERATION & CONFIGURATION

3.1 Home Page

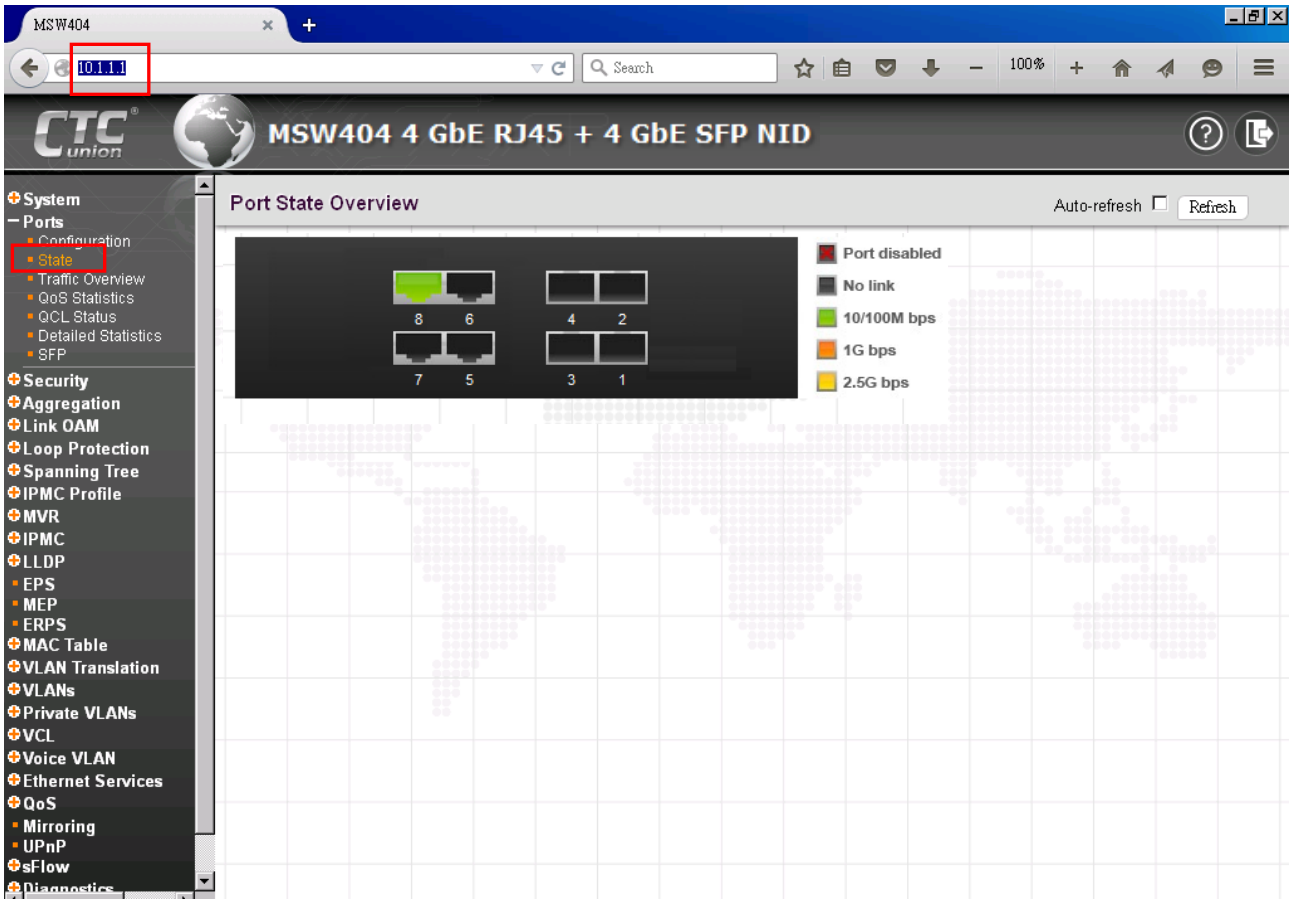
Using Internet Explorer (Version 9.0 or above is recommended), Firefox, Chrome or other stable web browser, enter the IP address of the FRM220-MSW404 in the browser's location bar. The factory default address is 10.1.1.1.

3.1.1 Login

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



The factory default is username 'admin' with no password.



Web Home Page

3.1.2 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 indicates a LAN connection with a speed of 10/100Mbps. The "Amber" colored port indicates a connection speed of 1000Mbps.

The status display can be reached by using the left side menu, and return to **Ports>State**.

3.1.3 Refresh

To update the screen, click the "Refresh" button. For automatic updating of the screen, the "Auto-refresh" checkbox may be selected. The screen will be auto refreshed every 3 seconds.

Unless connected directly on a local LAN, we recommend not using the auto-refresh function as it does generate a bit of traffic.

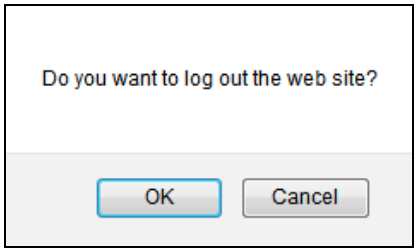
3.1.4 Help System

The FRM220-MSW404 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.

3.1.5 Logout

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

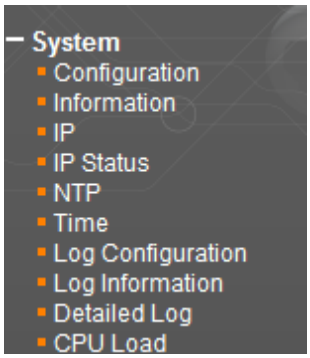
After clicking the logout icon, a confirmation screen will be displayed. Click "OK" to finish logging out or click "Cancel" to return to the web configuration GUI.



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.

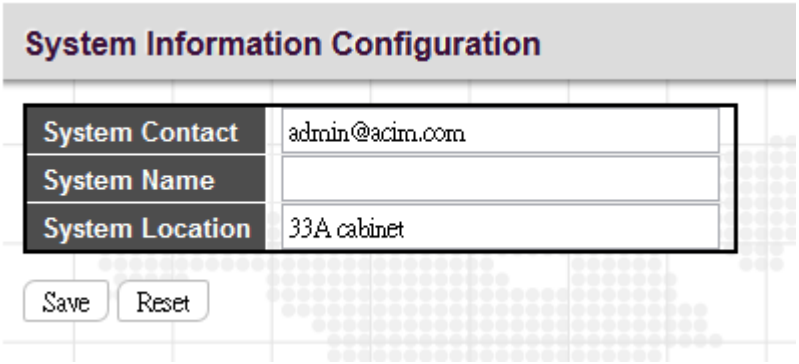
3.2 System

The configuration under the "System" menu includes device settings such as IP address, time server, etc.



3.2.1 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.



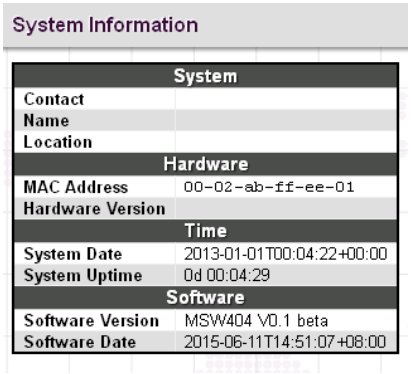
System Contact: Indicate the descriptive contact information. This could be a person’s name, email address or other descriptions. The allowed string length is 0~255 and the allowed content is the ASCII characters from 32~126.

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.

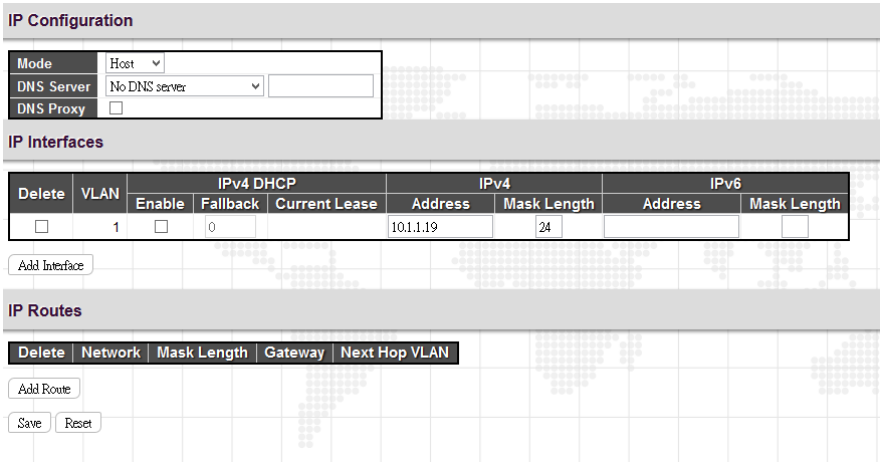
3.2.2 System Information

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.



3.2.3 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.

IPv4 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.

Fallback: The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables fallback mechanism. The DHCP will keep retrying until a valid lease is obtained when fallback is disabled. Valid value is from 0 to 4294967295.

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

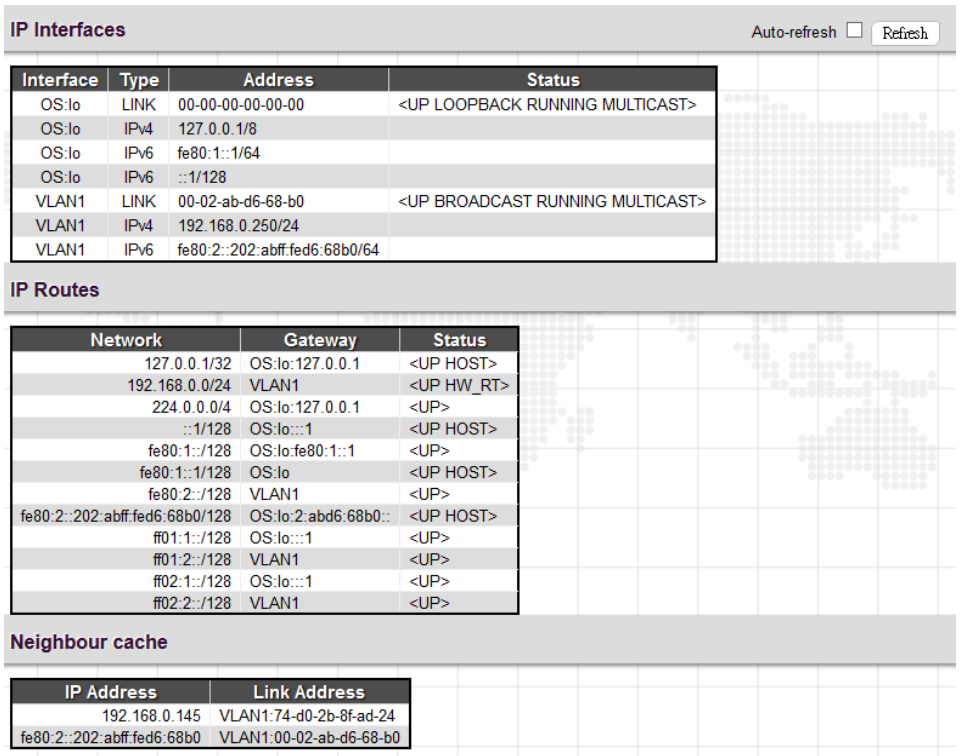
Route Network: The IP route is the destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or for IPv6 use the :: notation.

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.

3.2.4 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>

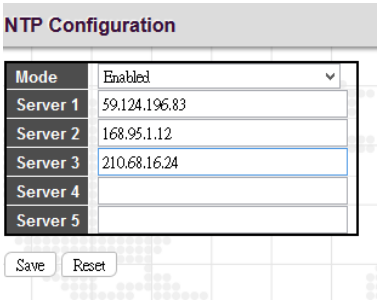
Neighbour cache

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.

3.2.5 System NTP

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



NTP Configuration

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

Save Reset

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

Enabled: Enable NTP client mode operation.

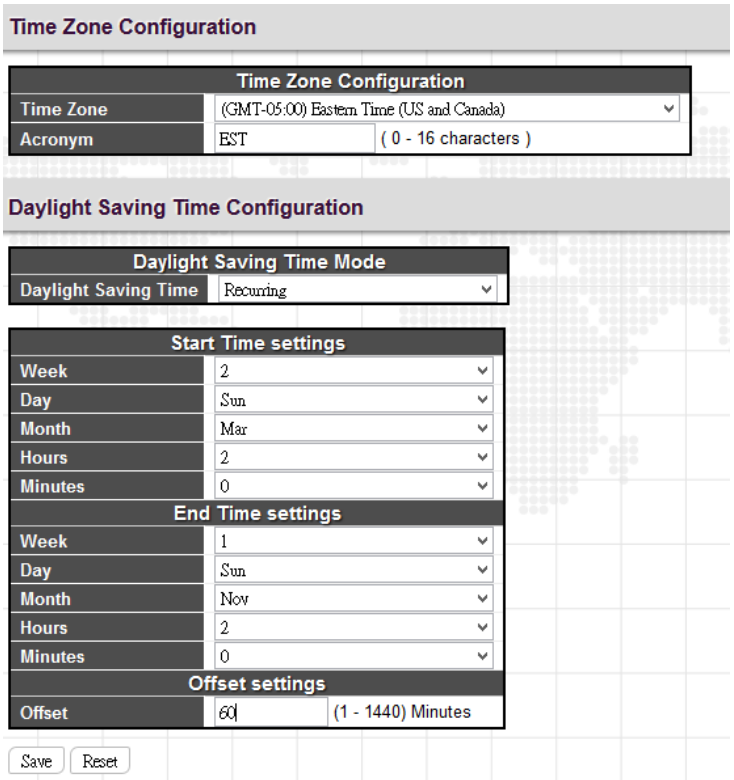
Disabled: Disable NTP client mode operation.

Server #: Enter the IPv4 or IPv6 address of an NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. NTP servers can also be represented by a legally valid IPv4 address. For example,

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

3.2.6 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:

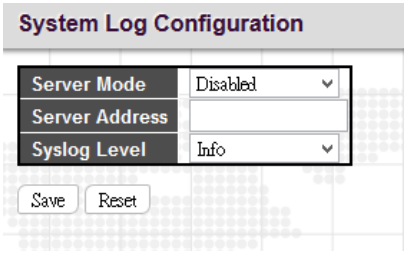
Start time settings: Select the starting week, day, month, year, hours, and minutes.

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.

3.2.7 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:

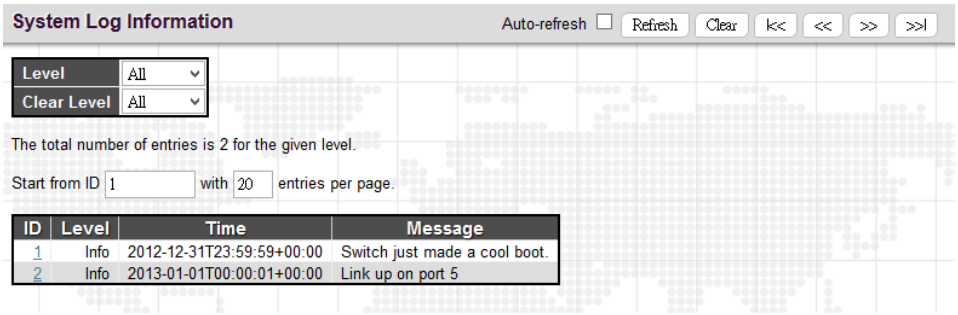
Info: Send information, warnings and errors.

Warning: Send warnings and errors.

Error: Send errors only.

3.2.8 System Log Information

Displays the collected log information.



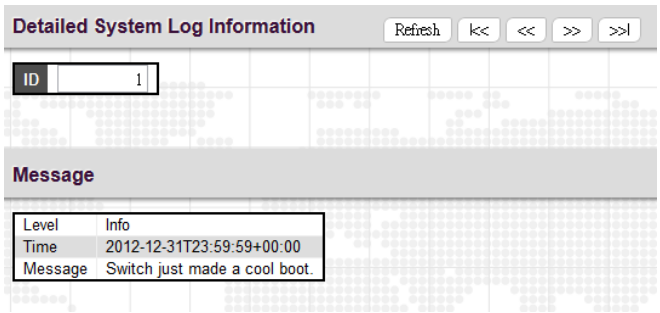
Level: Use this pull down to display all messages or messages of type info, warning or error.

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.

3.2.9 System Detailed Log

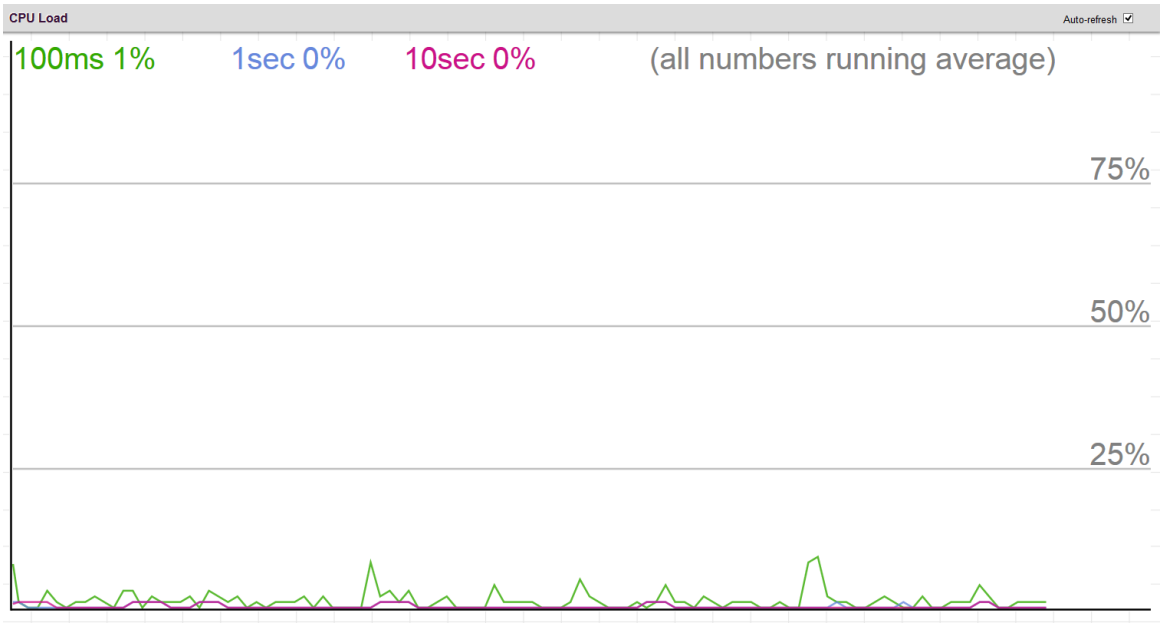
Displays individual log records.



View each log, by ID number.

3.2.10 System CPU Load

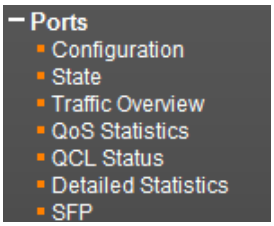
This page displays the CPU load, using an SVG graph.



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.

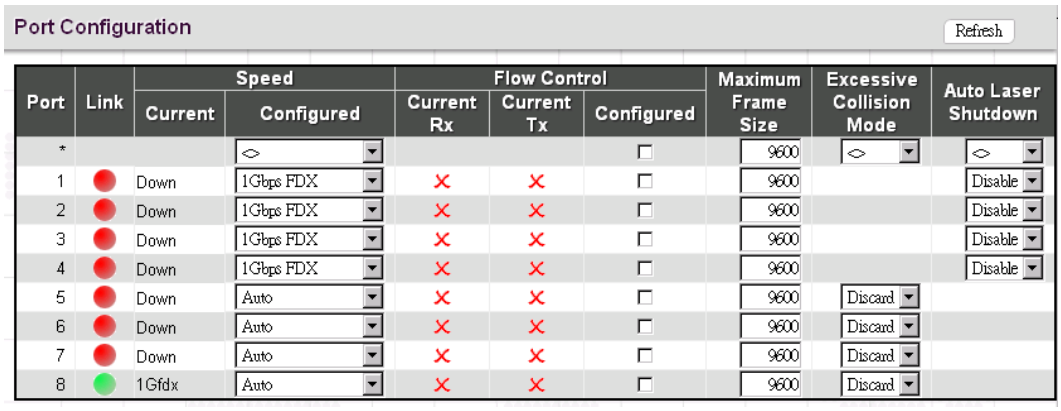
3.3 Ports

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



3.3.1 Ports Configuration

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



Port: This device has three fiber optical ports (for SFP modules) numbered 1~3 and one electrical LAN ports numbered 4. The fifth port is used to connect the device to the FRM-220 device. 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.

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

Possible fiber port settings are:

Disabled: Disables the switch port operation.

Auto: Port auto negotiates speed with the link partner. This option selects the highest speed that is compatible with the link partner. Please note that port 1~4 only support auto speed in 1Gbps and 2.5Gbps. If your port speed is 100Mbps, please select “100Mbps FDX” option.

100Mbps FDX: Forces the fiber port to 100Mbps full duplex mode.

1Gbps FDX: Forces the fiber port to 1Gbps full duplex mode.

2.5Gbps FDX: Forces the fiber port to 2.5Gbps full duplex mode.

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.

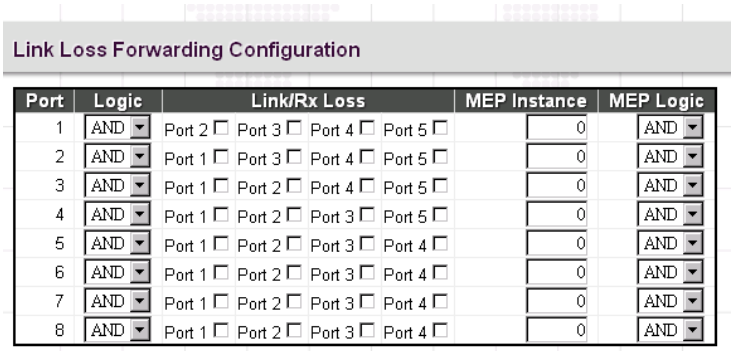
1Gbps FDX: Forces the port to 1Gbps full duplex.

Flow Control: The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is also related to the setting for Configured Link Speed.

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

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

Auto Laser Shutdown: Auto Laser Shutdown (ALS) is an optical safety mechanism which will shutoff laser transmission if the transceiver experiences a loss of receive signal. This function is disabled by default.



Link Loss Forwarding Configuration

In a simple media converter (two ports), a loss of fiber receive signal (link failure) can be used to force down the electrical Ethernet link and vice versa. This mechanism is referred to as "Link Loss Forwarding" or "Link Fault Pass-through".

This device is a eight-port L2 Ethernet switch with four fiber and four electrical Ethernet ports. With Link Loss Forwarding mechanism, when one Ethernet port detects a link down condition, this media converter can be programmed to logically force down any or all of the other Ethernet ports. The settings are done by checking the appropriate boxes in the matrix.

Logic: Select “AND” or “OR”

Link/Rx Loss: Select the appropriate ports that apply to this rule.

MEP Instance: The port Link Loss Forwarding depends on MEP instance.

MEP Logic: MEP instance logic of all Peer MEP ID.

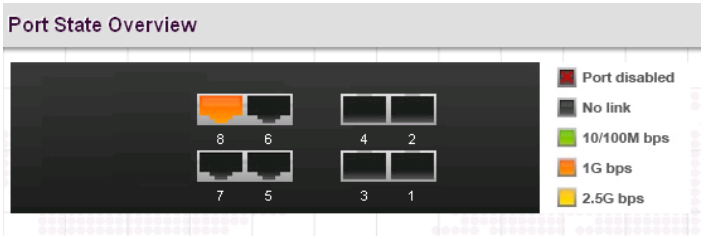
Example 1: Port 1 Tx off if any port 2, 3, 4 Rx loss:
Select “OR” logic and then select Port 1, 2, 3 Link/Rx Loss checkboxes.

Example 2: Port 1 Tx off if all ports 2, 3, 4 Rx loss
Select “AND” logic and then select Port 1, 2, 3 Link/Rx Loss checkboxes.

Example 3: Port 1 Tx off if port 3 Rx loss
Select “AND” or “OR” logic and then select Port 3 Link/Rx Loss checkbox.

3.3.2 Ports State

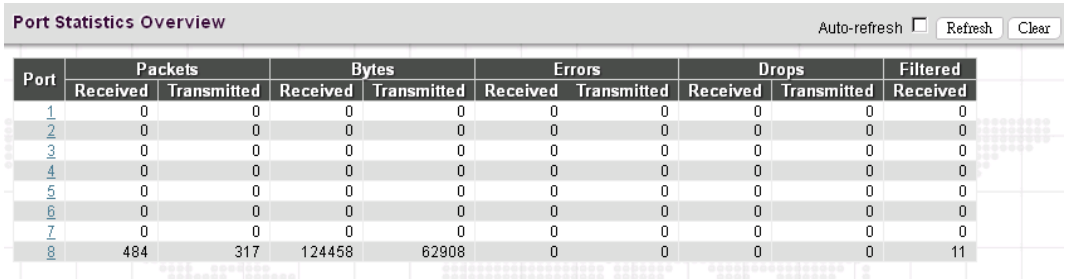
Display an overview graphic of the switch.



This is the same graphic overview shown when first logging into the switch for management. "Green" colored ports indicate a 10/100M linked state, while "Amber" colored ports indicate a 1G linked state. The “Yellow” colored ports indicate a 2.5G linked state. "Black" 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.

3.3.3 Ports Traffic Overview

Displays a comprehensive overview of traffic on all ports.



Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	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	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	484	317	124458	62908	0	0	0	0	11

The displayed counters are:

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

Packets: The number of received and transmitted packets per port.

Bytes: The number of received and transmitted bytes per port.

Errors: The number of frames received in error and the number of incomplete transmissions per port.

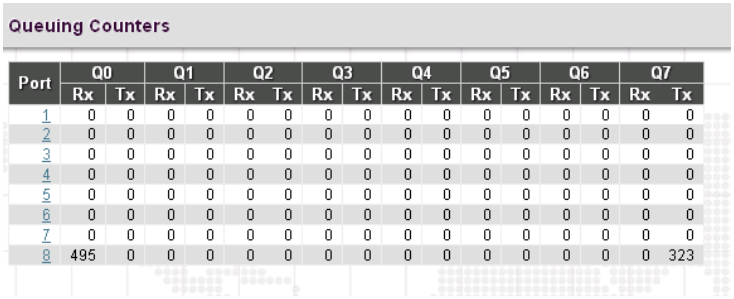
Drops: The number of frames discarded due to ingress or egress congestion.

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

The counter display can be updated by clicking the "Refresh" button. When "Auto-refresh" is checked, the display will be updated every 3 seconds. Clicking the "Clear" button will zero all counters and start counting again.

3.3.4 Ports QoS Statistics

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



Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	495	0	0	0	0	0	0	0	0	0	0	0	0	0	0	323

The displayed counters are:

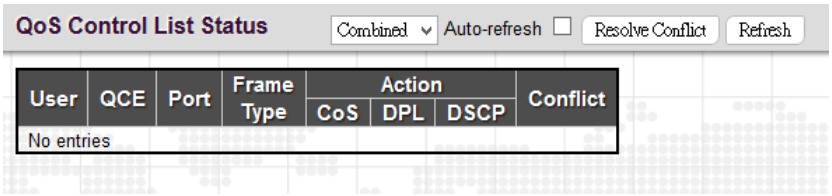
Port: The logical port for the settings contained in the same row.

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.

3.3.5 Ports QCL Status

This page shows the QCL status by different QCL users.



QoS Control List Status

Combined | Auto-refresh | Resolve Conflict | Refresh

User	QCE	Port	Frame Type	Action			Conflict
				CoS	DPL	DSCP	
No entries							

Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

User: Indicates the QCL user.

QCE#: Indicates the index of QCE.

Frame Type: Indicates the type of frame to look for incoming frames. Possible frame types are:

Any: The QCE will match all frame type.

Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed.

SNAP: Only (SNAP) frames are allowed.

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

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

Action: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP.

CoS: Classified QoS class; if a frame matches the QCE it will be put in the queue.

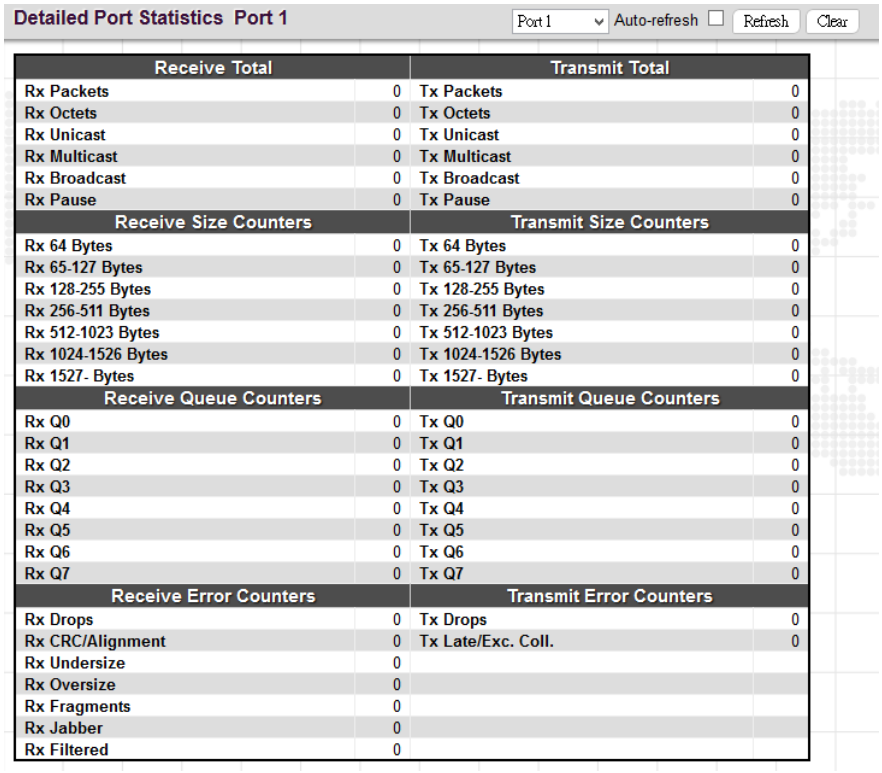
DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.

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

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.

3.3.6 Ports Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit. Use the port select pull down to select which switch port details to display.



Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
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.

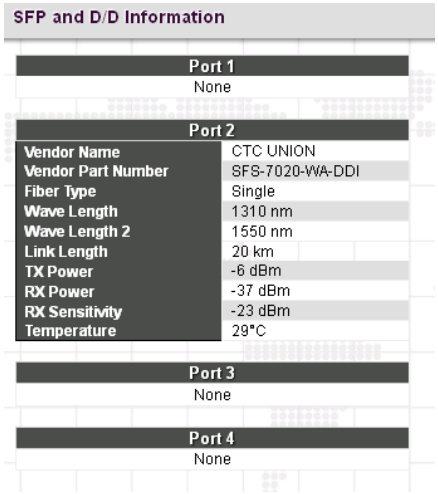
Transmit Error Counters:

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.

3.3.7 Ports SFP

This page displays current SFP status for all three fiber ports.



Vendor Name: SFP vendor (manufacturer's) name.

Vendor Part Number: 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).

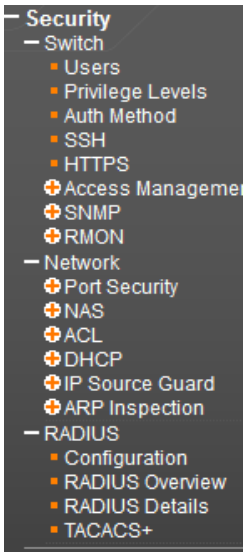
RX Power: The receive optical power is reported by SFP that support DDI.

RX Sensitivity: The Receive Sensitivity is reported by SFP that support DDI.

Temperature: The internal temperature is reported by SFP that support DDI.

3.4 Security

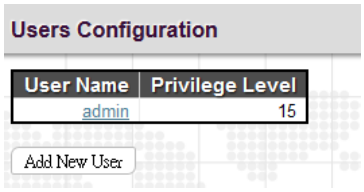
Under the security heading are three major icons, switch, network and RADIUS.



3.4.1 Switch

3.4.1.1 Users

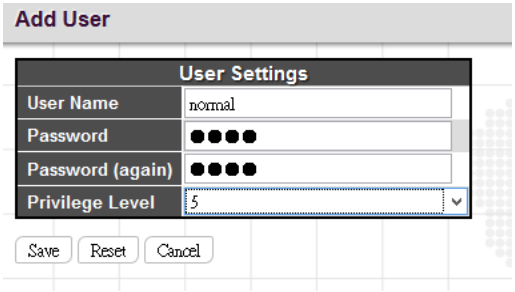
This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.



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

Click the entries in User Name column to edit the existing users. Or click the “Add New User” button to insert a new user entry.

Add User



User Name: Enter the new user name.

Password: Enter the password for this user account.

Password (again): Retype the password for this user account.

Privilege Level: Select the appropriate privilege level for this user account. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

3.4.1.2 Privilege Levels

This page provides an overview of the privilege levels.

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
Dhcp_Client	5	10	5	10
Diagnostics	5	10	5	10
EPS	5	10	5	10
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10
EVC	5	10	5	10
IP2	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
MEP	5	10	5	10
Mirroring	5	10	5	10
NTP	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10

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

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

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

IP: Everything except 'ping'.

Port: Everything except 'VeriPHY'.

Diagnostics: 'ping' and 'VeriPHY'.

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

Debug: Only present in CLI.

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

configuration read-only

configuration/execute read-write

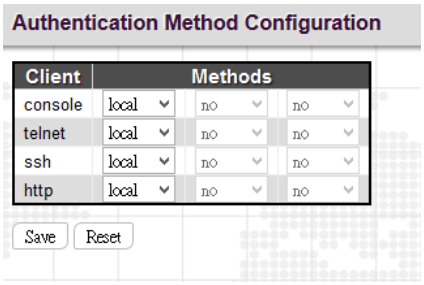
status/statistics read-only

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

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

3.4.1.3 Auth Method

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



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.

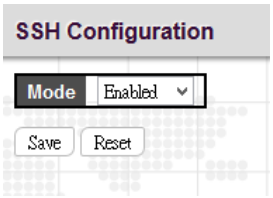
radius: Use remote RADIUS server(s) for authentication.

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.*

3.4.1.4 SSH

Configure SSH on this page.



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

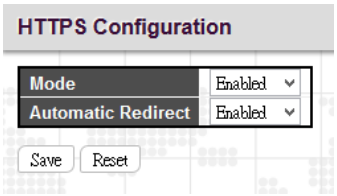
Enabled: Enable SSH mode operation. By default, SSH mode operation is enabled.

Disabled: Disable SSH mode operation.

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

3.4.1.5 HTTPS

Configure HTTPS on this page.



Mode: Indicates the HTTPS operation mode. When the current connection is HTTPS and HTTPS mode operation is disabled, web browser will automatically redirect to an HTTP connection. Possible modes are:

Enabled: Enable HTTPS mode operation.

Disabled: Disable HTTPS mode operation.

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

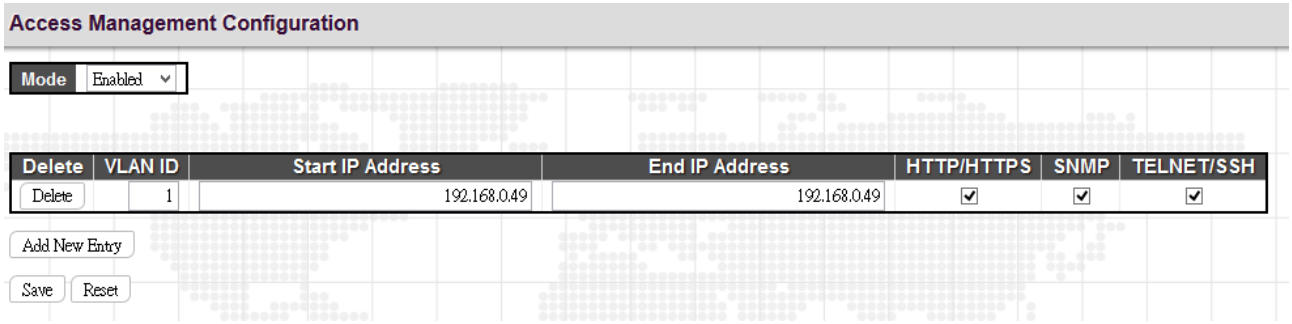
Enabled: Enable HTTPS redirect mode operation.

Disabled: Disable HTTPS redirect mode operation.

3.4.2 Access Management

3.4.2.1 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.

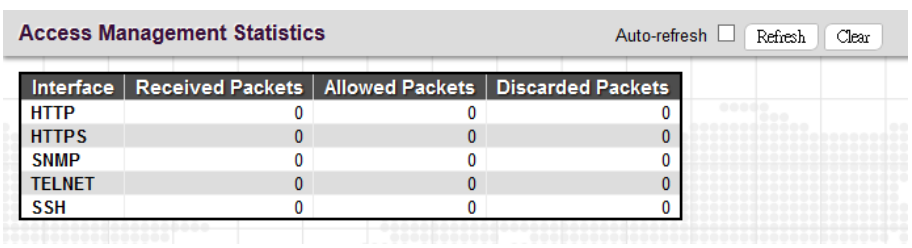
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

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

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

3.4.2.2 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.

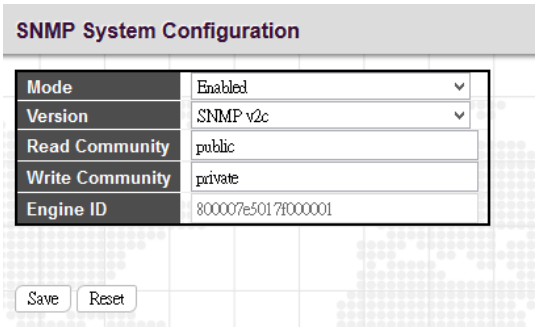
Allowed Packets: The number of allowed packets from the interface when access management mode is enabled.

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

3.4.3 SNMP

3.4.3.1 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.

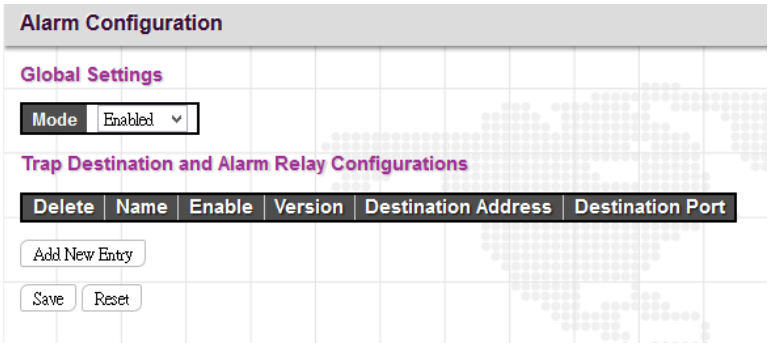
Read Community: Indicates the community read access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E.

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.

3.4.3.2 Trap Configuration

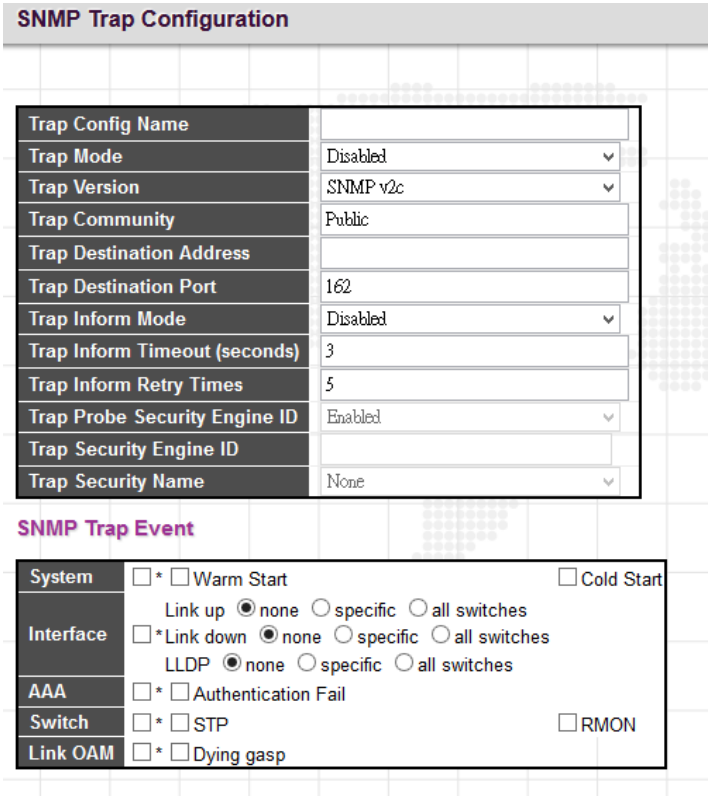
Configure SNMP trap on this page.



Global Settings

Mode: Globally enable or disable trap function.

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



SNMP Trap Configuration

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

Trap Mode: Indicates the SNMP trap mode operation.

Enabled: Enable SNMP trap mode operation.

Disabled: Disable SNMP trap mode operation.

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

SNMP v1: Set SNMP trap supported version 1.

SNMP v2c: Set SNMP trap supported version 2c.

SNMP v3: Set SNMP trap supported version 3.

Trap Community: Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 0x21 to 0x7E.

Trap Destination Address: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). Also allowed is a valid hostname. A valid hostname is a string drawn from the alphabet (A-Z; a-z), digits (0-9), dot (.) and dash (-). Spaces are not allowed. The first character must be an alpha character, and the first and last characters cannot be a dot or a dash.

Trap Destination port: Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. The default SNMP trap port is 162.

Trap Inform Mode: Indicates the SNMP trap inform mode operation. Possible modes are:

Enabled: Enable SNMP trap inform mode operation.

Disabled: Disable SNMP trap inform mode operation.

Trap Inform Timeout (seconds): Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

Trap Inform Retry Times: Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

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

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

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

Trap Security Engine ID: Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs use USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

Trap Security Name: Indicates the SNMP trap security name. SNMPv3 traps and informs use USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

SNMP Trap Event

System: The system trap events include the following.

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

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

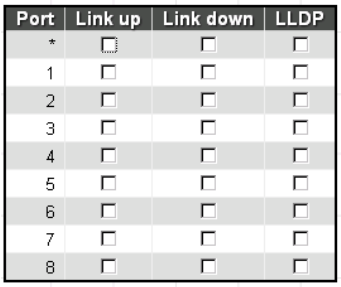
Interface: Indicates the Interface group's traps. Possible traps are:

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

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

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

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



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

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

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

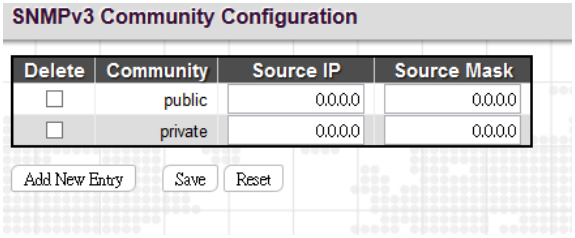
RMON: Select the checkbox to enable RMON trap. Clear to disable RMON trap.

Link OAM: Select the checkbox to enable Dying Gasp trap. A trap will be issued when the remote device encounters power failure.

After completing all the trap settings, click the "Save" button.

3.4.3.3 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.

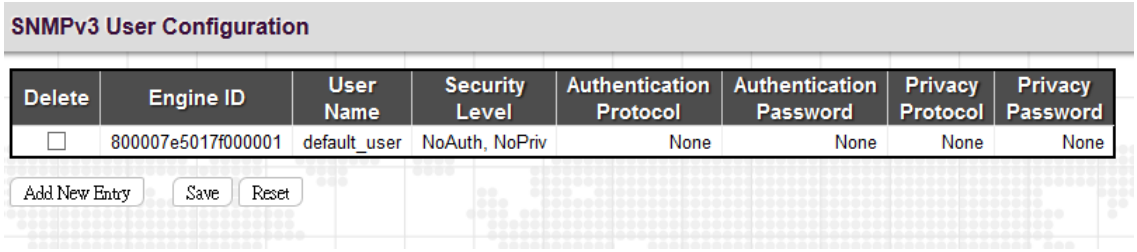
Community: Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string. This string is case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

3.4.3.4 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.

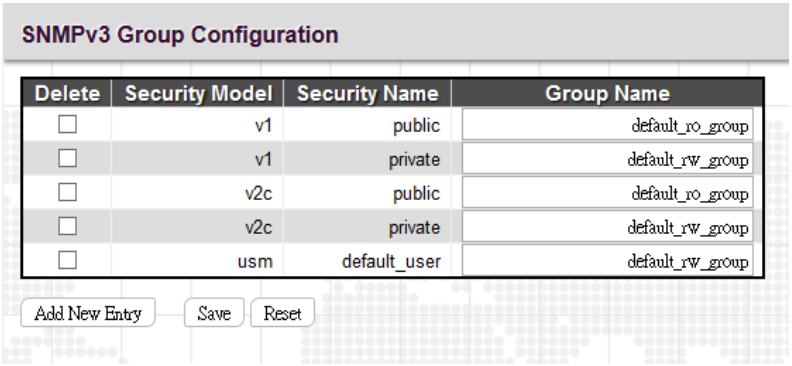
Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

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

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

3.4.3.5 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.

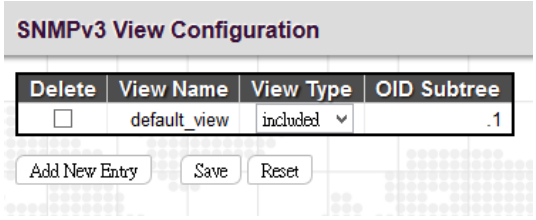
usm: User-based Security Model (USM) for SNMPv3.

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.

3.4.3.6 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:

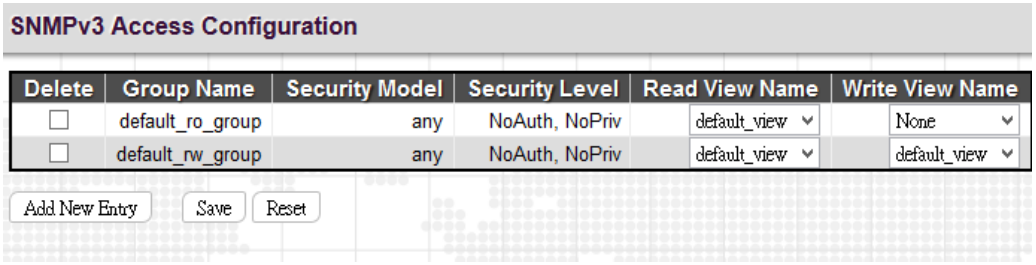
included: An optional flag to indicate that this view subtree should be included.

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 (*).

3.4.3.7 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.

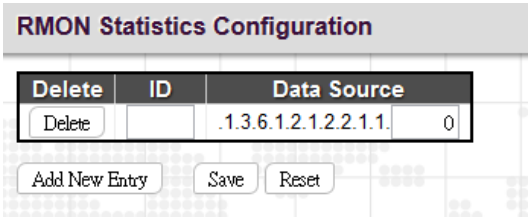
Read View Name: The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

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.

3.4.4 RMON

3.4.4.1 RMON Statistics Configuration

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



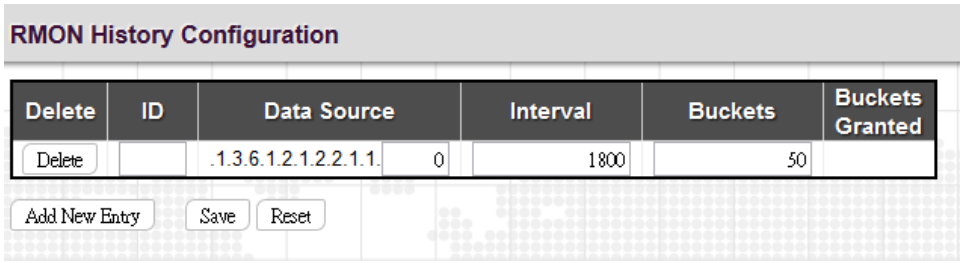
Delete: Check to delete the entry. It will be deleted during the next save.

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.

3.4.4.2 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.

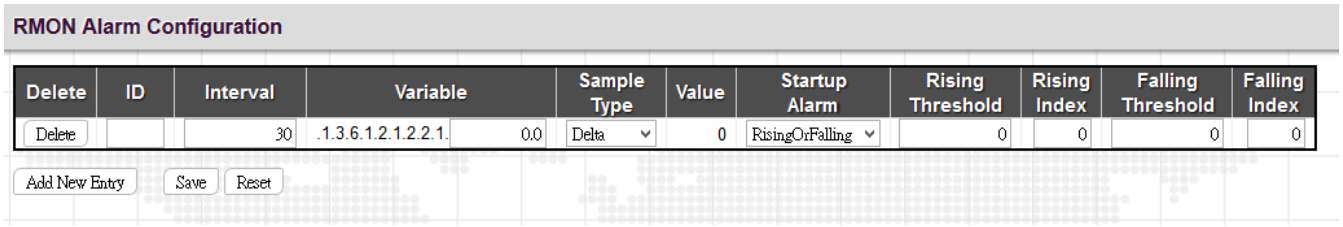
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

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

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

3.4.4.3 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.

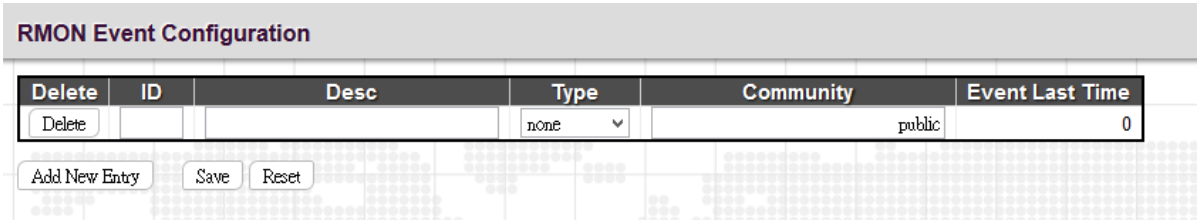
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

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

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

3.4.4.4 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.

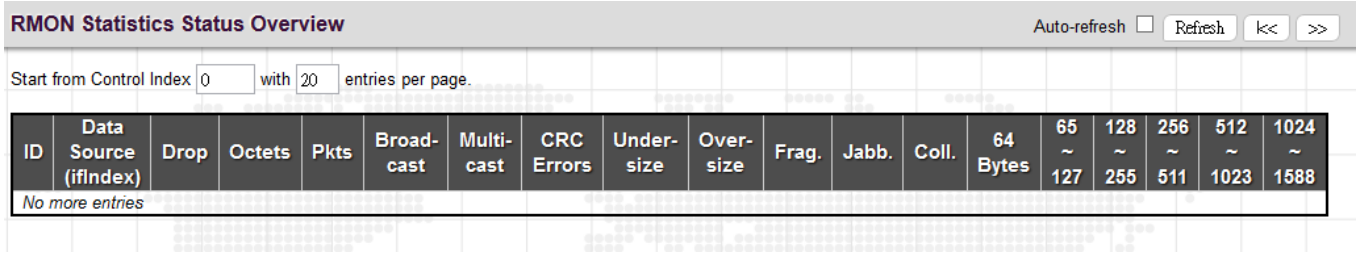
logandtrap: Logs an event and sends a trap message.

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.

3.4.4.5 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.

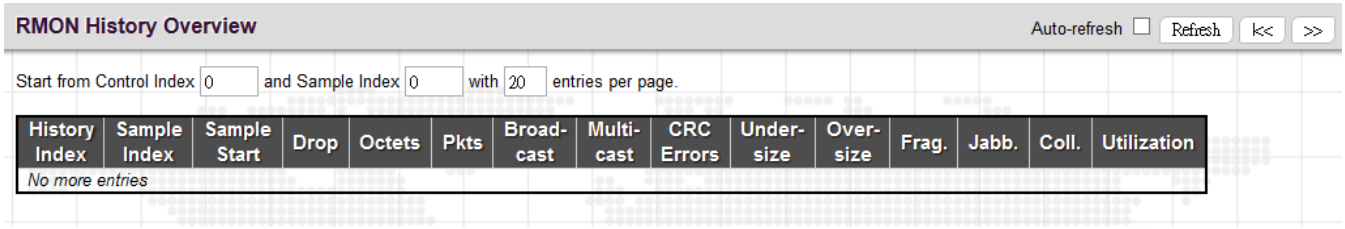
Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

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.

3.4.4.6 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.

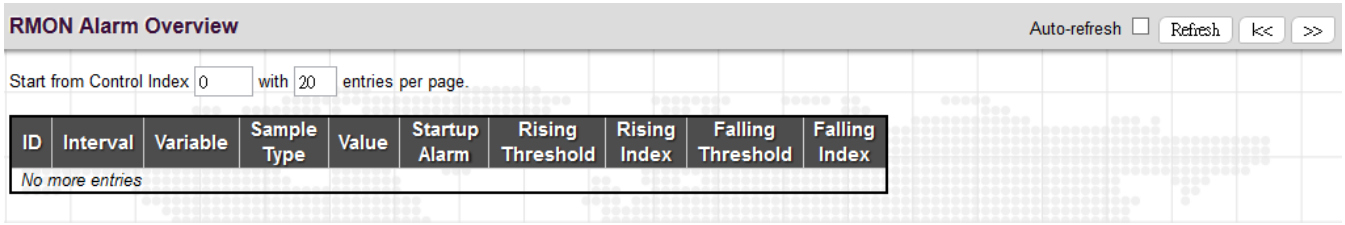
Frag.: The number of frames which size is less than 64 octets received with invalid CRC.

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.

3.4.4.7 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.

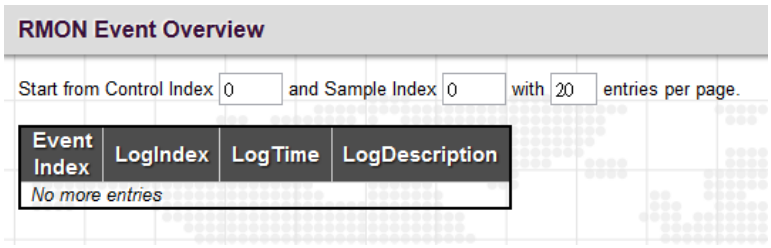
Rising Threshold: If the current value is greater than the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated.

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.

3.4.4.8 Event Overview



Event Index: Display the event entry index.

Log Index: Display the log entry index.

Log Time: Display Event log time.

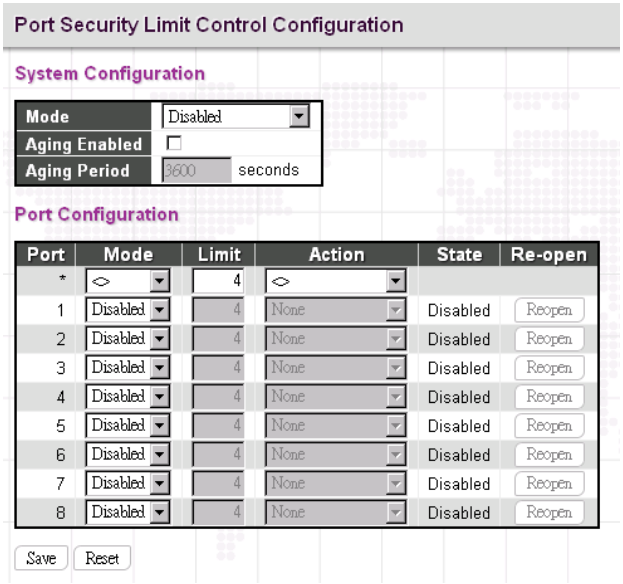
Log Description: Display Event description.

3.4.5 Network

3.5.5.1 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.

3.4.5.1.1 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.

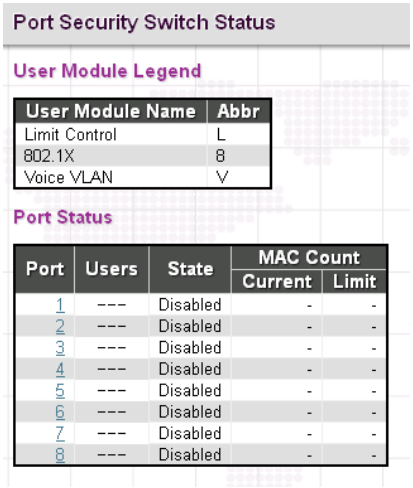
Ready: The limit is not reached yet.

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.

3.4.5.1.2 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: The 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.

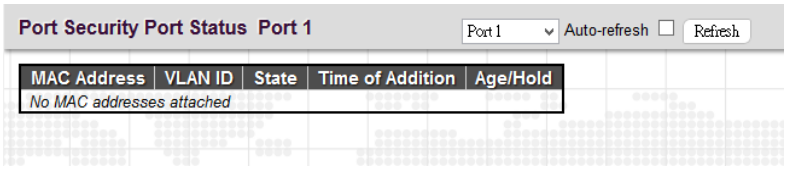
Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

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 (-).

3.4.5.1.3 Port Status



This page shows MAC addresses learned on a particular port.

MAC Address: When "Port Security Limit Control" is enabled globally and on a port, MAC addresses learned on a port show in here.

VLAN ID: Display VLAN ID that is seen on this port.

State: Display whether the corresponding MAC address is forwarding or blocked. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition: Display the date and time when this MAC address was seen on the port.

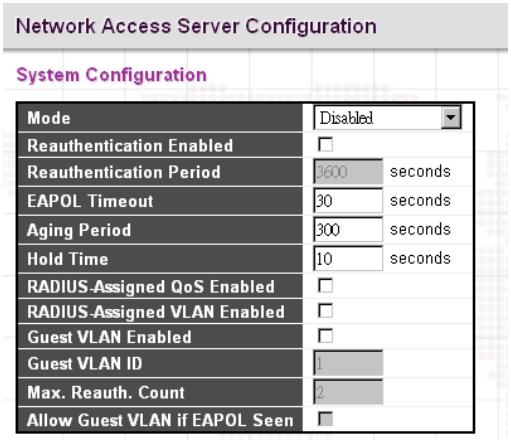
Age/Hold: If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address is still forwarding traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

3.4.5.2 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.

3.4.5.2.1 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.

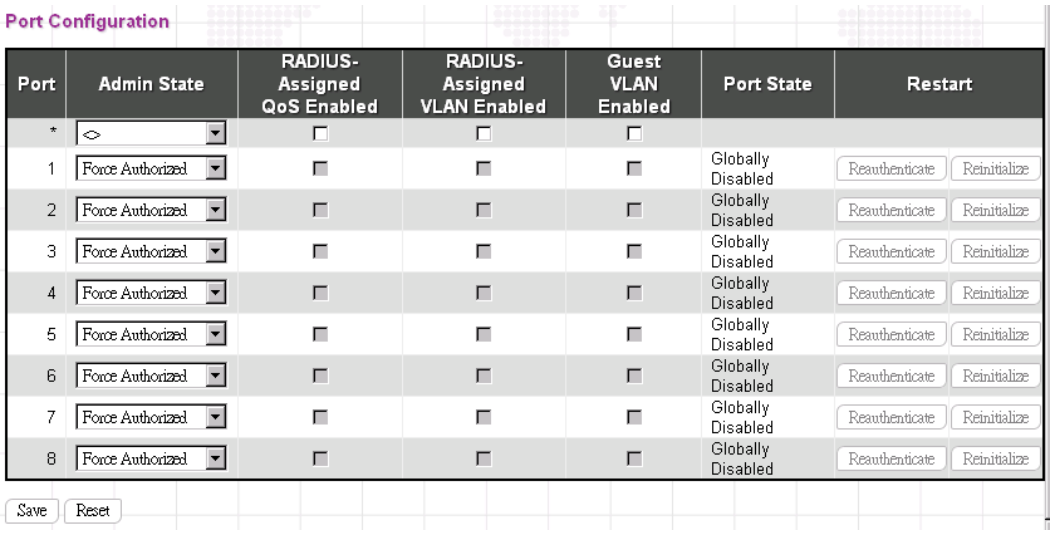
The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled 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	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
*	<>	☐	☐	☐		
1	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
2	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
3	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
4	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
5	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
6	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
7	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
8	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize

Save Reset

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.

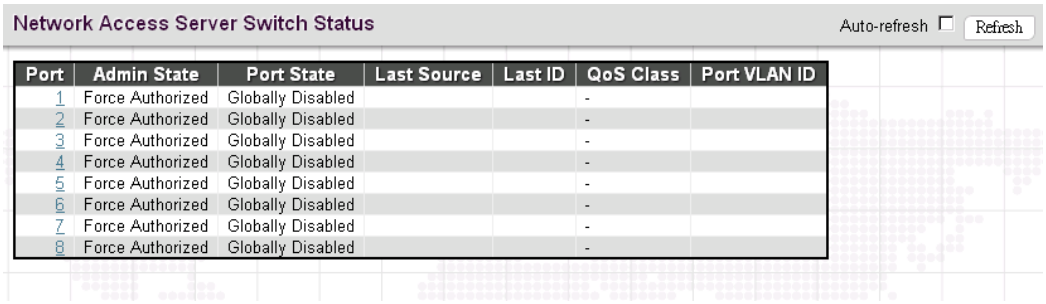
X Auth/Y Unauth: The port is in a multi-supplicant mode. X clients are authorized and Y are unauthorized.

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.

3.4.5.2.2 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			-	

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.

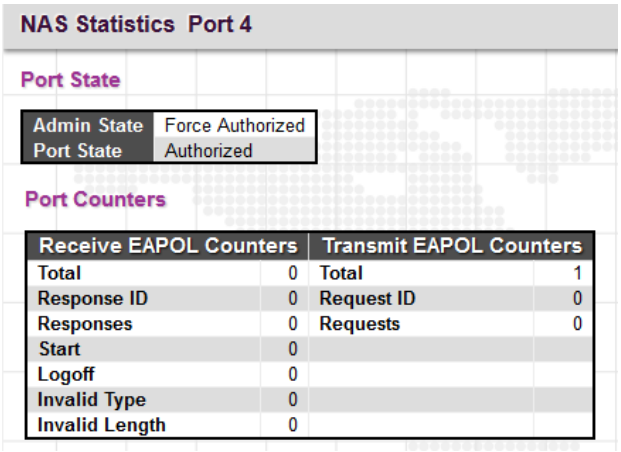
Last Source: The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication.

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.

3.4.5.2.3 Port Statistics



Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	1
Response ID	0	Request ID	0
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		

Port State

Admin State: Display the port's current administrative state.

Port Status: Display the port state.

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.

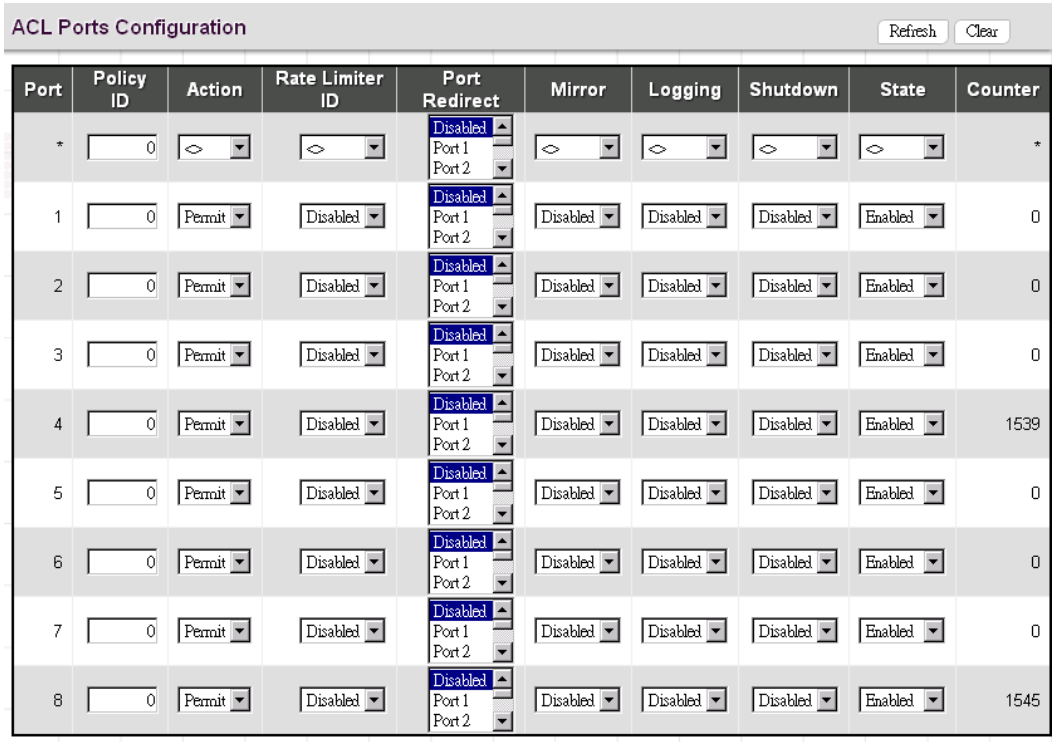
Request ID: The number of valid EAPOL Request Identity frames that have been received by the switch.

Requests: The number of valid EAPOL request frames (other than Request Identity frames) that have been received by the switch.

3.4.5.3 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.

3.4.5.3.1 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.

EVC Policer: Enable or disable EVC Policer on a port. Note that ACL rate limiter and EVC Policer cannot be enabled at the same time.

EVC Policer ID: Select EVC Policer ID to apply to a port. The allowed values are "Disabled" and 1 through 256.

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.

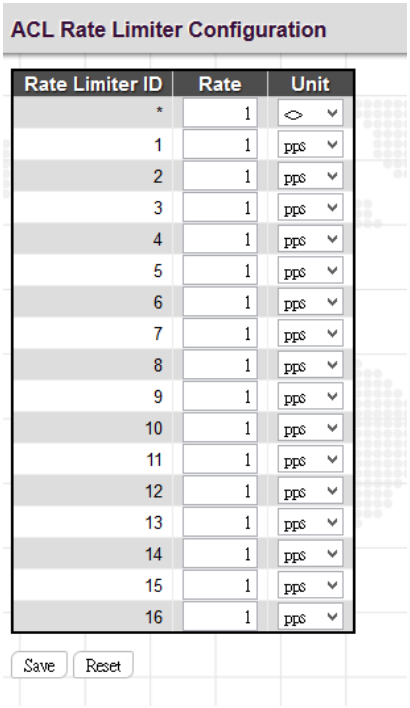
State: Select a port state.

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.

3.4.5.3.2 Rate Limiters



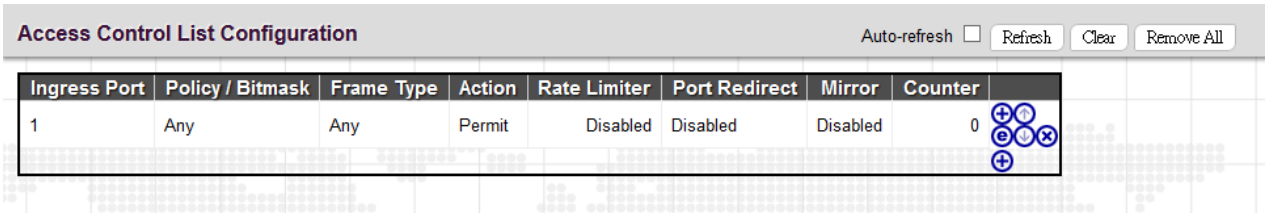
Rate Limiter ID: Display every rate limiter ID.

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.

3.4.5.3.3 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.

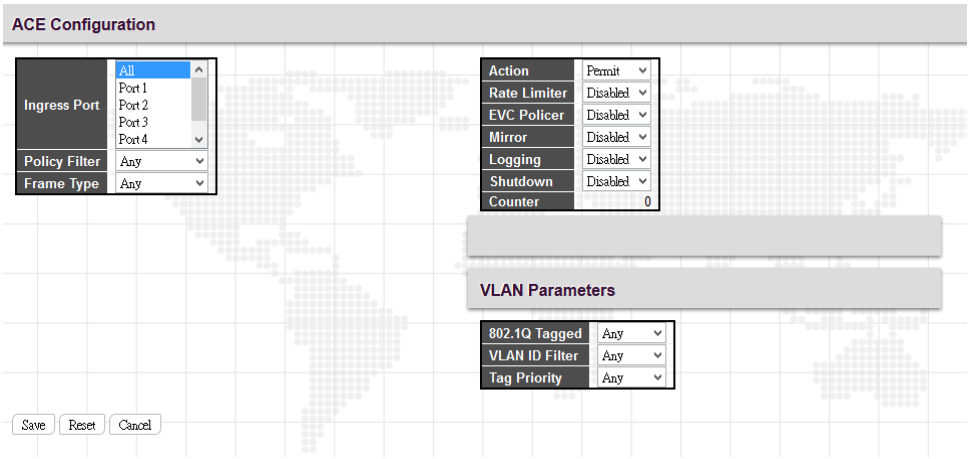
Rate Limiter: Display rate limiter is enabled or disabled when matched frames are found.

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.

EVC Policer: Enable or disable EVC Policer. Note that ACL rate limiter and EVC Policer cannot be enabled at the same time.

EVC Policer ID: When EVC Policer is enabled, you can further select EVC Policer ID. The allowed values are "Disabled" and 1 through 256.

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.

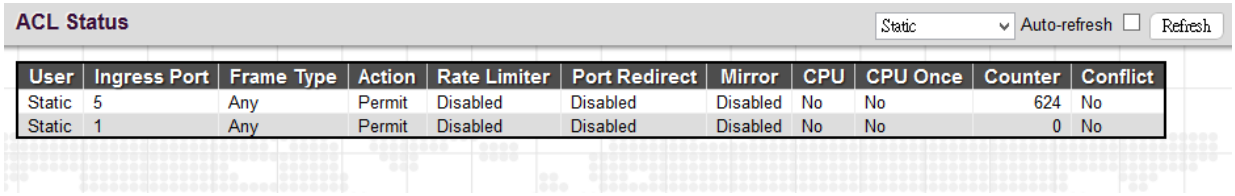
IPv6 Parameters

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.

3.4.5.3.4 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.

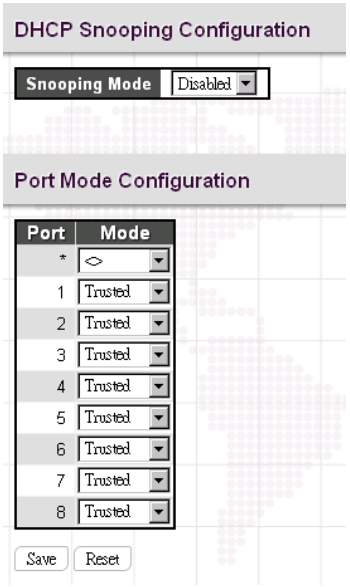
Counter: The counter indicates the number of times the ACE was hit by a frame.

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

3.4.5.4 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.

3.4.5.4.1 Snooping Configuration



DHCP Snooping Configuration

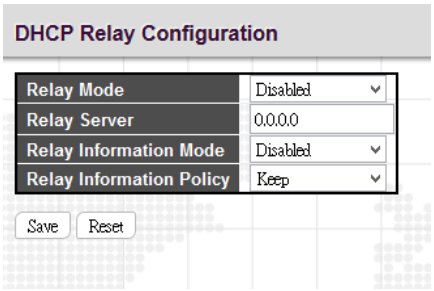
Snooping Mode: Enable or disable DHCP Snooping function globally. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

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”.

3.4.5.4.2 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.

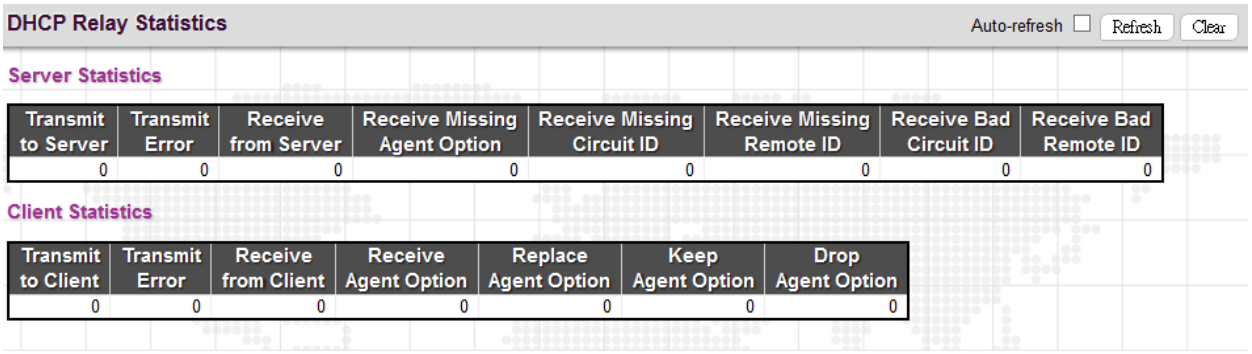
Relay Information Policy: Select Relay Information policy for DHCP client that includes option 82 information.

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.

3.4.5.4.3 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.

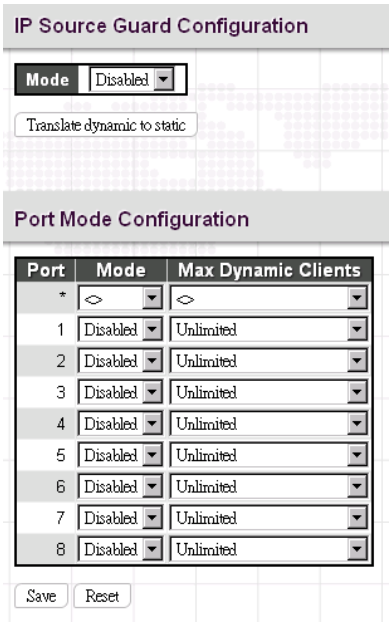
Replace Agent Option: The number of packets which were replaced with relay agent information option.

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.

3.4.5.5 IP Source Guard

3.4.5.5.1 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.

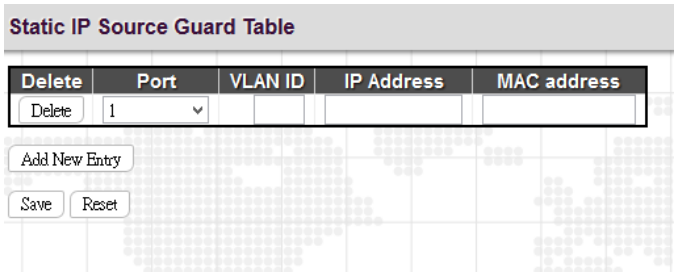
Port Mode Configuration

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.

3.4.5.5.2 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.

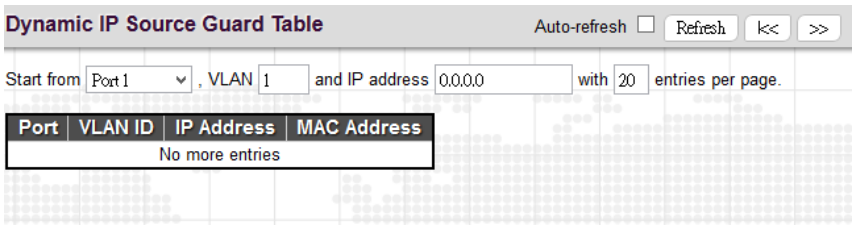
Select the “Delete” checkbox to remove the entry during the next save.

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

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

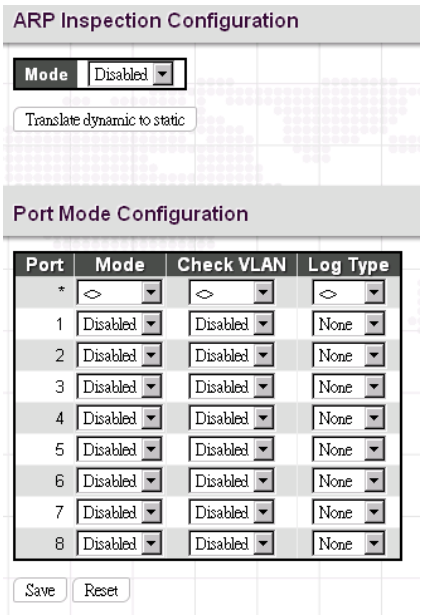
3.4.5.5.3 Dynamic Table

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.



3.4.5.6 ARP inspection

3.4.5.6.1 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.

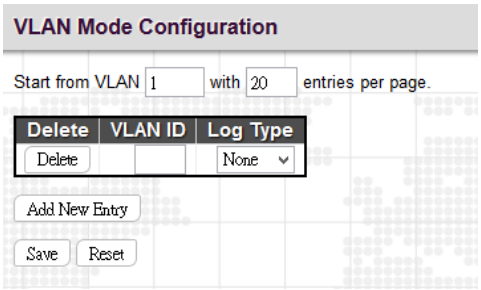
None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

All: Log all entries.

3.4.5.6.2 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.

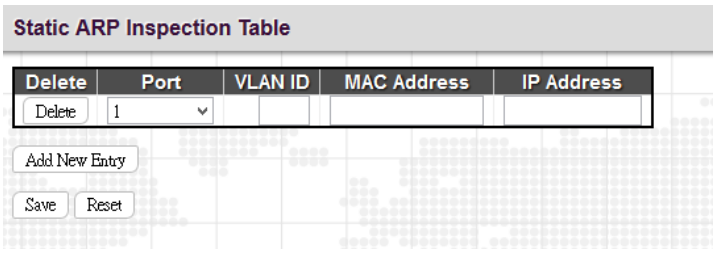
Click the “Add New Entry” button to insert an entry to the table.

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.

3.4.5.6.3 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.

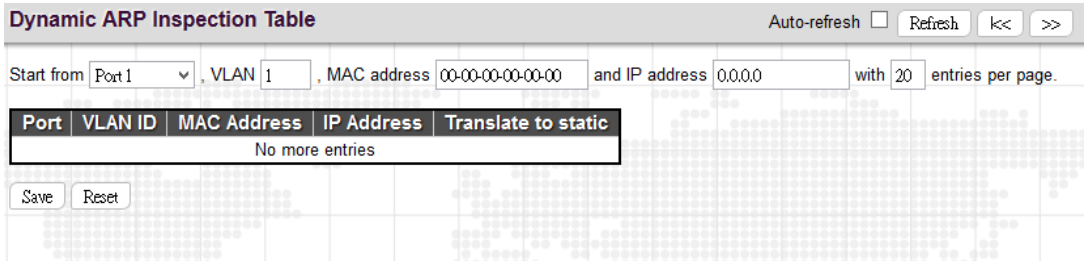
Click the “Add New Entry” button to insert an entry to the table.

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.

3.4.5.6.4 Dynamic Table Configuration



Port: The port number of this entry.

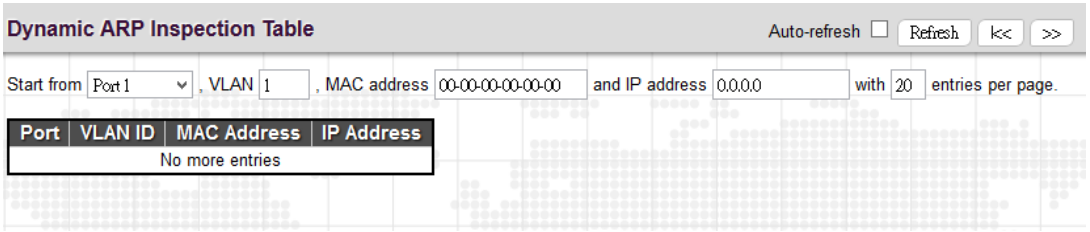
VLAN ID: VLAN ID in which the ARP traffic is permitted.

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.

3.4.5.6.5 Dynamic Table Status



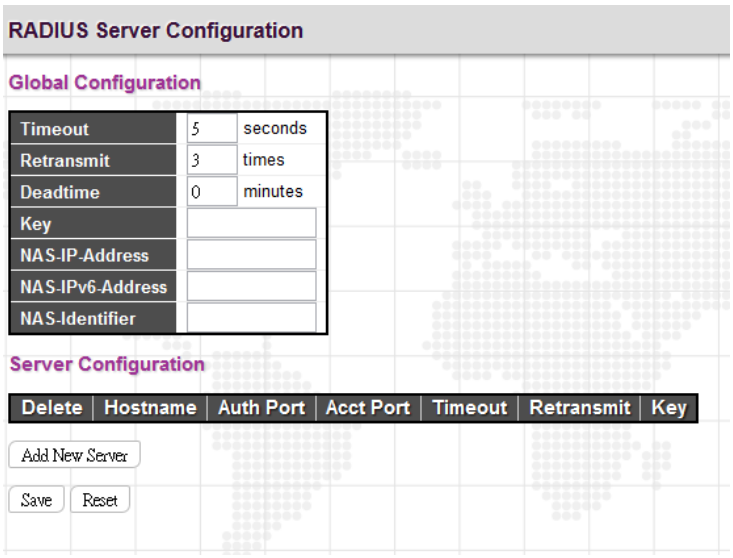
Port: The port number of this entry.

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

MAC Address: User MAC address of this entry.

3.4.6 RADIUS

3.4.6.1 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 1440 minutes.

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

NAS-IP-Address: The IPv4 address is used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-IPv6-Address: The IPv6 address is used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

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

Sever Configuration

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

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

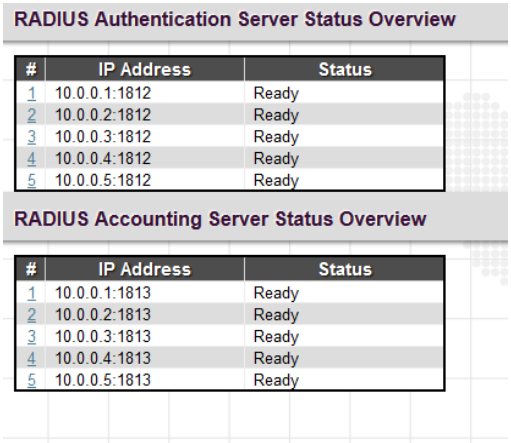
Acct Port: The UDP port to be used on the RADIUS server for accounting.

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

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

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

3.4.6.2 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.

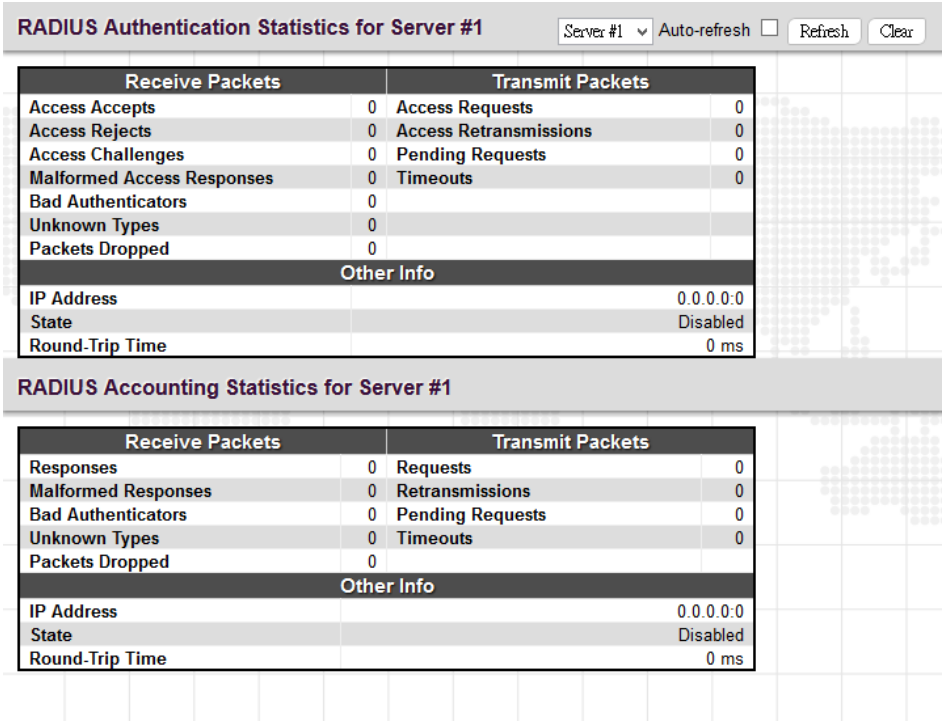
Status: The current state of RADIUS authentication server. Displayed states include the following:

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.

3.4.6.3 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.

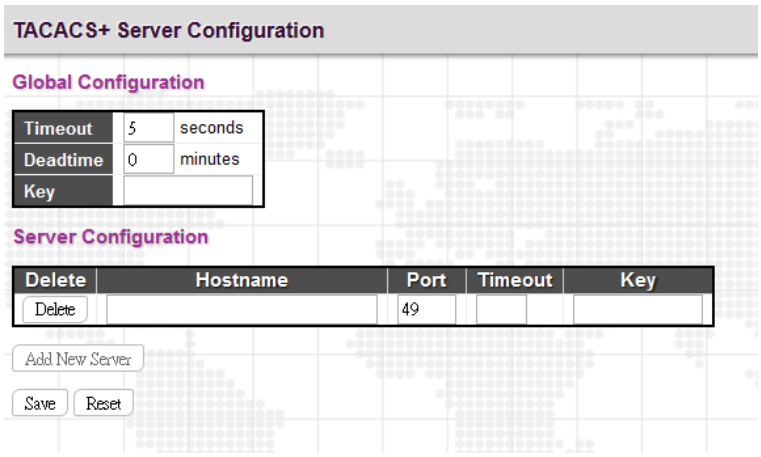
Not Ready: The server is enabled, but IP communication is not yet up and running.

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.

3.4.6.4 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 1440minutes..

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

Server Configuration

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

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

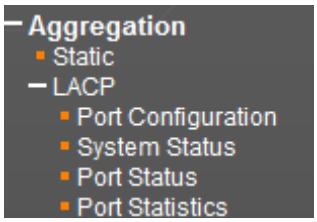
Timeout: If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

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

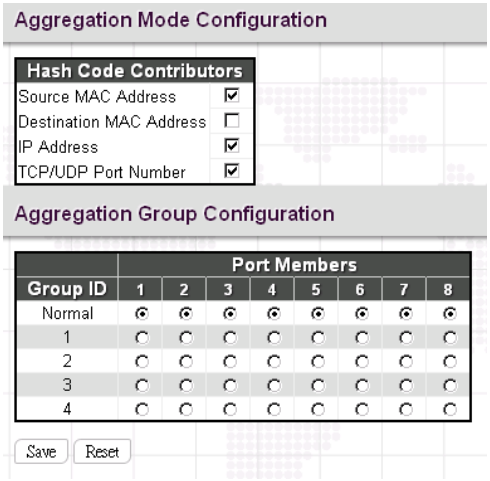
3.5 Aggregation

Compared with adding cost to install extra cables to increase the redundancy and link speed, link aggregation is a relatively inexpensive way to set up a high-speed backbone network that transfers much more data than any one single port or device can deliver. Link aggregation uses multiple ports in parallel to increase the link speed. And there are two types of aggregation that are available, namely “Static” and “LACP”.

Under the Aggregation heading are two major icons, static and LACP.



3.5.1 Static



Aggregation Mode Configuration

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

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

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

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

Aggregation Group Configuration

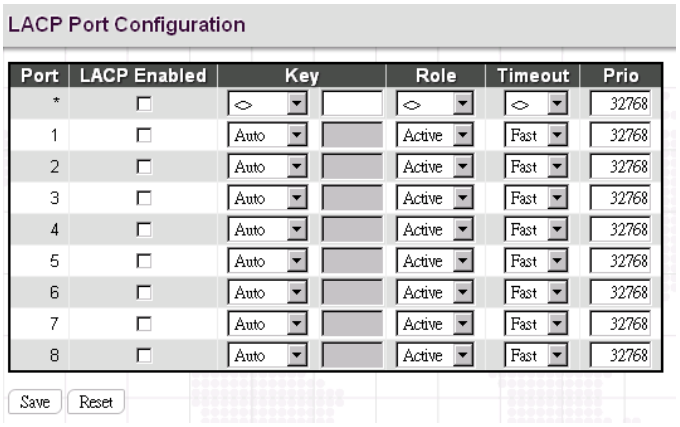
Group ID: Trunk ID number. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group. Two aggregation groups are available for use. Each group contains at least 2 to 5 links (ports). Please note that each port can only be used once in each group.

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

3.5.2 LACP

The Switch supports dynamic Link Aggregation Control Protocol (LACP) which is specified in IEEE 802.3ad. Static trunks have to be manually configured at both ends of the link. In other words, LACP configured ports can automatically negotiate a trunked link with LACP configured ports on another devices. You can configure any number of ports on the Switch as LACP, as long as they are not already configured as part of a static trunk. If ports on other devices are also configured as LACP, the Switch and the other devices will negotiate a trunk link between them.

3.5.2.1 Port Configuration



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

LACP Enabled: Enable LACP on a switch port.

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

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

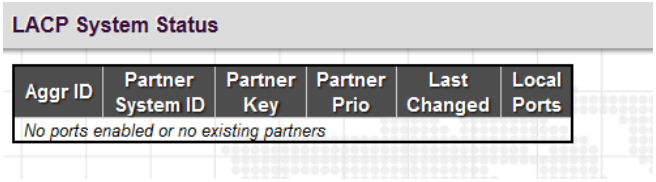
Ports that are designated as "Active" are able to process and send LACP control frames. Hence, this allows LACP compliant devices to negotiate the aggregated like so that the group may be changed dynamically as required. In order to add or remove ports from the group, at least one of the participating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

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

Timeout: The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

Prio: The priority of the port. The lower number means greater priority. This priority value controls which ports will be active and which ones will be in a backup role.

3.5.2.2 System Status



Aggr ID: Display the aggregation ID associated with the Link Aggregation Group (LAG).

Partner System ID: LAG's partner system ID (MAC address).

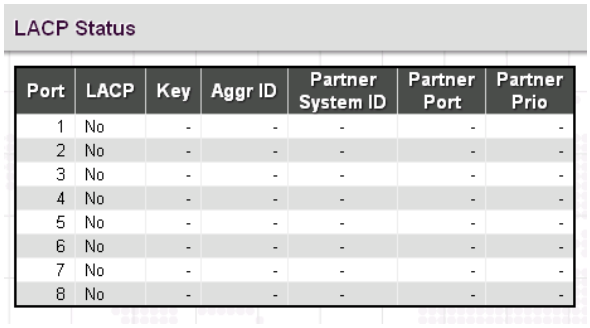
Partner Key: The partner key assigned to this LAG.

Partner Prio: The priority value of the partner.

Last Changed: The time since this LAG changed.

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

3.5.2.3 Port Status



Port: The port number.

LACP: Show LACP status on a port.

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

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

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

Key: The aggregation key value on a port.

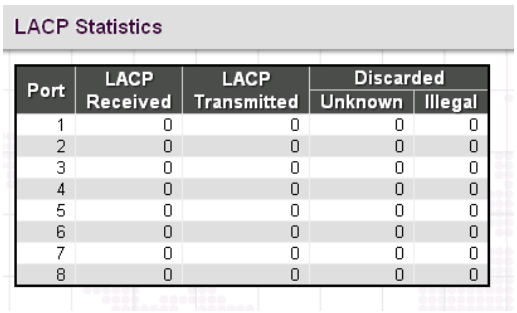
Aggr ID: Display the aggregation ID active on a port.

Partner System ID: LAG partner's system ID.

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

Partner Prio: The priority value of the partner.

3.5.2.4 Port Statistics


LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0

Port: The port number.

LACP Received: The number of LACP packets received on a port.

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

Discarded: The number of unknown and illegal packets that have been discarded on a port.

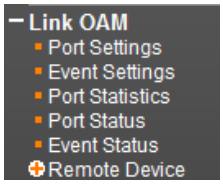
3.6 Link OAM

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

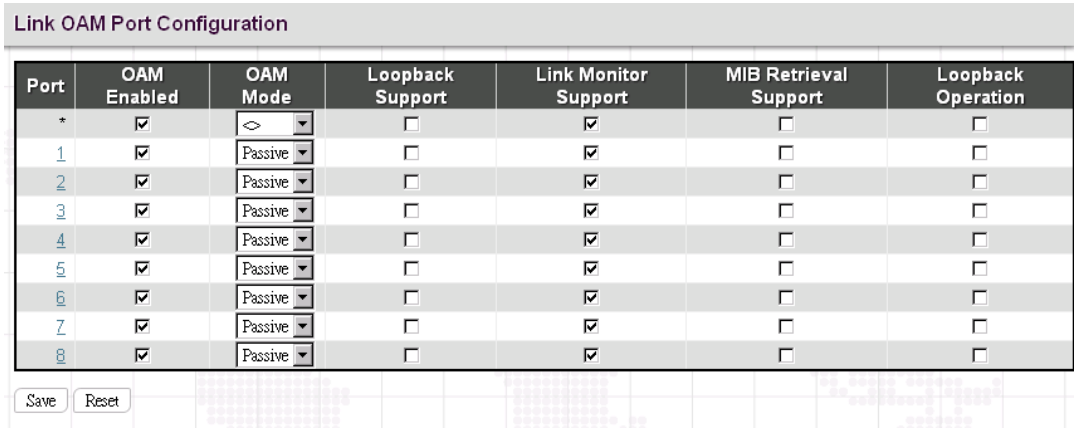
IEEE 802.3ah provides the following features:

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

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



3.6.1 Port Settings



Port: The port number. Click on the port to view its OAM status details.

OAM Enabled: Select the checkbox to enable OAM function on a port. Clear the checkbox to disable OAM.

OAM Mode: Select the OAM mode on a per port basis. The default mode is "Passive".

Active: The device set in Active mode initiates the exchange of Information OAMPDUs

Passive: The device in Passive mode does not initiate the Discovery process but reacts to the initiation of the Discovery process by the remote 802.3ah-enabled device.

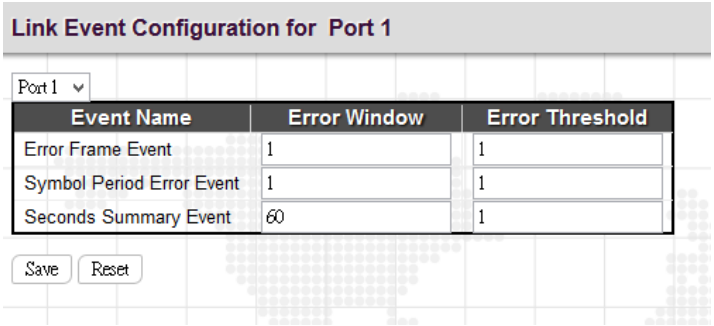
Loopback Support: Select the checkbox to enable loopback support on a port. Link OAM remote loopback support can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection.

Link Monitor Support: Select the checkbox to enable link monitor support. Once enabled, the DTE supports event notification that permits the inclusion of diagnostic information.

MIB Retrieval Support: Select the checkbox to enable MIB retrieval support. Once enabled, the DTE supports polling of various link OAM based MIB variables' contents.

Loopback Operation: If the "Loopback Support" is enabled, selecting the "Loopback Operation" checkbox will start a loopback operation for the port.

3.6.2 Event Settings



Link Event can be configured on a per-port basis. Select the desire port number from the pull-down menu to configure its Link Event settings.

Event Name: Ethernet OAM entities monitor link status by exchanging Event Notification OAMPDUs. When one of the events listed here is detected, an OAM entity sends an Event Notification OAMPDU to its peer OAM entity.

Error Frame Event: The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-0xffffffff and its default value is '0'.

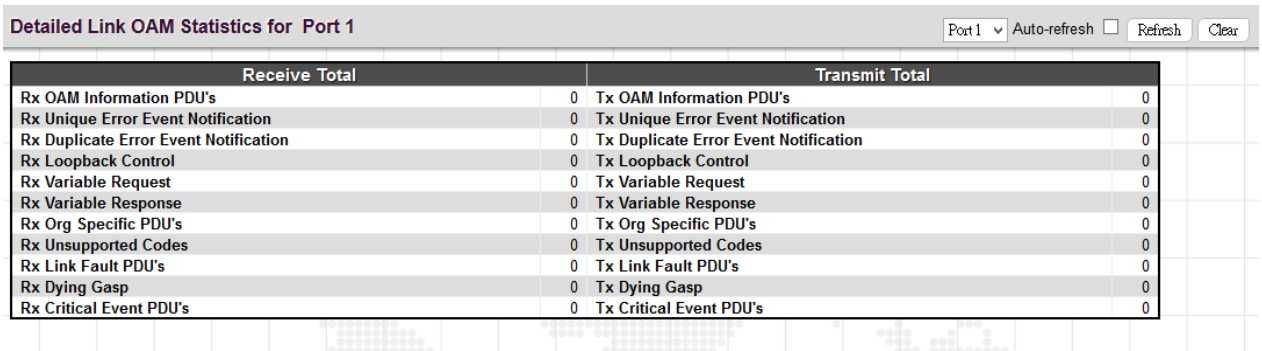
Symbol Period Error Event: The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-0xffffffff and its default value is '0'.

Seconds Summary Event: The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10-900 and its default value is '60'. Whereas Error Threshold must be between 0-0xffff and its default value is '1'.

Error Window: Specify the window period in the order of 1 sec for the observation of various link events.

Error Threshold: Specify the error threshold value for the window period for the appropriate Link event so as to notify the peer of this error.

3.6.3 Port Statistics



Rx & Tx OAM Information PDU's: The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.

Rx & Tx Unique Error Event Notification: A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as

an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

Rx & Tx Duplicate Error Event Notification: A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

Rx & Tx Loopback Control: The number of Loopback Control OAMPDUs received and transmitted on this interface.

Rx & Tx Variable Request: The number of Variable Request OAMPDUs received and transmitted on this interface.

Rx & Tx Variable Response: The number of Variable Response OAMPDUs received and transmitted on this interface.

Rx & Tx Org Specific PDU's: The number of Organization Specific OAMPDUs transmitted on this interface.

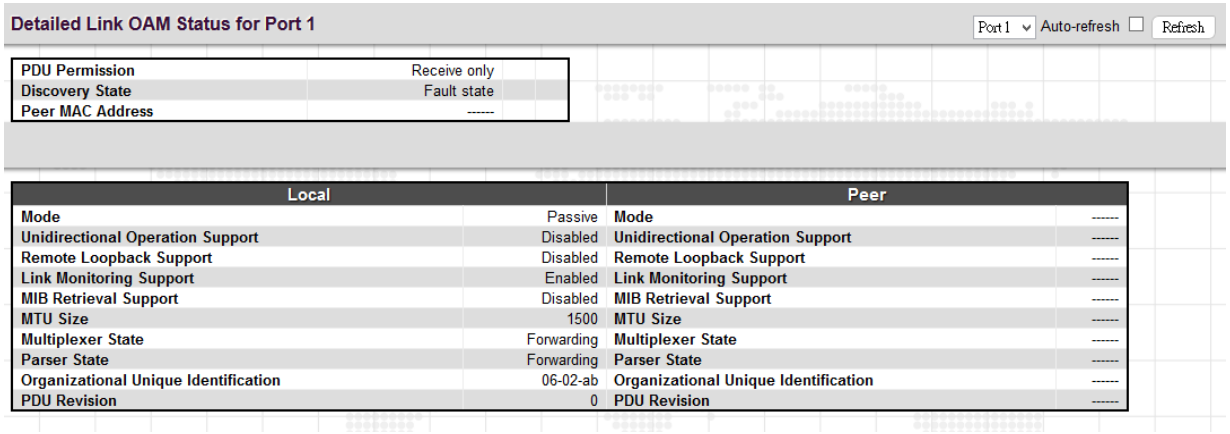
Rx & Tx Unsupported Codes: The number of OAMPDUs transmitted on this interface with an unsupported op-code.

Rx & Tx Link fault PDU's: The number of Link fault PDU's received and transmitted on this interface.

Rx & Tx Dying Gasp: The number of Dying Gasp events received and transmitted on this interface.

Rx & Tx Critical Event PDU's: The number of Critical event PDU's received and transmitted on this interface.

3.6.4 Port Status



Detailed Link OAM Status

PDU Permission: Displays the current permission rules set for the local DTE. Possible values are "Link fault", "Receive only", "Information exchange only", "ANY".

Discovery State: Displays the current state of the discovery process. Possible states are Fault state, Active state, Passive state, SEND_LOCAL_REMOTE_STATE, SEND_LOCAL_REMOTE_OK_STATE, SEND_ANY_STATE.

Peer MAC Address: Displays the MAC address of the peer device.

Local & Peer

Mode: This field shows the Mode in which the Link OAM is operating, Active or Passive.

Unidirectional Operation Support: This feature is not available to be configured by the user. The status of this configuration is retrieved from the PHY.

Remote Loopback Support: If status is enabled, the device is capable of OAM remote loopback mode.

Link Monitoring Support: If status is enabled, the device supports interpreting Link Events.

MIB Retrieval Support: If status is enabled, the device supports sending Variable Response OAMPDUs.

MTU Size: It represents the largest OAMPDU, in octets, supported by the device. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.

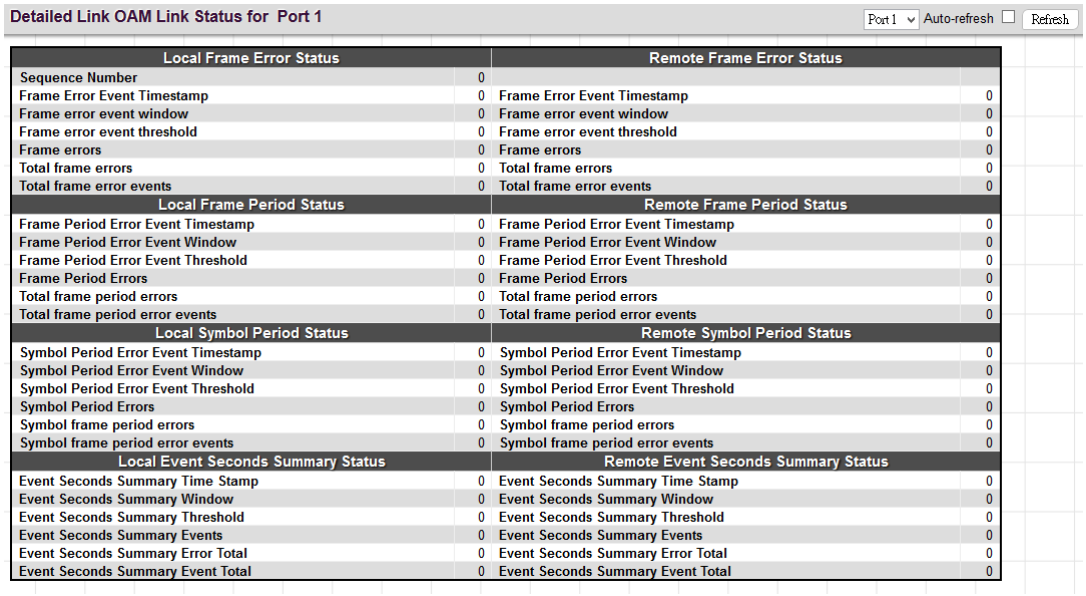
Multiplexer State: When in forwarding state, the device is forwarding non-OAMPDUs to the lower sub-layer. In case of discarding, the device discards all the non-OAMPDU's.

Parser State: When in forwarding state, the device is forwarding non-OAMPDUs to higher sub-layer. When in loopback, the device is looping back non-OAMPDUs to the lower sub-layer. When in discarding state, the device is discarding non-OAMPDUs.

Organizational Unique Identification: 24-bit Organizationally Unique Identifier of the vendor.

PDU Revision: It indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).

3.6.5 Event Status



Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0		
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame error event window	0	Frame error event window	0
Frame error event threshold	0	Frame error event threshold	0
Frame errors	0	Frame errors	0
Total frame errors	0	Total frame errors	0
Total frame error events	0	Total frame error events	0
Local Frame Period Status		**Remote Frame Period Status**	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		**Remote Symbol Period Status**	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Symbol frame period errors	0	Symbol frame period errors	0
Symbol frame period error events	0	Symbol frame period error events	0
Local Event Seconds Summary Status		**Remote Event Seconds Summary Status**	
Event Seconds Summary Time Stamp	0	Event Seconds Summary Time Stamp	0
Event Seconds Summary Window	0	Event Seconds Summary Window	0
Event Seconds Summary Threshold	0	Event Seconds Summary Threshold	0
Event Seconds Summary Events	0	Event Seconds Summary Events	0
Event Seconds Summary Error Total	0	Event Seconds Summary Error Total	0
Event Seconds Summary Event Total	0	Event Seconds Summary Event Total	0

Local & Remote Frame Error Status

Sequence Number: This two-octet field indicates the total number of events occurred at the remote end.

Frame Error Event Timestamp: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame error event window: This two-octet field indicates the duration of the period in terms of 100 ms intervals. 1) The default value is one second. 2) The lower bound is one second. 3) The upper bound is one minute.

Frame error event threshold: This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be generated. 1) The default value is one frame error. 2) The lower bound is zero frame errors. 3) The upper bound is unspecified.

Frame errors: This four-octet field indicates the number of detected errored frames in the period.

Total frame errors: This eight-octet field indicates the sum of errored frames that have been detected since the OAM sub-layer was reset.

Total frame error events: This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset.

Local & Remote Frame Period Status

Frame Period Error Event Timestamp: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame Period Error Event Window: This four-octet field indicates the duration of period in terms of frames.

Frame Period Error Event Threshold: This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.

Frame Period Errors: This four-octet field indicates the number of frame errors in the period.

Total frame period errors: This eight-octet field indicates the sum of frame errors that have been detected since the OAM sub-layer was reset.

Total frame period error events: This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sub-layer was reset.

Local & Remote Symbol Period Status

Symbol Period Error Event Timestamp: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Symbol Period Error Event Window: This eight-octet field indicates the number of symbols in the period.

Symbol Period Error Event Threshold: This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated.

Symbol Period Errors: This eight-octet field indicates the number of symbol errors in the period.

Symbol frame period errors: This eight-octet field indicates the sum of symbol errors since the OAM sub-layer was reset.

Symbol frame period error events: This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sub-layer was reset.

Local & Remote Event Seconds Summary Status

Event Seconds Summary Time Stamp: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Event Seconds Summary Window: This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

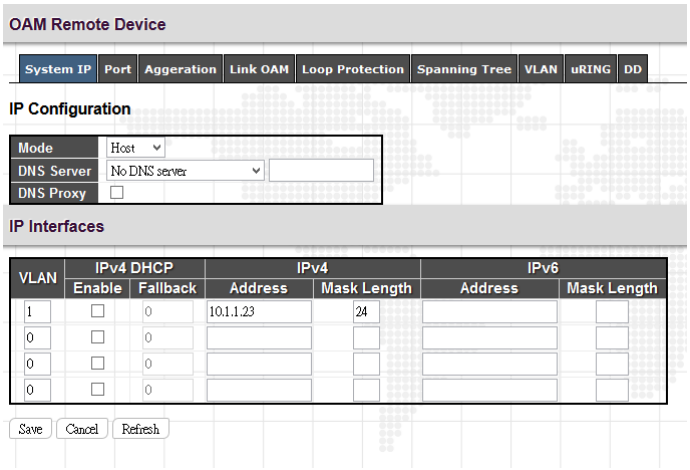
Event Seconds Summary Threshold: This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer.

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

Event Seconds Summary Error Total: This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sub-layer was reset.

Event Seconds Summary Event Total: This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sub-layer was reset, encoded as a 32bit unsigned integer.

3.6.6 Remote Device

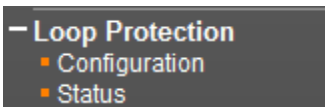


This device enables users to configure features of the remote FRM220-MSW404 device using proprietary in-band management protocol. To do so, the local FRM220-MSW404 device must be set to “Active” mode. The remote device can be set to either “Active” or “Passive” mode. Once two devices are successfully connected, click on the “Remote A”, “Remote B”, “Remote C” or “Remote D” option on the left function menu in local FRM220-MSW404 device. Then, the screen same as above will appear.

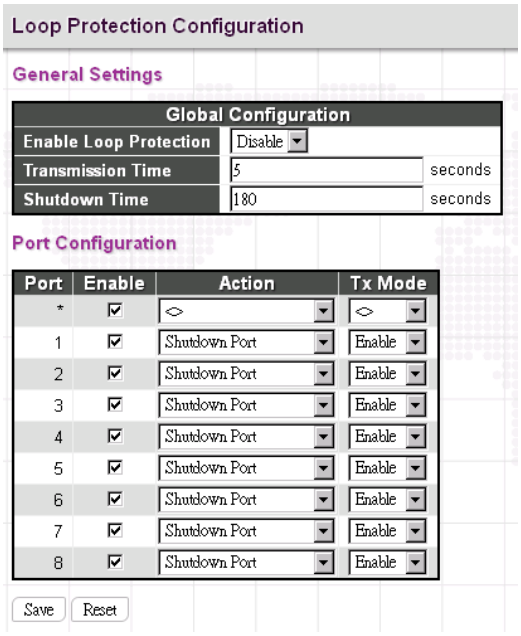
NOTE: *Apart from the method described above to manage the remote FRM220-MSW404 device in local side, both local and remote FRM220-MSW404 devices can also be managed via NMC card in FRM220 chassis. However, using this method only enables the NMC to manage two remote devices that are connected with the slide-in local FRM220-MSW404 via fiber optical cables. For detailed descriptions about proprietary in-band management via FRM 220 chassis, please refer to FRM220 user manual.*

3.7 Loop Protection

Loops sometimes occur in a network due to improper connecting, hardware problem or faulty protocol settings. When loops are seen in a switched network, they consume switch resources and thus downgrade switch performance. Loop Protection feature is provided in this switch and can be enabled globally or on a per port basis. Using loop protection enables the switch to automatically detect loops on a network. Once loops are detected, ports received the loop protection packet form the switch can be shut down or loopped events can be logged.



3.7.1 Configuration



General Settings

Enable Loop Protection: Enable or disable loop protection function.

Transmission Time: The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.

Shutdown Time: The period for which a port will be kept disabled. Valid values are 0 to 604800 seconds. 0 means that a port is kept disabled until next device restart.

Port Configuration

Port: List the number of each port. “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”.

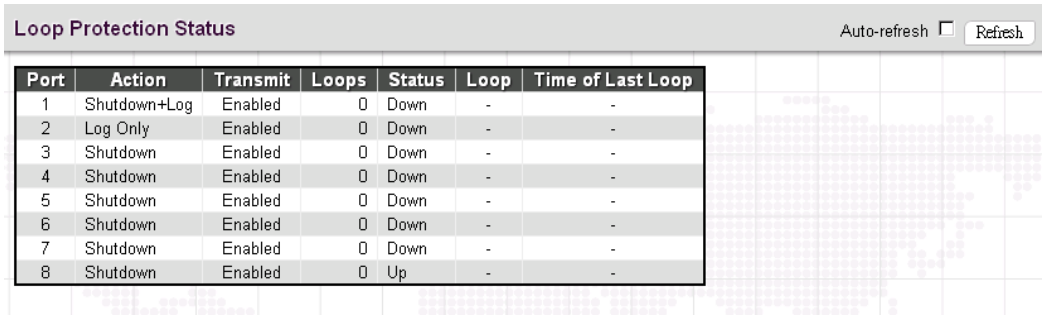
Shutdown Port: A loop-detected port is shutdown for a period of time configured in “Shutdown Time”.

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.

3.7.2 Status



Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown+Log	Enabled	0	Down	-	-
2	Log Only	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Up	-	-

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.

3.8 Spanning Tree

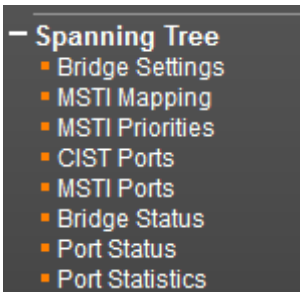
For some networking services, always-on connections are required to ensure that end users' online related activities are not interrupted due to unexpected disconnections. In these circumstances, multiple active paths between network nodes are established to prevent disconnections from happening. However, multiple paths interconnected with each other have a high tendency to cause bridge loops that make networks unstable and in worst cases make networks unusable. For example, the MAC address table used by the switch or bridge can fail, since the same MAC addresses (and hence the same network hosts) are seen on multiple ports. Second, a broadcast storm occurs. This is caused by broadcast packets being forwarded in an endless loop between switches. A broadcast storm can consume all available CPU resources and bandwidth.

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

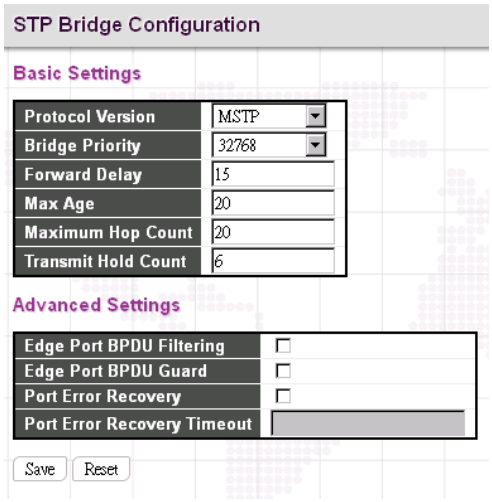
The Spanning Tree Protocol (STP), defined in the IEEE Standard 802.1s, can create a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches) and disable the links which are not part of that tree, leaving a single active path between any two network nodes.

To provide faster spanning tree convergence after a topology change, an evolution of the Spanning Tree Protocol "Rapid Spanning Tree Protocol (RSTP)", is introduced by IEEE 802.1w. RSTP is a refinement of STP; therefore, it shares most of its basic operation characteristics. This essentially creates a cascading effect away from the root bridge where each designated bridge proposes to its neighbors to determine if it can make a rapid transition. This is one of the major elements which allows RSTP to achieve faster convergence times than STP.

The other extension of RSTP is IEEE 802.1s Multiple Spanning Tree protocol (MSTP) that allows different VLANs to travel along separate instances of spanning tree. Unlike STP and RSTP, MSTP eliminates the needs for having different STP for each VLAN. Therefore, in a large networking environment that employs many VLANs, MSTP can be more useful than legacy STP.



3.8.1 Bridge Settings



Basic Settings

Protocol Version: Select the appropriate spanning tree protocol. Protocol versions provided include "STP", "RSTP", and "MSTP".

Bridge Priority: Each switch has a relative priority and cost that is used to decide what the shortest path is to forward a packet. The lowest cost path (lowest numeric value) has a higher priority and is always used unless it is down. If you have multiple bridges and interfaces then you need to adjust the priorities to achieve optimized performance. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Forward Delay: Fort STP bridges, the Forward Delay is the time spent in each Listening and Learning state before the Forwarding state is entered. This delay occurs when a new bridge comes onto a network. Valid values are 4-30 seconds.

Max Age: If another switch in the spanning tree does not send out a hello packet for a period of time, it is considered to be disconnected. Valid values are 6 to 40 seconds, and Max Age values must be smaller than or equal to (Forward Delay-1)*2.

Maximum Hop Count: The maximum number of hops allowed for MST region before a BPDU is discarded. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the BPDU is discarded. The default hop count is 20. The allowed range is 6-40.

Transmit Hold Count: The number of BPDU sent by a bridge port per second. When exceeded, transmission of the next BPDU will be delayed. By default, it is set to 6. The allowed transmit hold count is 1 to 10. Please note that increasing this value might have a significant impact on CPU utilization and decreasing this value might slow down convergence. It is recommended to remain Transmit Hold Count to the default setting.

Advanced Settings

Edge Port BPDU Filtering: The purpose of Port BPDU Filtering is to prevent the switch from sending BPDU frames on ports that are connected to end devices.

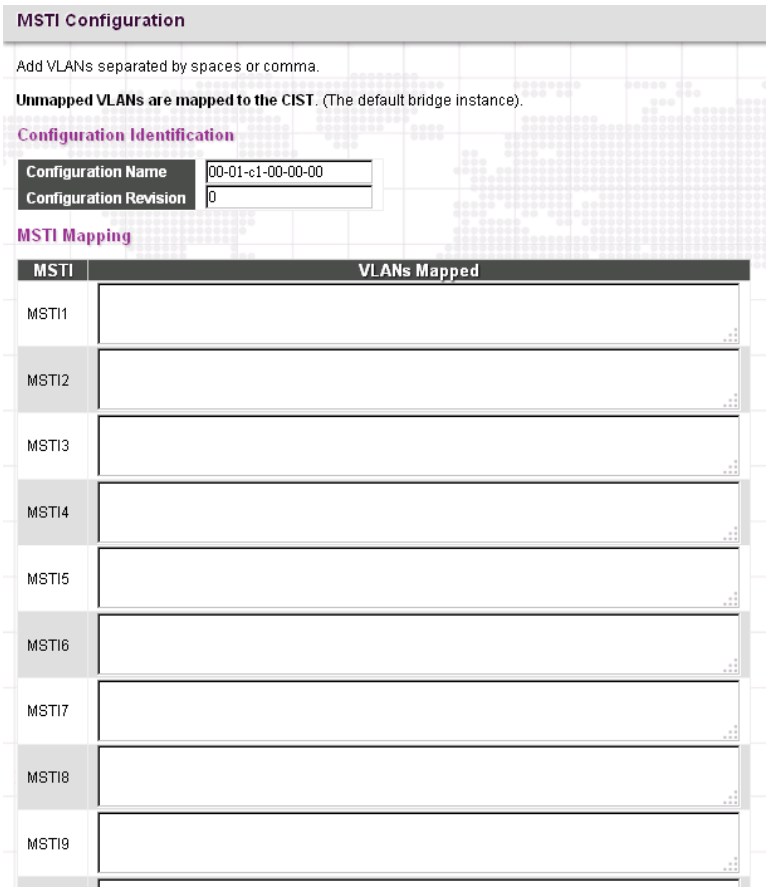
Edge Port BPDU Guard: Edge ports generally connect directly to PC, file servers or printers. Therefore, edge ports are configured to allow rapid transition. Under normal situations, edge ports should not receive configuration BPDUs. However, if they do, this probably is due to malicious attacks or mis-settings. When edge ports receive configuration BPDUs, they will be automatically set to non-edge ports and start a new spanning tree calculation process.

BPDU Guard is therefore used to prevent the device from suffering malicious attacks. With this function enabled, when edge ports receive configuration BPDUs, STP disables those affected edge ports. After a period of recovery time, those disabled ports are re-activated.

Port Error Recovery: When enabled, a port that is in the error-disabled state can automatically be enabled after a certain time.

Port Error Recovery Timeout: The time that has to pass before a port in the error-disabled state can be enabled. The allowed range is 30 – 86400 seconds.

3.8.2 MSTI Mapping



Configuration Identification

Configuration Name: The name for this MSTI. By default, the switch's MAC address is used. The maximum length is 32 characters. In order to share spanning trees for MSTI, bridges must have the same configuration name and revision value.

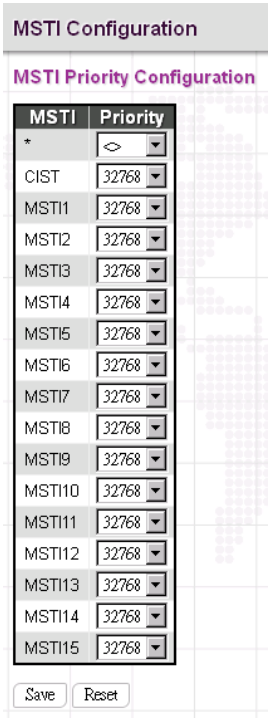
Configuration Revision: The revision number for this MSTI. The allowed range is 0~65535.

MSTI Mapping

MSTI: MSTI instance number.

VLAN Mapped: Specify VLANs mapped to a certain MSTI. Both a single VLAN and a range of VLANs are allowed. Separate VLANs with a comma and use hyphen to denote a range of VLANs. (Example: 2,5,20-40) Leave the field empty for unused MSTI.

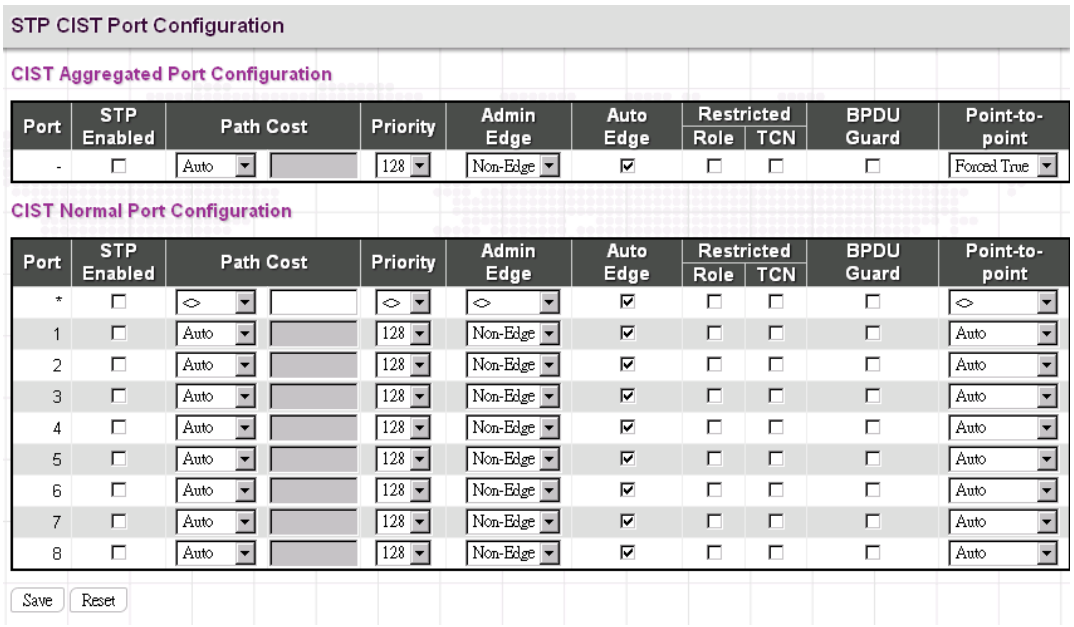
3.8.3 MSTI Priorities



MSTI: Display MSTI instance number. "MSTI *" priority rule applies to all ports.

Priority: Select an appropriate priority for each MSTI instance. Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Note that lower numeric values indicate higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

3.8.4 CIST Ports



CIST Aggregated Port Configuration

Port: The port number.

STP Enabled: Enable STP function

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

Priority: Select port priority.

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

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

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

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

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

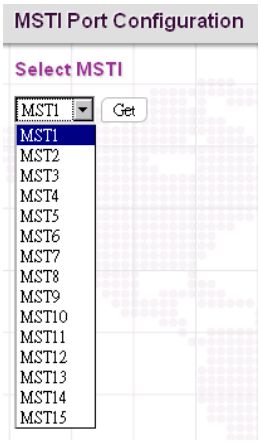
Point-to-Point: Select the link type attached to an interface.

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

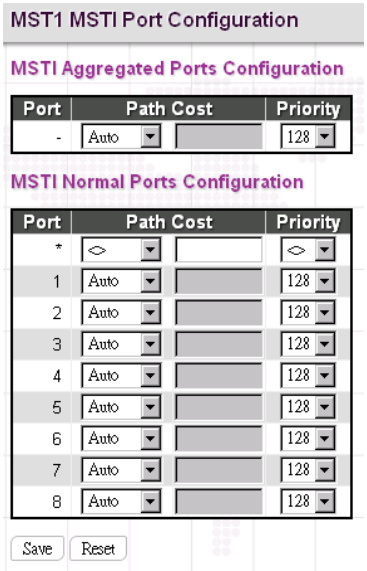
Forced True: It is a point-to-point connection.

Forced False: It is a shared medium connection.

3.8.5 MSTI Ports



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

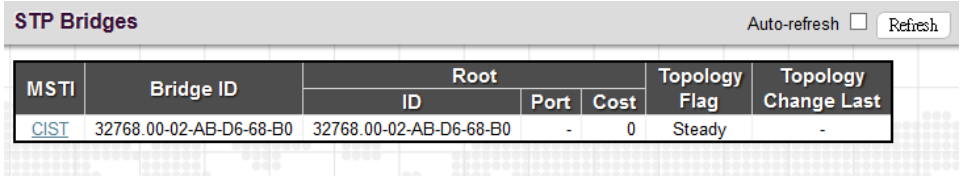


Port: The port number.

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

Priority: Select port priority.

3.8.6 Bridge Status



STP Bridge

MSTI: The bridge instance. Click this instance to view STP detailed bridge status.

Bridge ID: The unique bridge ID for this instance consisting a priority value and MAC address of the bridge switch.

Root ID: Display the root device's priority value and MAC address.

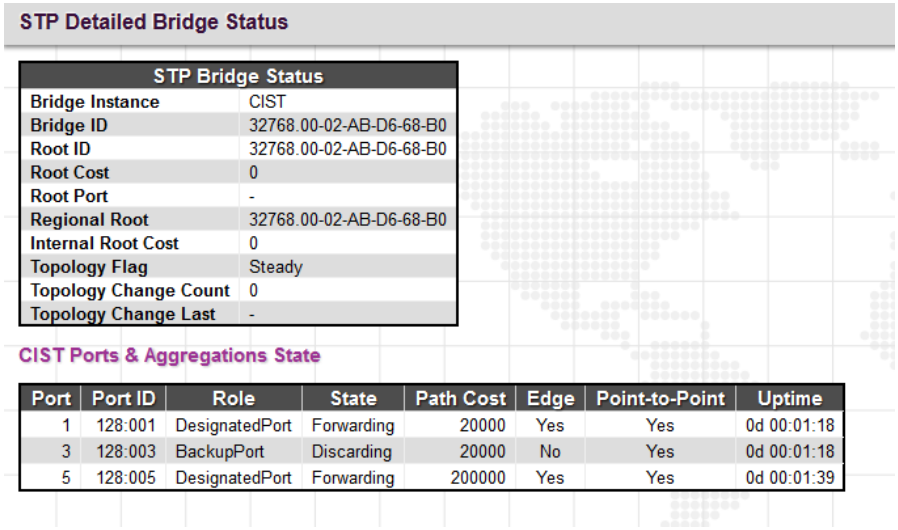
Root Port: The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

Root Cost: The path cost from the root port on the switch to the root device. For the root bridge this is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.

Topology Flag: The current state of the Topology Change Notification flag for this bridge instance.

Topology Change Last: The time since this spanning tree was last configured.

Click the MSTI instance to view STP detailed bridge status.



STP Detailed Bridge Status

Bridge Instance: The bridge instance.

Bridge ID: The unique bridge ID for this instance consisting a priority value and MAC address of the bridge switch.

Root ID: Display the root device's priority value and MAC address.

Root Cost: The path cost from the root port on the switch to the root device. For the root bridge this is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.

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

Regional Root: The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (This parameter only applies to the CIST instance.)

Internal Root Cost: The Regional Root Path Cost. For the Regional Root Bridge the cost is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (This parameter only applies to the CIST instance.)

Topology Flag: The current state of the Topology Change Notification flag for this bridge instance.

Topology Change Last: The time since this spanning tree was last configured.

CIST Ports & Aggregations State

Port: Display the port number.

Port ID: The port identifier used by the RSTP protocol. This port ID contains the priority and the port number.

Role: The role assigned by Spanning Tree Algorithm. Roles can be “Designated Port”, “Backup Port”, “Root Port”.

State: Display the current state of a port.

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

Learning: Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses

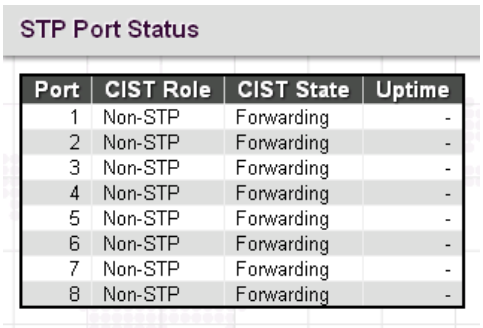
Forwarding: Ports forward packets and continue to learn addresses.

Edge: Display whether this port is an edge port or not.

Point-to-Point: Display whether this point is in point-to-point connection or not. This can be both automatically and manually configured.

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

3.8.7 Port Status


STP Port Status

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-

Port: The port number.

CIST Role: The role assigned by Spanning Tree Algorithm. Roles can be “Designated Port”, “Backup Port”, “Root Port” or “Non-STP”.

CIST State: Display the current state of a port. The CIST state must be one of the following:

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

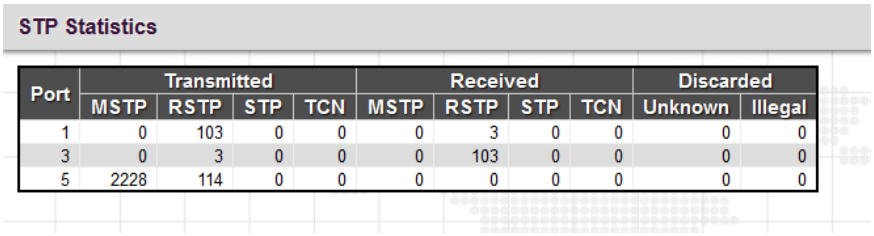
Learning: Port has transmitted configuration messages for an interval set by the Forward Delay parameter

without receiving contradictory information. Port address table is cleared, and the port begins learning addresses

Forwarding: Ports forward packets and continue to learn addresses.

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

3.8.8 Port Statistics


STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	0	103	0	0	0	3	0	0	0	0
3	0	3	0	0	0	103	0	0	0	0
5	2228	114	0	0	0	0	0	0	0	0

Port: Display the port number.

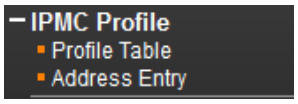
Transmitted & Received MSTP/RSTP/STP: The number of MSTP/RSTP/STP configuration BPDU messages transmitted and received on a port.

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

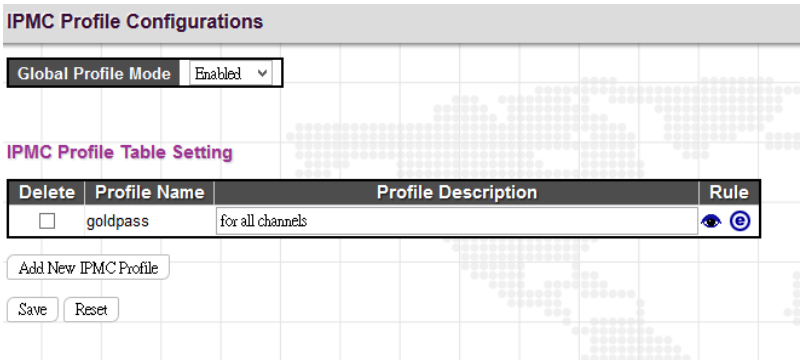
Discarded Unknown/Illegal: The number of unknown and illegal packets discarded on a port.

3.9 IPMC Profile

The "IPMC Profile" includes the following two sub menus.



3.9.1 Profile Table



IPMC Profile Configuration

Global Profile Mode: Enable or disable IPMC Profile feature globally.

IPMC Profile Table Setting

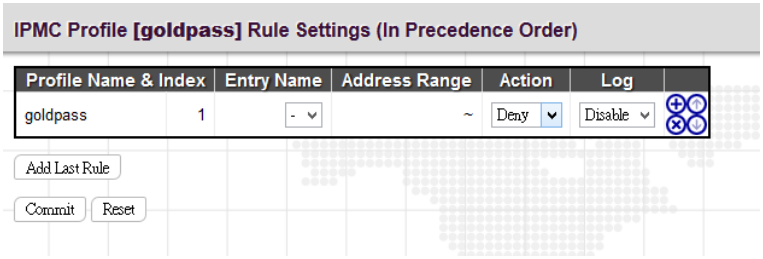
Profile Name: Enter a name for this profile.

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.

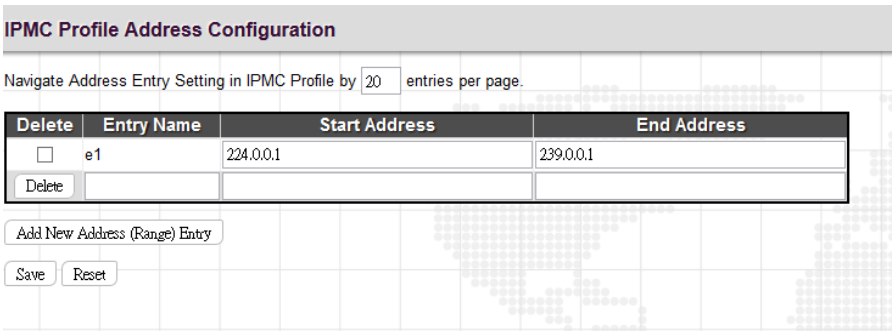
Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged.

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.

3.9.2 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.

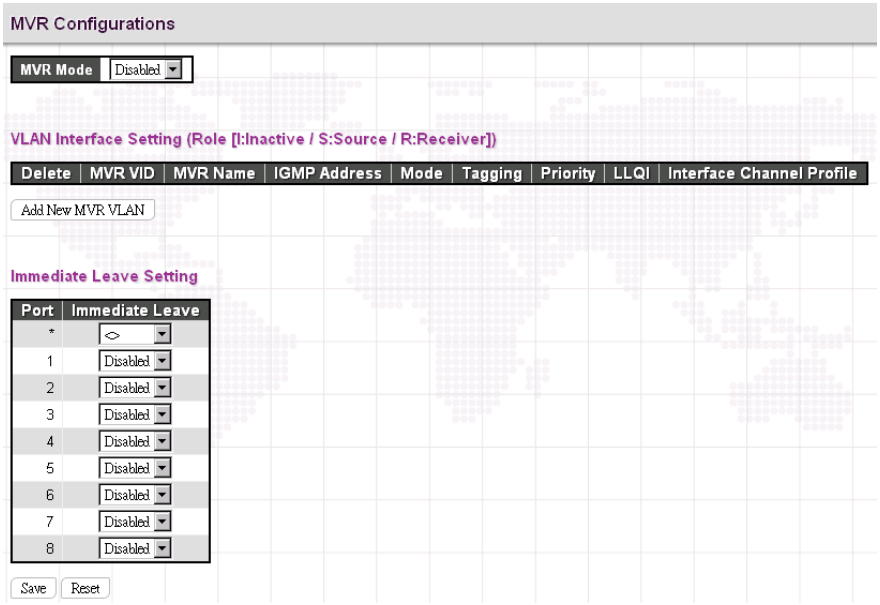
Select the "Delete" checkbox to delete an entry during the next save.

3.10 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).

3.10.1 Configurations



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.

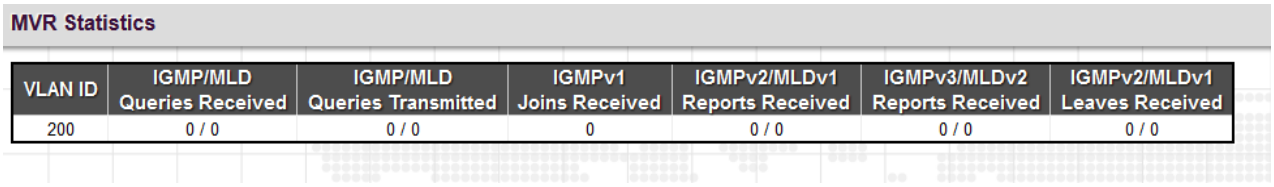
Receiver (R): Set a port to receiver port. Client or subscriber ports are configured to receiver ports so that they can issue IGMP/MLD messages to receive multicast data.

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.

3.10.2 Statistics


MVR Statistics

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
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.

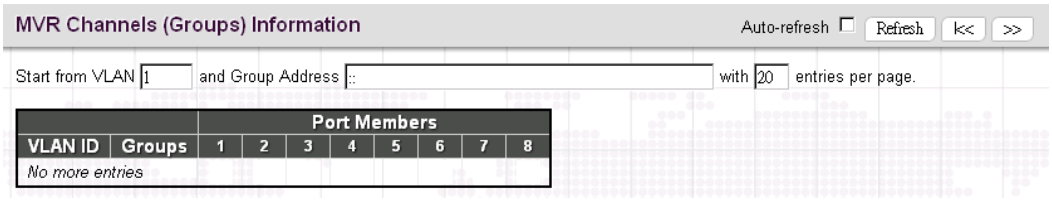
IGMPv1 Joins Received: The number of IGMPv1 received joins

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.

3.10.3 MVR Channel Groups



Start from VLAN ____ and Group Address _____ with 20 entries per page.

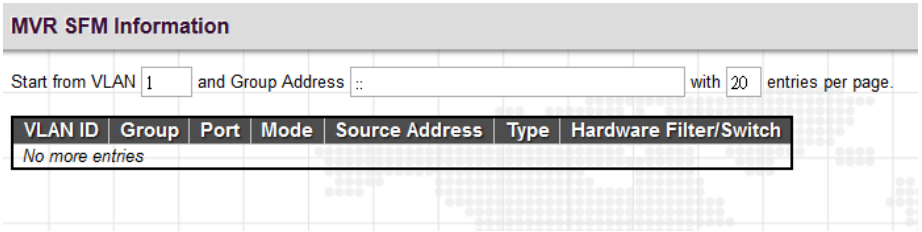
This table displays MVR channels (groups) information and is sorted by VLAN ID.

VLAN ID: VLAN ID of the group.

Groups: Group ID

Port Members: Ports that belong to this group.

3.10.4 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.

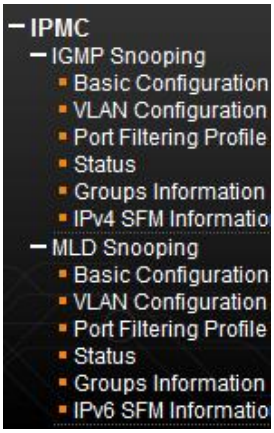
Source Address: The source IP Address. Currently, the system limits the total number of source IP addresses for filtering to be 128. When there is no source filtering address, "None" is shown in the Source Address field.

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.

3.11 IPMC

The “IPMC” menu includes IGMP Snooping and MLD Snooping sub menu. Select the appropriate menu to set up detailed configurations.



3.11.1 IGMP Snooping

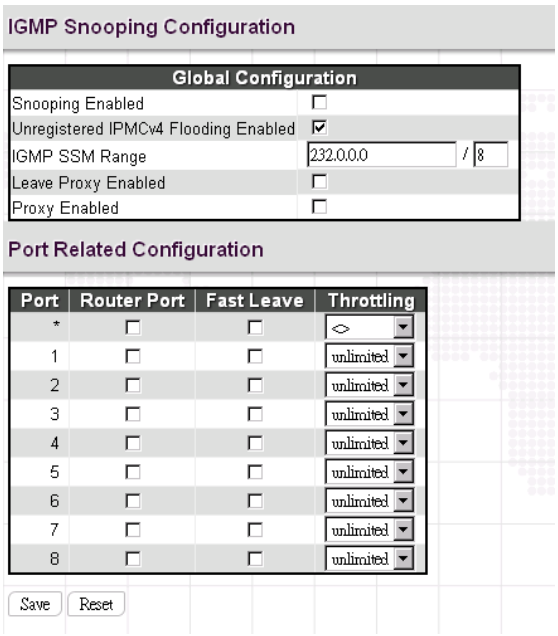
The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It can be used more efficiently when supporting activities,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

3.11.1.1 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

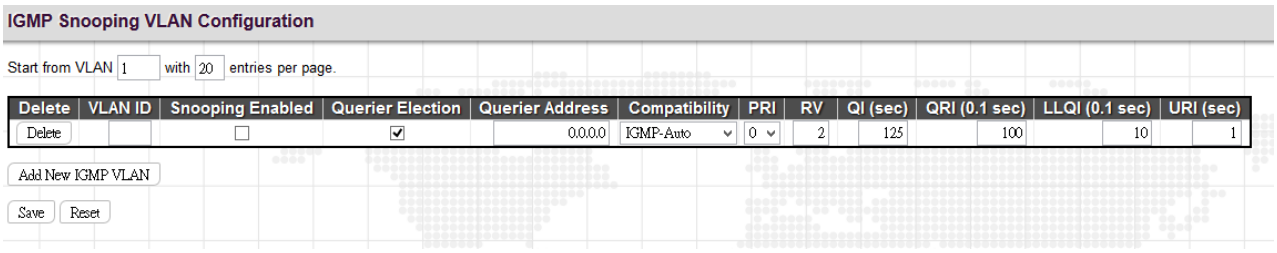
Port: The port number.

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

3.11.1.2 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.

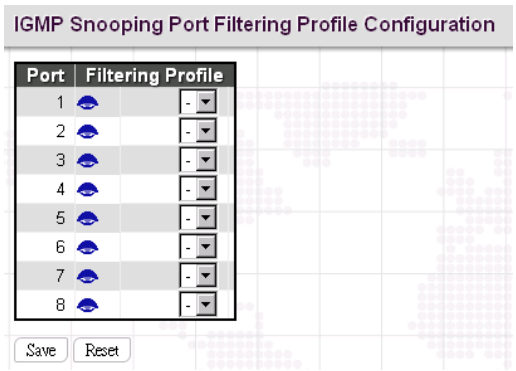
QRI: The Query Response Interval is the maximum amount of time that the IGMP router waits to receive a response to a General Query message. The QRI applies when the switch is acting as the querier and is used to inform other devices of the maximum time this system waits for a response to general queries.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

3.11.1.3 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.

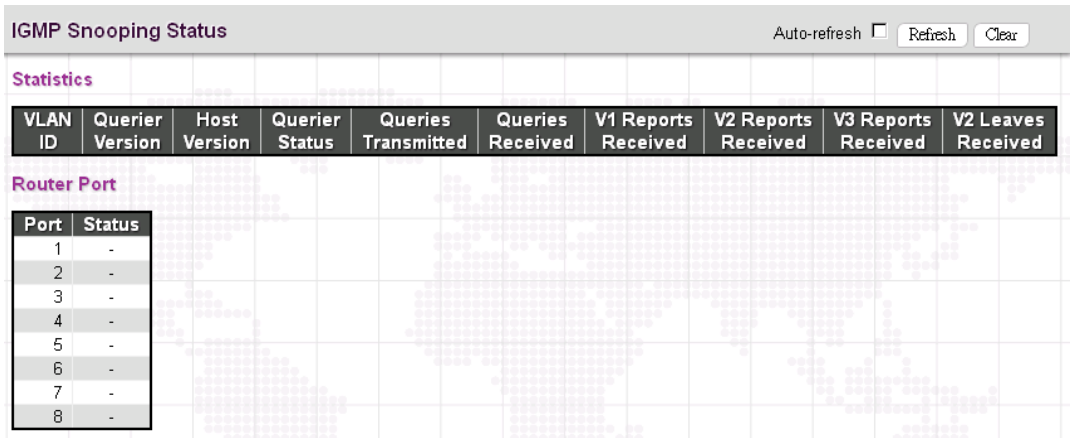


Port: The port number.

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.

3.11.1.4 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.

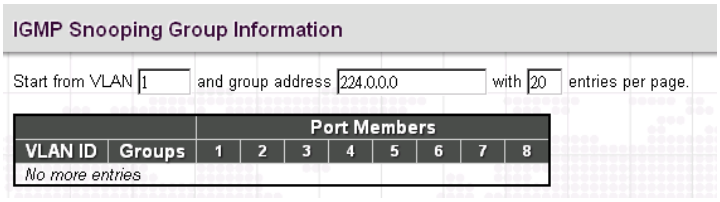
V2 Leaves Received: The number of Received V2 Leaves.

Router Port

Port: The port number.

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

3.11.1.5 Groups Information

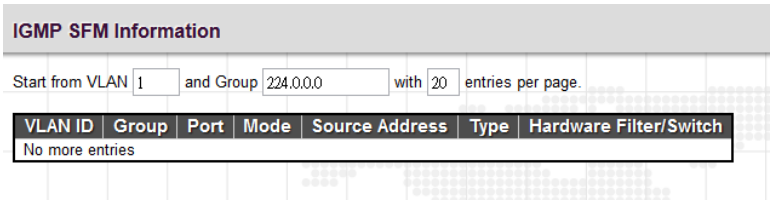


VLAN ID: Display the VLAN ID of the group.

Groups: Display the group address.

Port Members: Ports that belong to this group.

3.11.1.6 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.

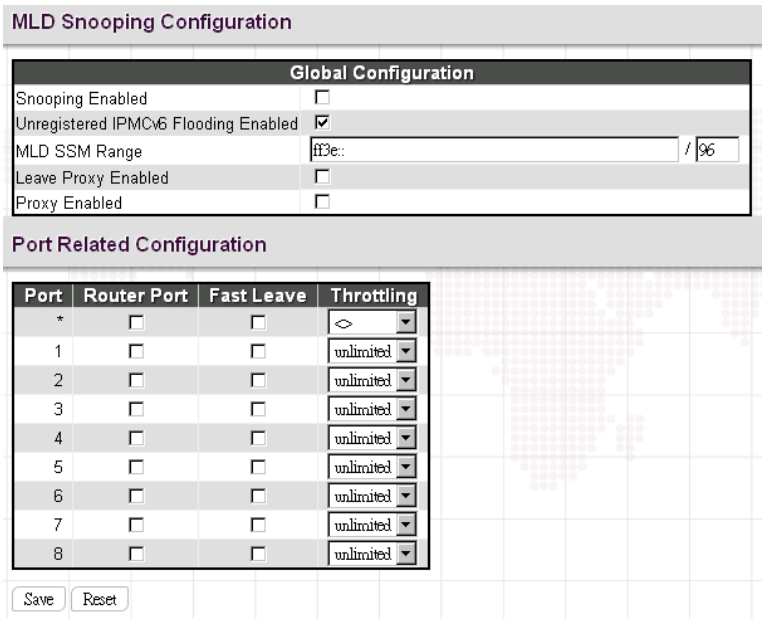
Type: Display either Allow or Deny type.

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.

3.11.2 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.

3.11.2.1 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

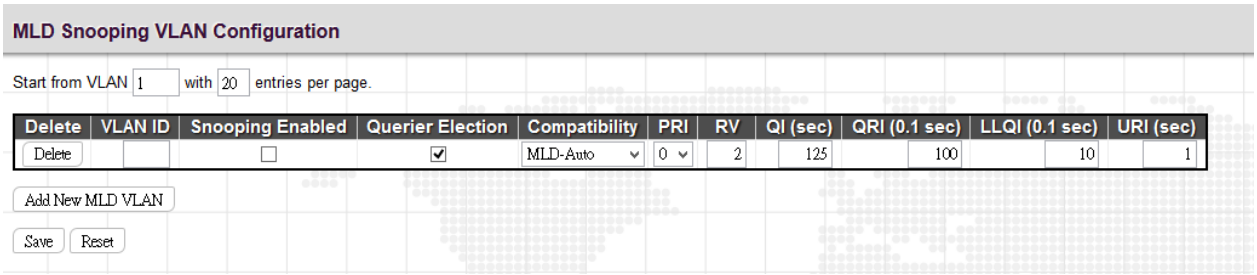
Port: The port number.

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.

3.11.2.2 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.

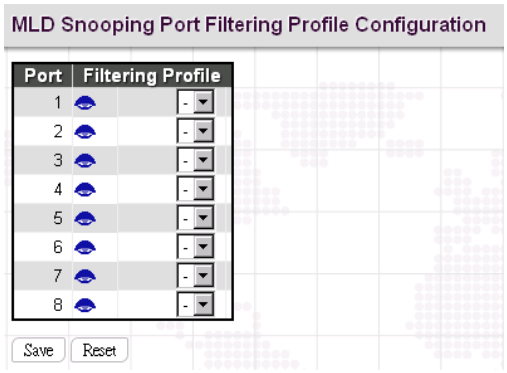
LLQI: The Last Listener Query Interval sets the interval that waits for a response to a group-specific or group-and-source specific query message.

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.

3.11.2.3 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.

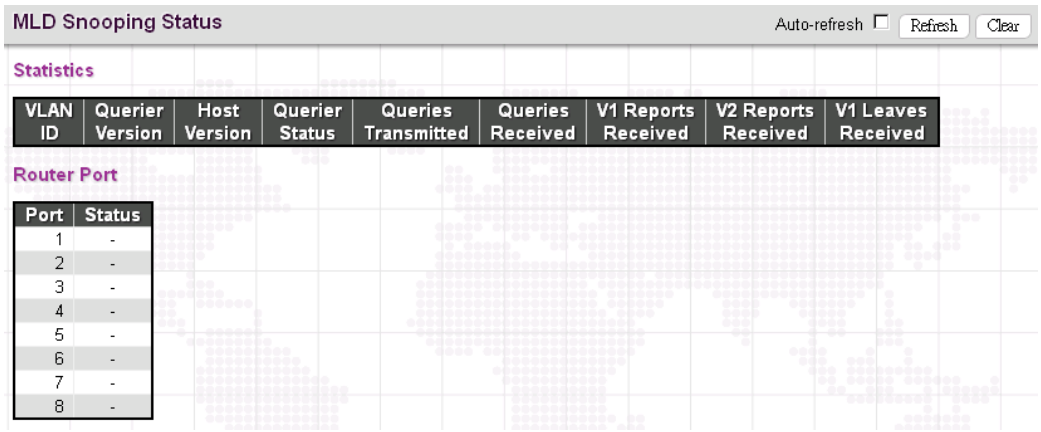


Port: List the number of each port.

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.

3.11.2.4 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.

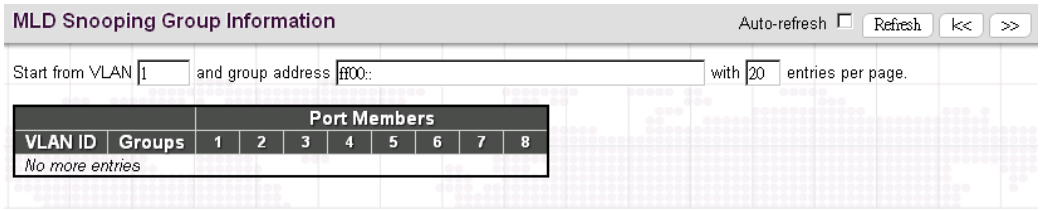
V2 Leaves Received: The number of Received V2 Leaves.

Router Port

Port: The port number.

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

3.11.2.5 Groups Information

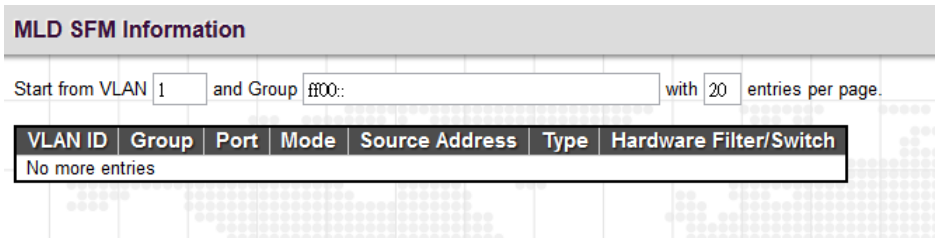


VLAN ID: Display the VLAN ID of the group.

Groups: Display the group address.

Port Members: Ports that belong to this group.

3.11.2.6 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.

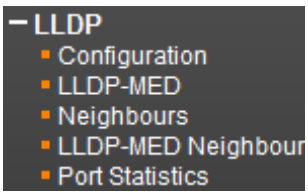
Type: Display either Allow or Deny type.

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.

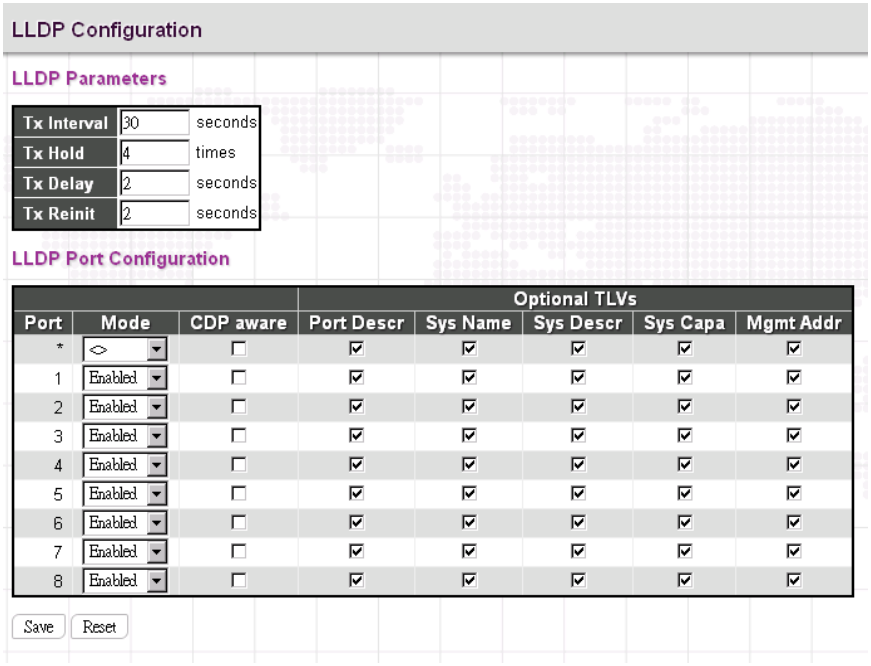
3.12 LLDP

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.



3.12.1 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.

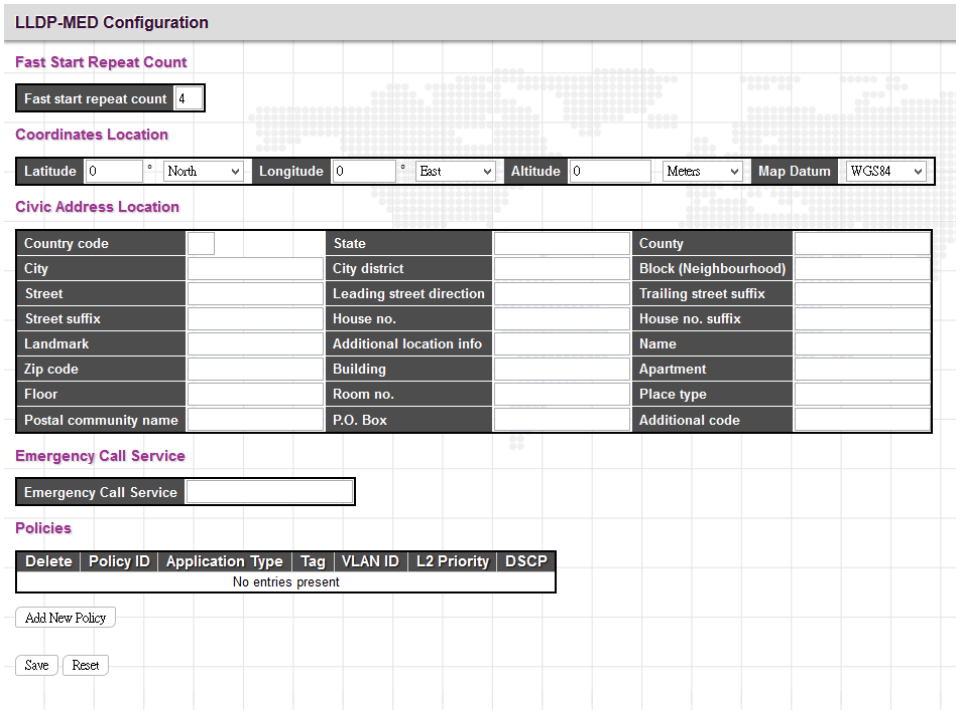
Tx Only: The switch will send out LLDP information but will drop LLDP information received from neighbours.

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.

3.12.2 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 Smith.

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”.

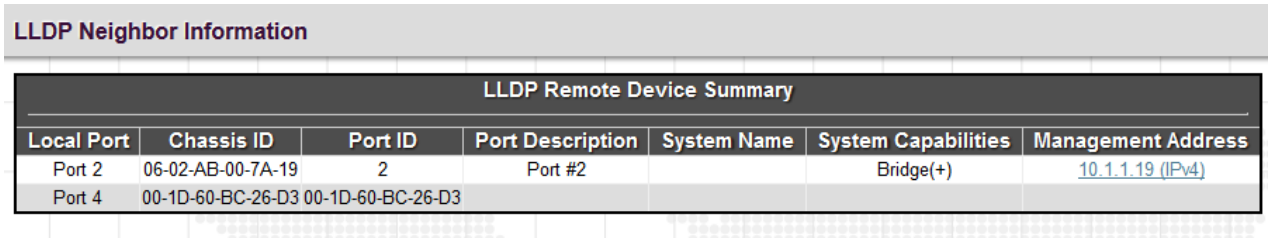
Tag: Tag indicating whether the specified application type is using a “tagged” or an “untagged” VLAN.

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.

3.12.3 Neighbours


LLDP Neighbor Information

LLDP Remote Device Summary

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
Port 2	06-02-AB-00-7A-19	2	Port #2		Bridge(+)	10.1.1.19 (IPv4)
Port 4	00-1D-60-BC-26-D3	00-1D-60-BC-26-D3				

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.

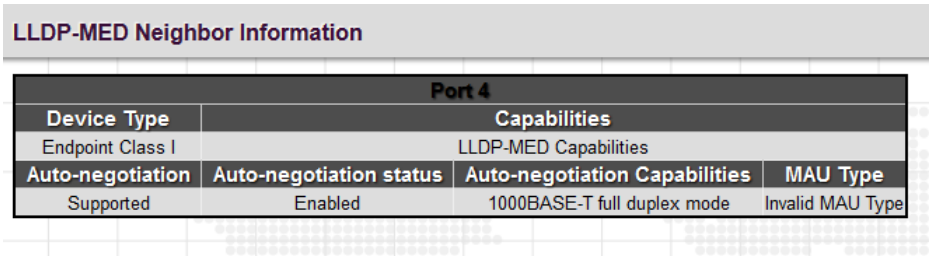
Port Description: A remote port's description.

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.

3.12.4 LLDP-MED Neighbours

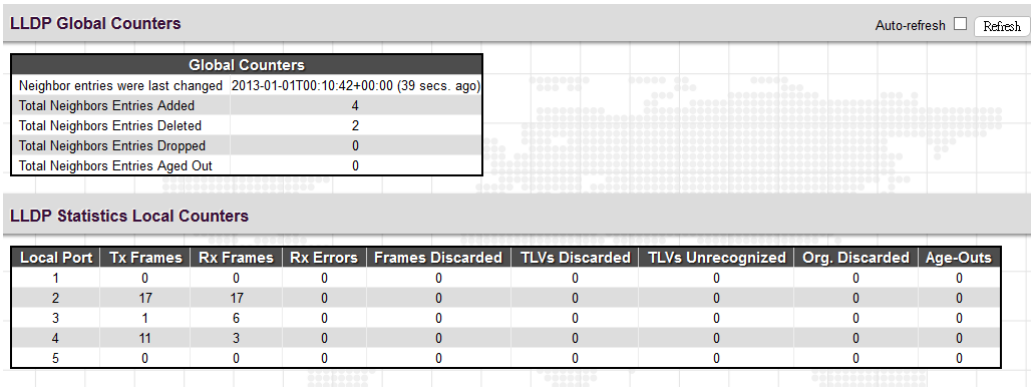


LLDP-MED Neighbor Information

Port 4			
Device Type	**Capabilities**		
Endpoint Class I	LLDP-MED Capabilities		
Auto-negotiation	**Auto-negotiation status**	**Auto-negotiation Capabilities**	**MAU Type**
Supported	Enabled	1000BASE-T full duplex mode	Invalid MAU Type

This page displays information about LLDP-MED neighbours detected on the network.

3.12.5 LLDP Global Counters



LLDP Global Counters

Auto-refresh ☐ Refresh

Global Counters	
Neighbor entries were last changed	2013-01-01T00:10:42+00:00 (39 secs. ago)
Total Neighbors Entries Added	4
Total Neighbors Entries Deleted	2
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	17	17	0	0	0	0	0	0
3	1	6	0	0	0	0	0	0
4	11	3	0	0	0	0	0	0
5	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.

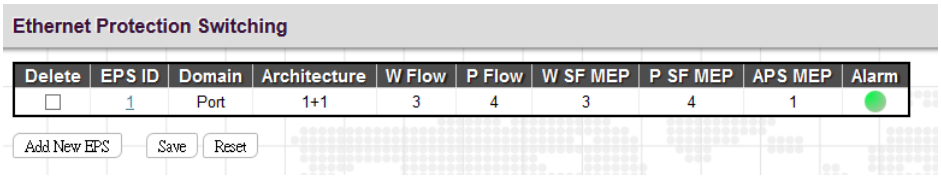
Org. Discarded: The number of organizational TLVs discarded.

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.

3.13 EPS

EPS (Ethernet Linear Protection Switching) operation, defined in ITU/T G.8031, is implemented in this device at the port level. EPS can perform 1+1 and 1:1 switching protection architecture where the former architecture operates with either unidirectional or bidirectional switching; while the latter one operates with unidirectional switching. It can also be configured to revertive mode allowing the traffic goes back to working transport entity when the original fault is repaired and WTR (wait to restore) timer has expired. The other timer supported is Hold-Off timer which configures the delay time of protection switching until an upstream device or the lower layer is ready for transmission.

In EPS configuration page, EPS instances are created to associate with MEPs on the working and protection entities that are responsible for sending and receiving APS protocol frames. APS frames can be either unicast or multicast depending on the types of traffic in the actual networking environment.



EPS ID: Specify EPS ID for this entry. Click the ID number to further configure detailed EPS settings.

Domain: Select the flow domain. Currently, only “Port” option is available for use.

Architecture: The EPS architecture. The architecture at both ends must match.

1+1: This will create a 1+1 EPS.

1:1: The APS protocol is mandatory for 1:1 protection.

W Flow: Working flow instance number.

P Flow: Protecting flow instance number.

W SF MEP: Working Signal Failure MEP instance number.

P SF MEP: Protecting Signal Failure MEP instance number.

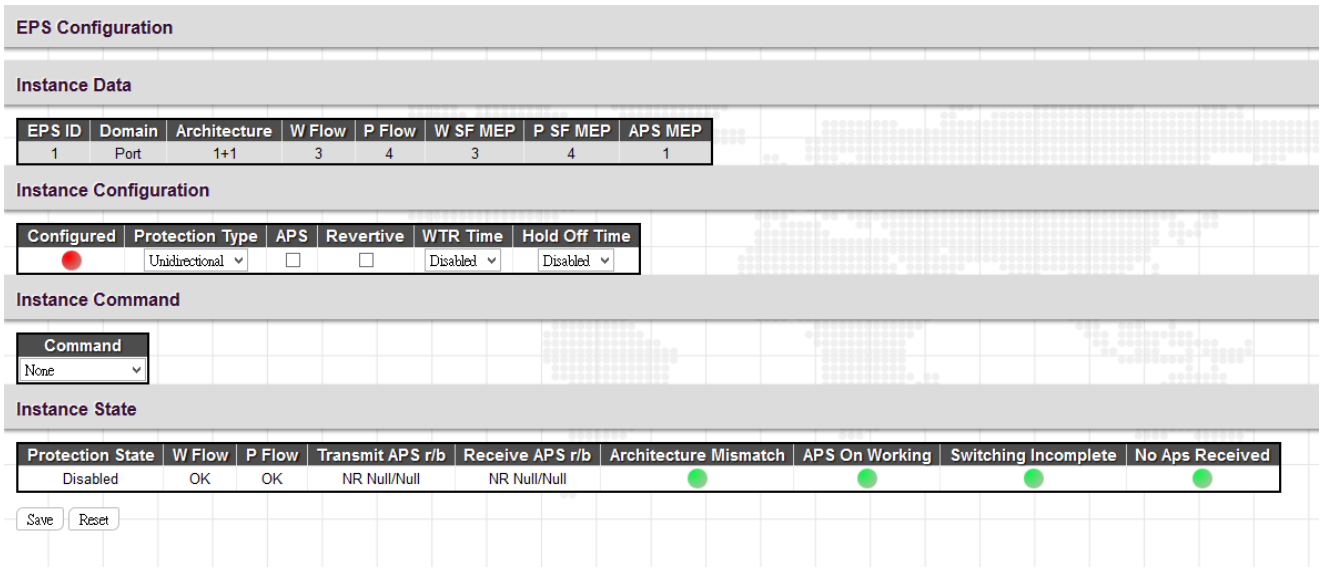
APS MEP: APS MEP instance number.

Alarm: When settings are complete, the switch will show an alarm status on the EPS.

Click the “Add New EPS” button to create a new entry.

Click “Delete” button to remove an entry from the table.

Click the EPS ID to further configure detailed settings of EPS.



Instance Data

This table shows settings configured above.

Instance Configuration

Protection Type: Select the protection type either unidirectional or bidirectional switching.

APS: Select the checkbox to enable APS (Automatic Protection Switching) feature.

Revertive: Select the checkbox to enable revertive mode. Leaving the checkbox unchecked will operate on non-revertive mode.

WTR Time: WTR stands for Wait To Restore and WTR timer is used in revertive mode to avoid a constant and rapid cycle between down and up states in a misconfigured or mismanaged network (known as flapping).

Hold Off Time: Hold Off timer would delay the protection switching until an upstream device or the lower layer is ready. Select the desired Hold-off-time from the drop-down menu.

Instance Command

Command: This field allows the switch to perform a particular action on an EPS instance. Available options are listed below.

None: No command is used.

Clear: Any active command is cleared.

Lockout: End-to-end lock out of the protection entity.

Forced Switch: Forced switch to the protection entity.

Manual Switch P: Manual switch to the protection entity.

Manual Switch W: Manual switch to the working entity.

Exercise: Exercise of APS protocol.

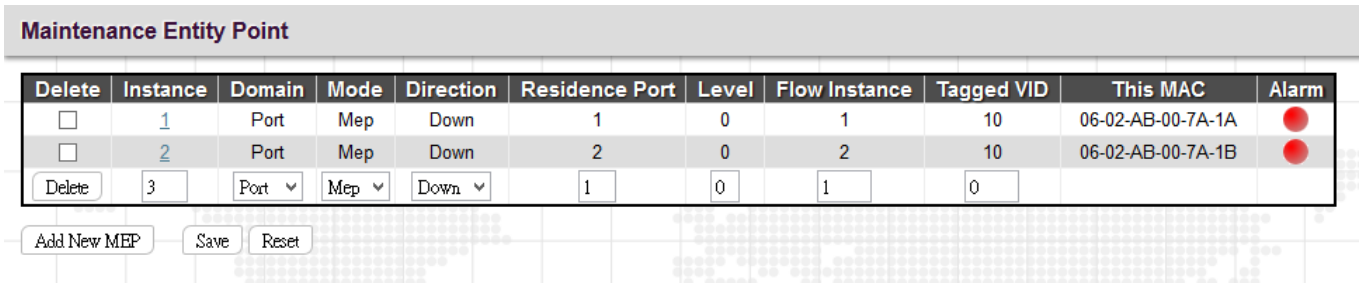
Freeze: Local freeze of protection entity.

Lock out Local: Local lock out of the protection entity.

Instance State

This table shows the current state of the configured instance including APS frames transmitted and received and APS working status.

3.14 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: Three domain options are available.

Port: This is a MEP in the Port Domain. 'Flow Instance' is a Port.

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

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

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

Direction: Select the traffic direction either down (Ingress) or up (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.

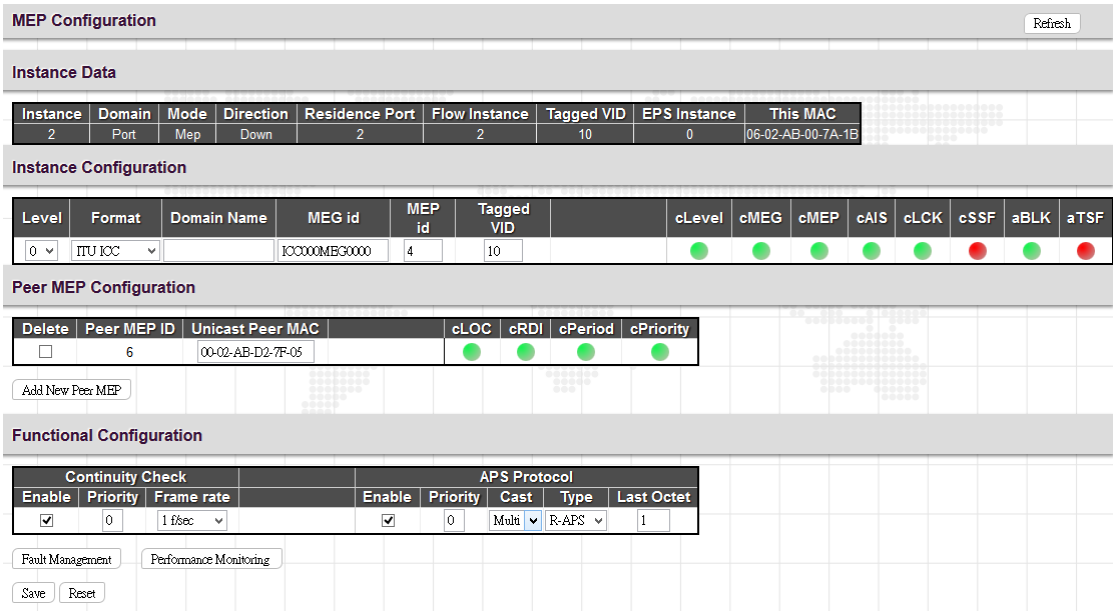
Tagged VID: A C-tag or S-tag (depending on VLAN port type) is added with this VID. Entering "0" means no tag will be added.

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.

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.

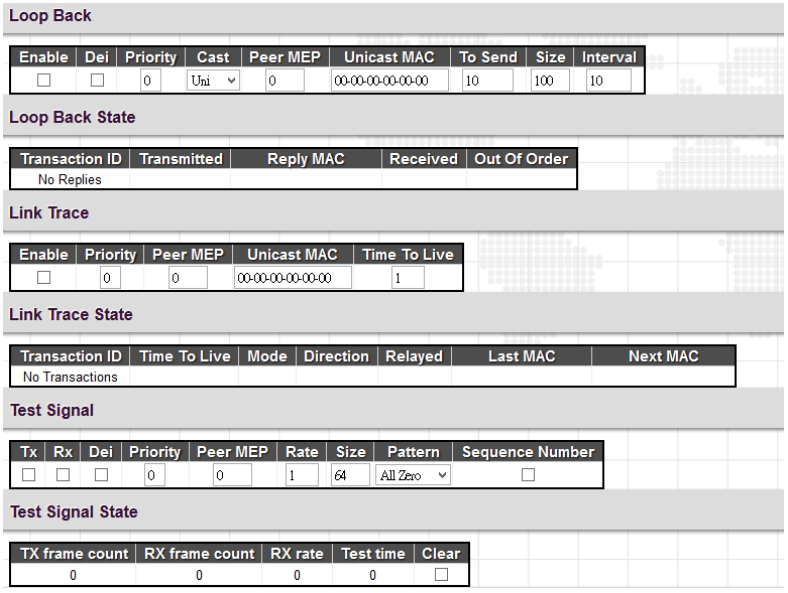
Type:

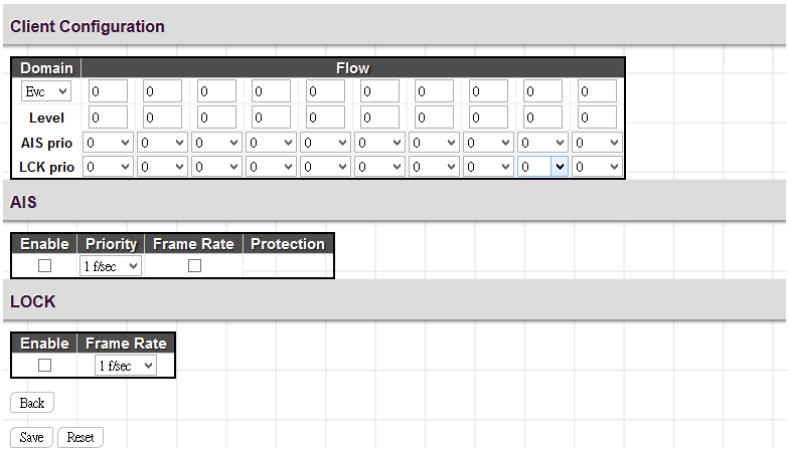
R-APS: APS PDU is transmitted as R-APS (this is for ERPS).

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 indicates 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. The domain can be EVC or VLAN.

Flow: The client layer instance numbers.

Level: The client layer level which means that PDU transmitted in client layer flows will be on this level.

AIS prio: The priority to be used when transmitting AIS in each client flow. Priority resulting in highest possible PCP can be selected.

LCK prio: The priority to be used when transmitting LCK in each client flow. Priority resulting in highest possible PCP can be selected.

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.

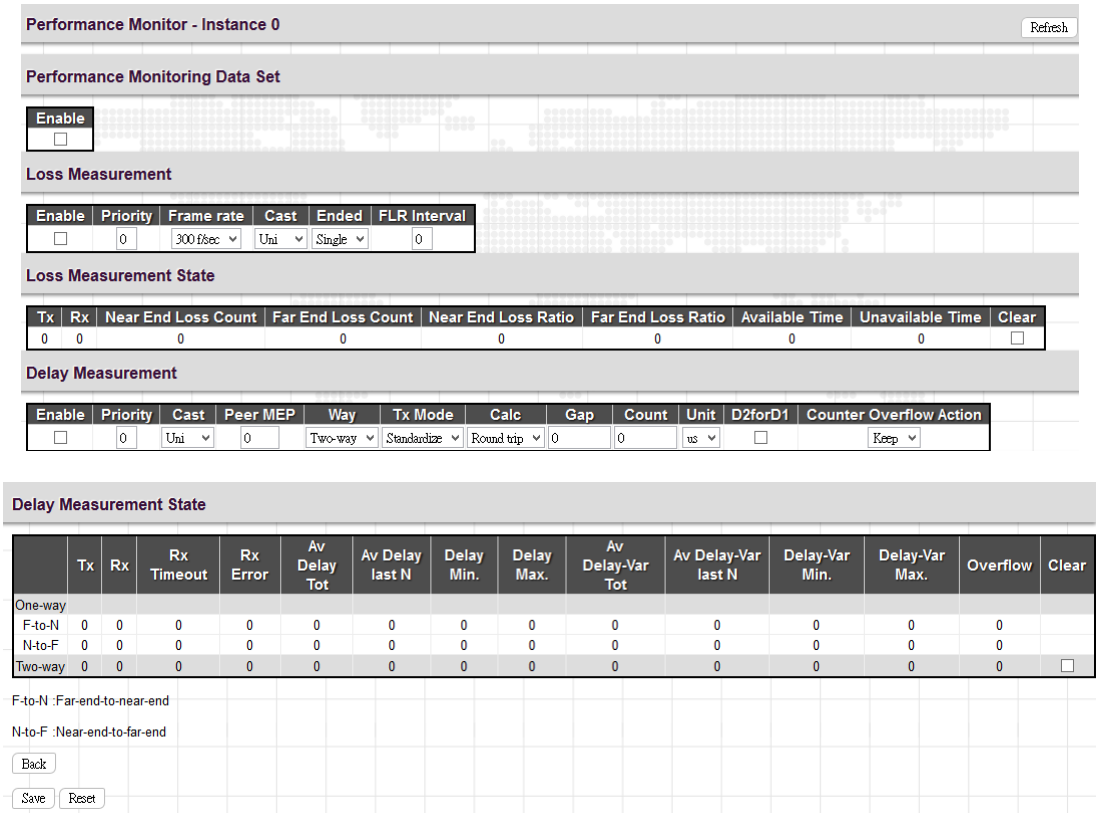
Lock

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.



Performance Monitoring Data Set

Enable: When enabled, this MEP instance will contribute to the Performance Monitoring Data Set gathered by the Performance Monitoring session.

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.

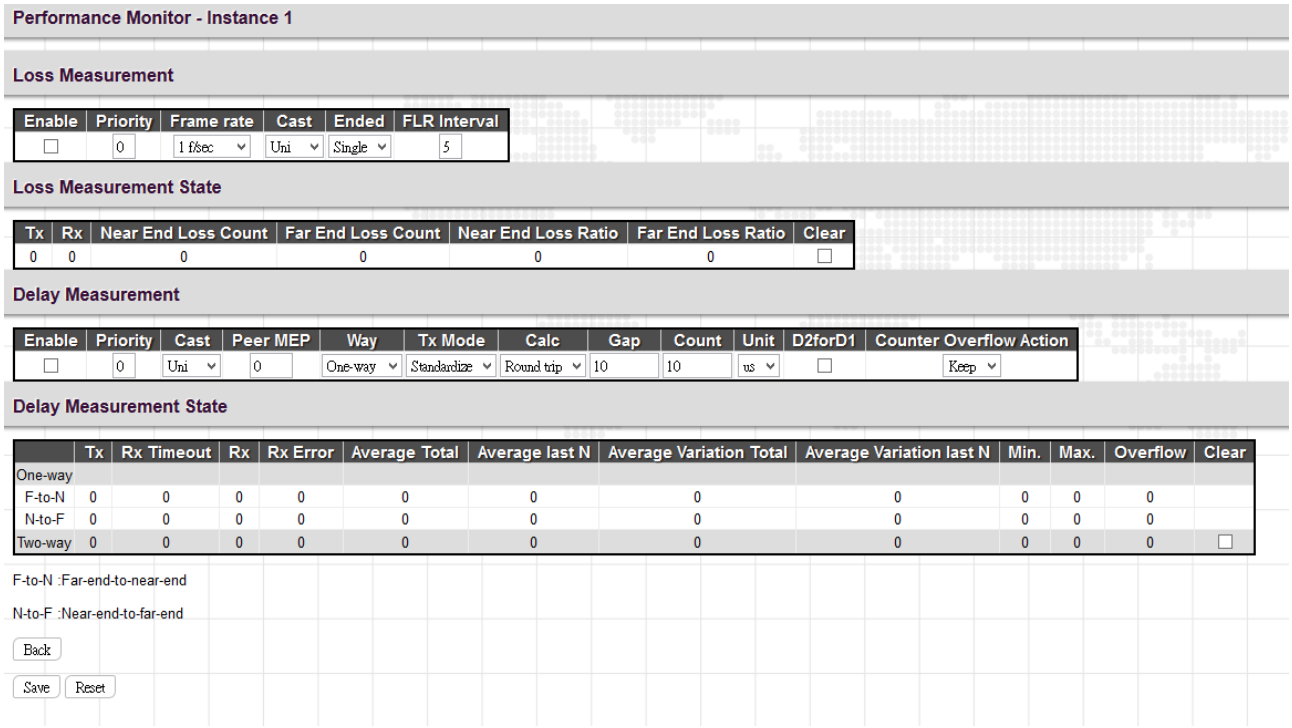
Count: The number of last records to calculate. The range is 10 to 2000.

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.

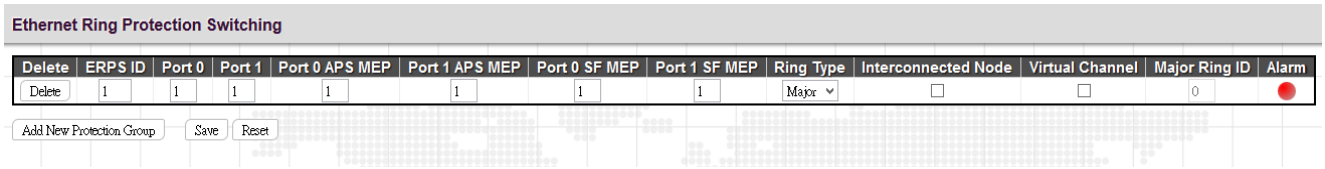
3.15 ERPS

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.



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.

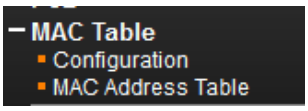
Click "Save" to save changes.

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

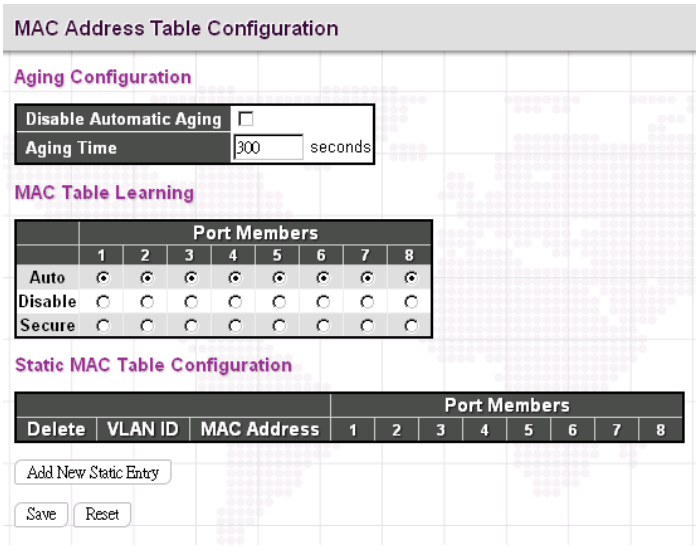
Click "Refresh" to manually refresh ERPS information.

3.16 MAC Table

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



3.16.1 Configuration



Disable Automatic Aging: Learned MAC addresses will appear in the table permanently.

Aging Time: Set up the aging time for a learned MAC to be appeared in MAC learning table. The allowed range is 10 to 1000000 seconds.

MAC Learning Table: Three options are available on each port.

Auto: On a given port, learning is automatically done once unknown SMAC is received.

Disable: Disable MAC learning function.

Secure: Only static MAC entries listed in "Static MAC Table Configuration" are learned. Others will be dropped.

NOTE: *Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.*

Static MAC Table Configuration: This table is used to manually set up static MAC entries. The total entries that can be entered are 64.

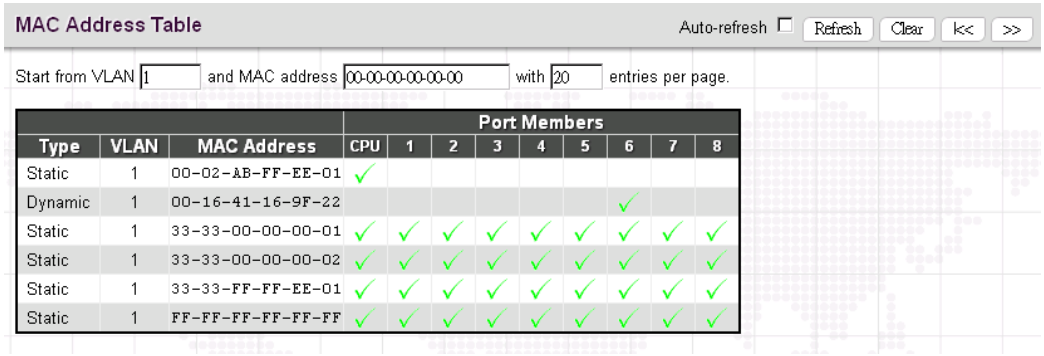
Delete: Delete this MAC address entry.

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.

3.16.2 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.



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.

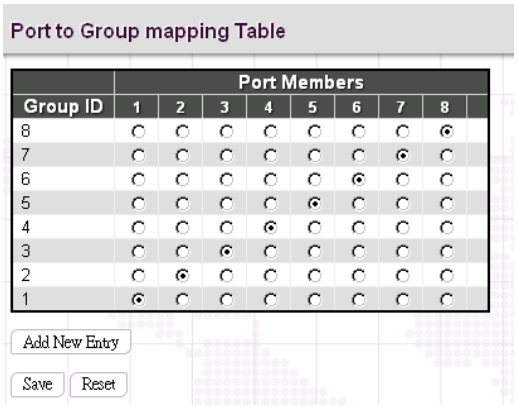
Port Members: Ports associated with this entry.

3.17 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.

3.17.1 Port to Group Mapping

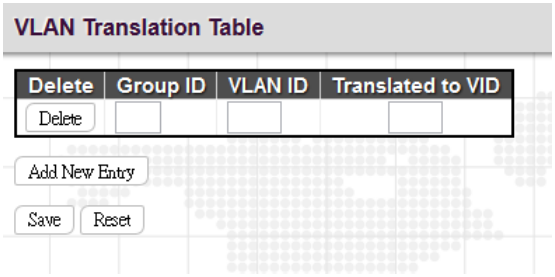


Group ID: The total VLAN Translation group can be used is 11 which is automatically created in Group Mapping Table when entering "Port to Group Mapping" page. A port can be mapped to any of the groups. Multiple ports can be mapped to a single group with the same Group ID.

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.

3.17.2 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.

3.18 VLANs

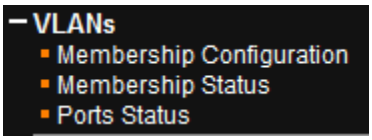
IEEE 802.1Q VLAN (Virtual Local Area Network) is a popular and cost-effectively way to segment your networking deployment by logically grouping devices with similar attributes irrespective of their physical connections. VLANs also segment the network into different broadcast domains so that packets are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

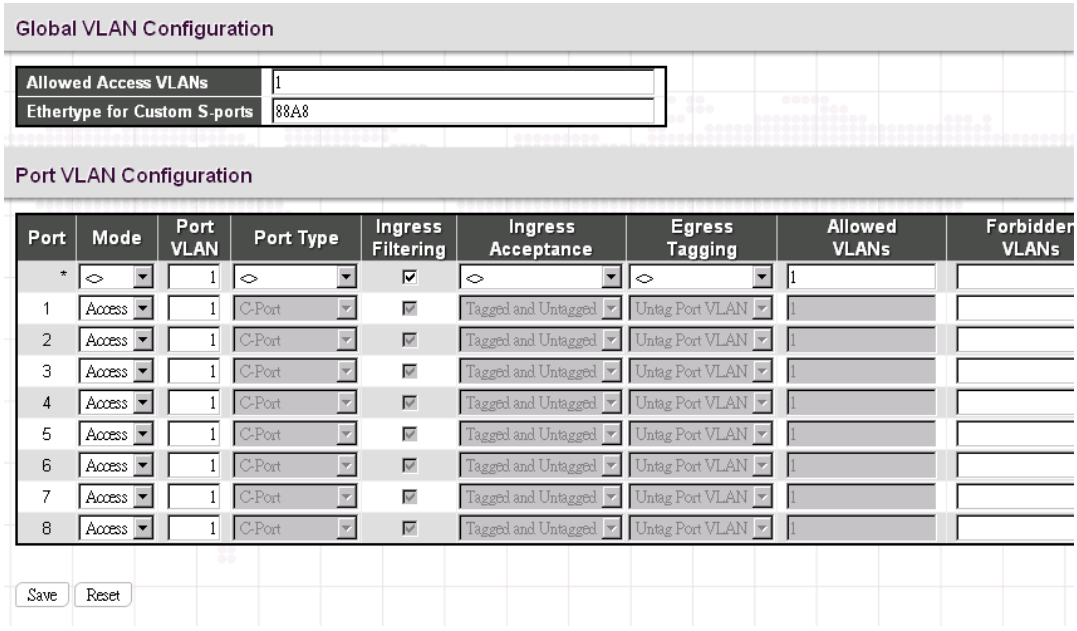
VLANs help control traffic: Traditionally, when networks are not segmented into VLANs, congestion can be easily caused by broadcast traffic that is directed to all devices. To minimize the possibility of broadcast traffic damaging the entire network, VLANs can help group devices that communicate frequently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



3.18.1 Membership Configuration



Global VLAN Configuration

Allowed Access VLANs: This shows the allowed access VLANs. This setting only affects ports set in “Access” mode. Ports in other modes are members of all VLANs specified in “Allowed VLANs” field. By default, only VLAN 1 is specified.

More allowed access VLANs can be entered by specifying the individual VLAN ID separated by comma. If you want to specify a range, separate it by a dash. For example, 1, 5, 10, 12-15, 100

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

Port VLAN Configuration

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

Mode: The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied.

Access: Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:

- Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1.
- Accepts untagged and C-tagged frames.
- Discards all frames that are not classified to the Access VLAN.
- On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged.

Trunk: Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:

- By default, a trunk port is member of all VLANs (1-4095).
- The VLANs that a trunk port is member of may be limited by the use of "Allowed VLANs".
- Frames classified to a VLAN that the port is not a member of are discarded.
- By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress.
- Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress.

Hybrid: Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

- Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware.
- Ingress filtering can be controlled.
- Ingress acceptance of frames and configuration of egress tagging can be configured independently.

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

The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

Port Type: When you select "Hybrid" mode, the Port Type field becomes selectable. There are four port types available. Each port type's ingress and egress action is described in the following table.

Action / Port Type	Ingress Action	Egress Action
Unaware	When a tagged frame is received on a port, 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.

Ingress Acceptance: Select the acceptable ingress traffic type on a port.

Tagged and Untagged: Both tagged and untagged ingress packets are acceptable on a port.

Tagged Only: Only tagged ingress packets are acceptable on a port. Untagged packets will be dropped.

Untagged Only: Only untagged ingress packets are acceptable on a port. Tagged packets will be dropped.

Egress Tagging: The action taken when packets are sent out from a port.

Untag Port VLAN: Frames that carry PVID will be removed when leaving from a port. Frames with tags other than PVID will be transmitted with the carried tags.

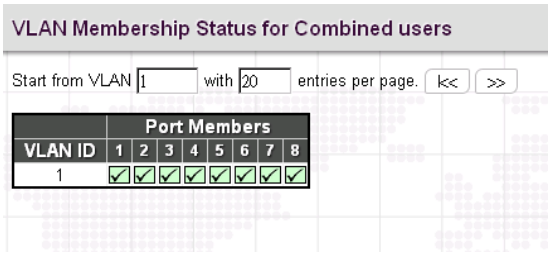
Tag All: Frames are transmitted with a tag.

Untag All: Frames are transmitted without a tag. This option is only available for ports in Hybrid mode.

Allowed VLAN: Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095.

Forbidden VLAN: A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. By default, the field is left blank, which means that the port may become a member of all possible VLANs.

3.18.2 Membership Status

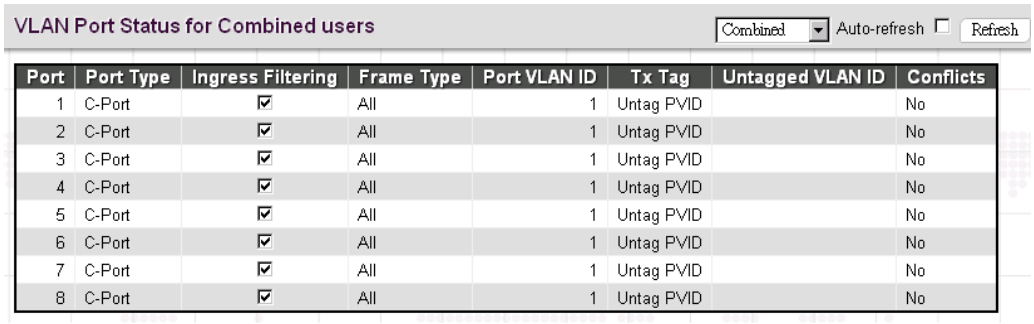


This page shows the current VLAN membership saved on the Switch.

VLAN ID: VLANs that are already created.

Port members: Display member ports on the configured VLANs.

3.18.3 Port Status



Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag PVID		No
2	C-Port	☑	All	1	Untag PVID		No
3	C-Port	☑	All	1	Untag PVID		No
4	C-Port	☑	All	1	Untag PVID		No
5	C-Port	☑	All	1	Untag PVID		No
6	C-Port	☑	All	1	Untag PVID		No
7	C-Port	☑	All	1	Untag PVID		No
8	C-Port	☑	All	1	Untag PVID		No

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

Port: The port number.

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

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

Frame Type: Displays the accepted Ingress frame type.

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

Tx Tag: Displays the Egress action on a port.

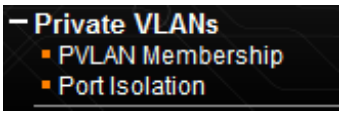
Untagged VLAN ID: Display the untagged VLAN ID. A port's UVID determines the packet's behavior at the egress side. If the VID of Ethernet frames leaving a port match the UVID, these frames will be sent untagged.

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

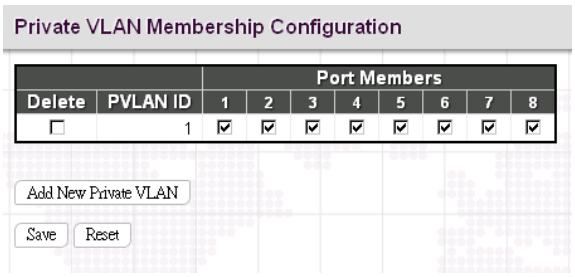
*Functional conflicts between features.
*Conflicts due to hardware limitations.
*Direct conflicts between user modules.

3.19 Private VLANs

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



3.19.1 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.

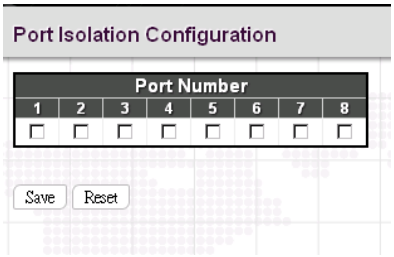
Delete: Delete this VLAN membership entry.

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.

3.19.2 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.

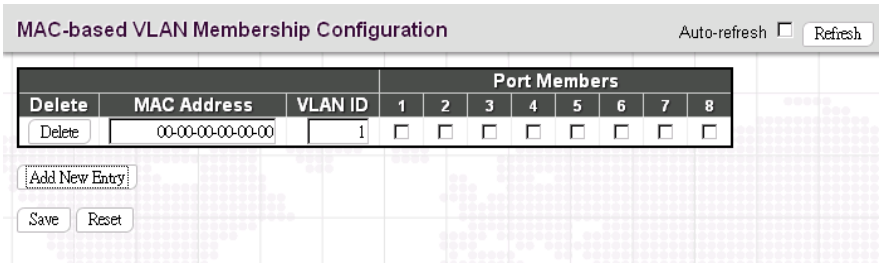
3.20 VCL

The "VCL" menu contains the following sub menus.

3.20.1 MAC-based

MAC-based VLAN configuration page is to set up VLANs based on source MAC addresses. When ingress untagged frames are received by a port, source MAC address is processed to decide which VLAN these untagged frames belong. When source MAC addresses does not match the rules created, untagged frames are assigned to the receiving port's native VLAN ID (PVID).

3.20.1.1 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.

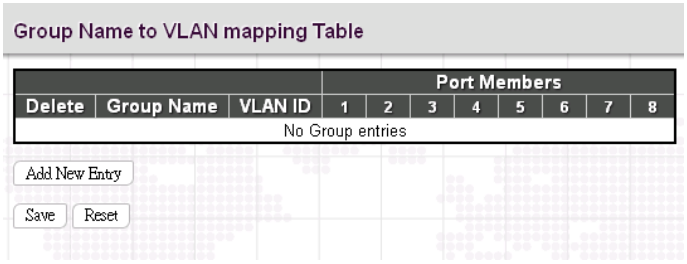
Port Members: Ports that belong to this VLAN.

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.

3.20.1.2 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.

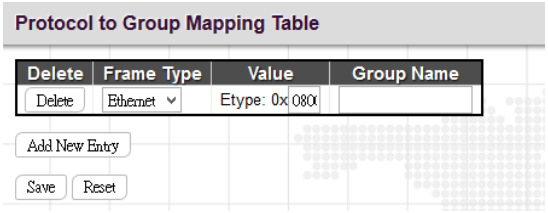
Port Members: Display ports that accept the configured MAC address.

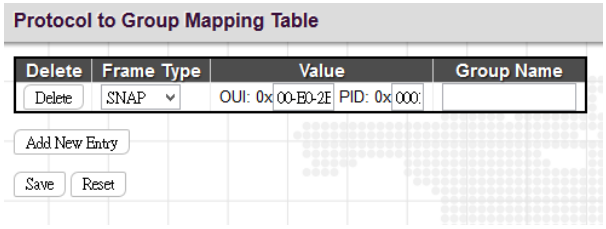
3.20.2 Protocol-based VLAN

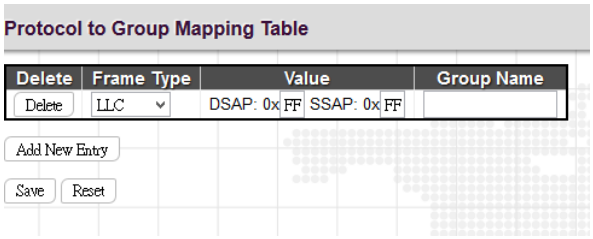
The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of 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.

3.20.2.1 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.

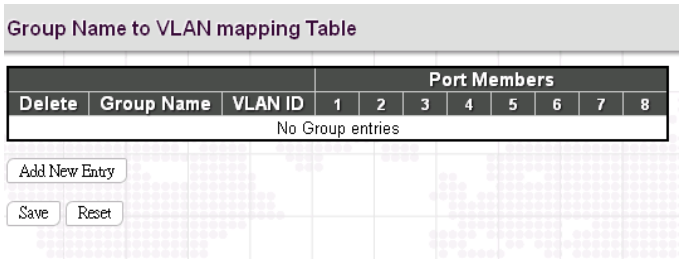
OUI: A value in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value in the ranges of 0x00-0xff.

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).

3.20.2.2 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).

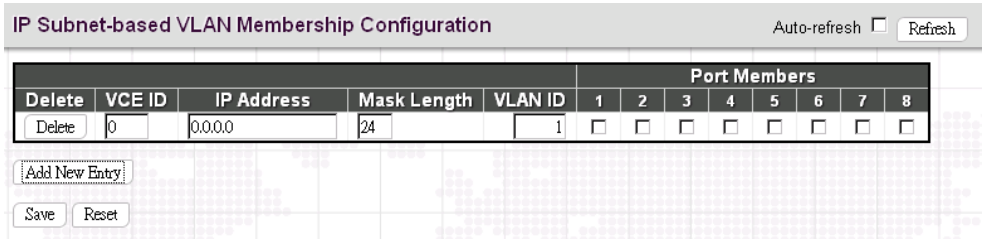
VLAN ID: Indicate the VLAN ID.

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.

3.20.3 IP Subnet-based VLAN



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

IP Address: Indicate the IP address for this rule.

Mask Length: Indicate the network mask length.

VLAN ID: Indicate the VLAN ID

Port Members: Assign ports to this rule.

Click the “Add New Entry” button to insert a new entry to the list.

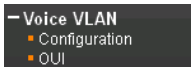
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

3.21 Voice VLAN

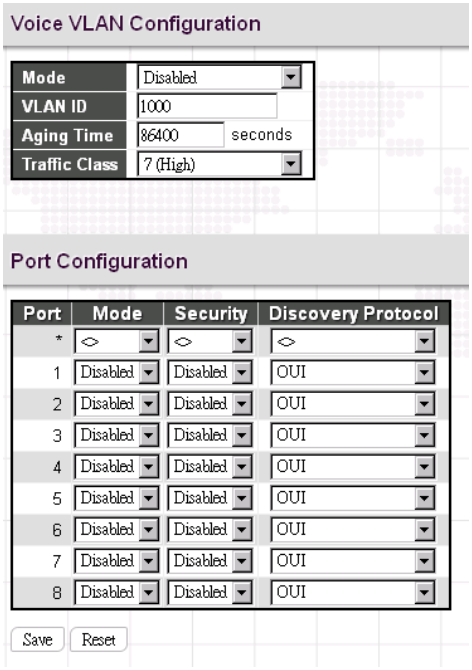
Nowadays, in the enterprise network, VoIP devices are commonly deployed to save operational cost due to its easy-to-setup feature and convenience. However, while deploying VoIP devices, it is recommended that VoIP traffic is separated from data traffic. By isolating traffic, VoIP traffic can be assigned to have the highest priority while forwarding so that higher voice quality can be achieved without encountering situations like excessive packet delays, packet loss, and jitters. Moreover,

This switch provides Voice VLAN feature that enables voice traffic to be forwarded on the voice VLAN. The user can also overwrite traffic priority by assigning higher traffic class value to voice traffic. Voice traffic can be detected on a port by using LLDP (IEEE 802.1ab) to discover VoIP devices attached to the switch or from devices’ OUI (Organizationally Unique Identifier). When voice packets are detected on a port, the switch automatically assigns the port as a tagged member of the Voice VLAN and forward packets based on configurations set in Voice VLAN configuration page.

The Voice VLAN section provides that following two sub menus:



3.21.1 Configuration



Voice VLAN Configuration

Mode: Enable or disable Voice VLAN function on this switch.

VLAN ID: Assign a VLAN ID to this Voice VLAN. Only one Voice VLAN is supported on the switch. By default, VLAN 1000 is set. The allowed range is 1 - 4095.

Note:

1. *The Voice VLAN cannot be the same as management VLAN, MVR VLAN, or the native VLAN assigned to any port.*
2. *MSTP must be disabled before the Voice VLAN is enabled or the Voice VLAN port mode is set to Auto or Forced. This prevents the spanning tree's ingress filter from dropping VoIP traffic tagged for the Voice VLAN.*

Aging Time: The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. By default, the aging time is set to 86400 seconds. The allowed aging time is 10 – 10,000,000 seconds.

Traffic Class: Select the traffic class value which defines a service priority for traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new traffic class when the Voice VLAN feature is active on a port. By default, 7 (Highest priority) is used. The allowed range is 0 (Lowest) ~ 7 (Highest).

Port Configuration

Port: The port number. "All" rules apply to all ports.

Mode: Select whether a particular is enabled with Voice VLAN feature or not. There are three options available:

Disabled: Disable Voice VLAN feature on a particular port.

Auto: Enable the Voice VLAN auto detection mode. When voice (VoIP) traffic is detected on a port, the port will be added as a tagged member to the Voice VLAN. When Auto mode is selected, you need to further decide a method for detecting voice traffic in "Discovery Protocol" field, either OUI or LLDP (802.1ab).

Forced: Enable Voice VLAN feature on a particular port.

Security: Enable or disable security filtering feature on a per port basis. When enabled, any non-VoIP packets received on a port with Voice VLAN ID will be discarded. VoIP traffic is identified by source MAC addresses configured in the telephony OUI list or through LLDP which is used to discover VoIP devices attached to the switch.

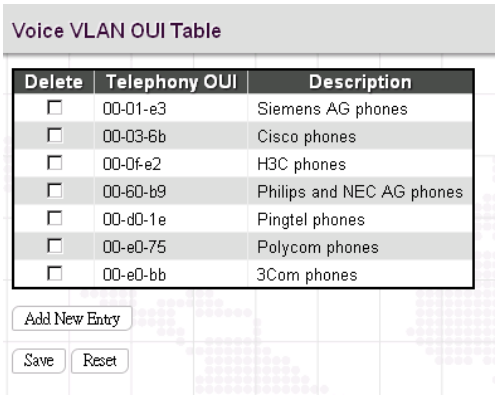
Discovery Protocol: Select a method for detecting VoIP traffic. By default, OUI is used.

OUI: Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to manufacturers and form the first three octets of a device MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.

LLDP: Use LLDP (IEEE 802.1ab) to discover VoIP devices attached to a port. LLDP checks that the "telephone bit" in the system capability TLV is turned on or not.

Both: Use both OUI table and LLDP to detect VoIP traffic on a port.

3.21.2 OUI



Telephony OUI: Specify your VoIP device's OUI. It must be 6 characters long and the input format is "xx-xx-xx" (x is hexadecimal digit)

Description: Specify a descriptive comments or information to this entry.

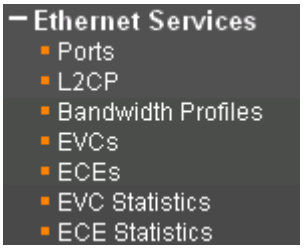
Click the "Add New Entry" button to insert a new entry to the list.

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

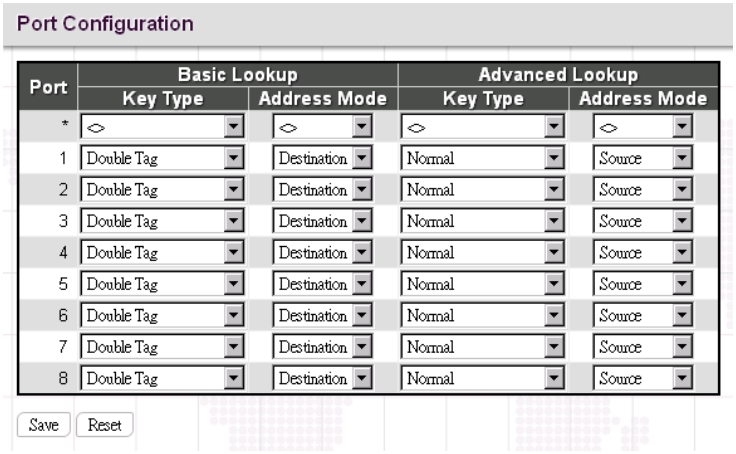
Click the "Save" button to save settings or changes.

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

3.22 Ethernet Services



3.22.1 Port Configuration



Port: The port number. Port * rule applies to all ports.

DEI Mode: The DEI mode for an NNI port determines whether frames transmitted on the port will have the DEI field in the outer tag marked based on the color of the frame. The allowed values are:

Coloured: The DEI is 1 for yellow frames and 0 for green frames.

Fixed: The DEI value is determined by ECE rules.

Tag Mode: The tag mode specifies whether the EVC classification must be based on the outer or inner tag. This can be used on NNI ports connected to another service provider, where an outer tunnel tag is added together with the inner tag identifying the EVC.

Inner: Enable inner tag in EVC classification.

Outer: Enable outer tag in EVC classification.

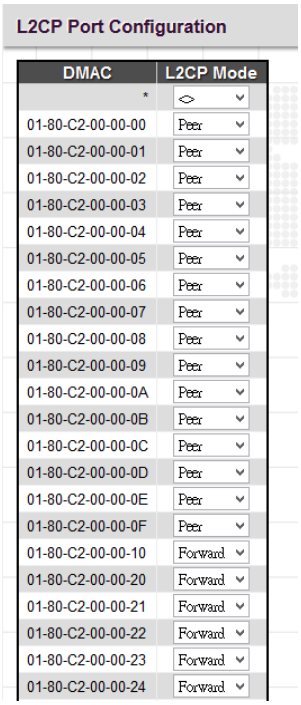
Address Mode: The address mode specifies whether the EVC classification must be based on source or destination address.

Source: Enable SMAC/SIP matching.

Destination: Enable DMAC/DIP matching.

3.22.2 L2CP

L2CP stands for Layer 2 Control Protocol and contains Ethernet control protocols such as Spanning Tree BPDUs, LACP, Pause frames, etc. A L2CP frame has a specific destination address (DA) belonging to reserved multicast MAC address ranges. MEF defines L2CP processing rules for Ethernet Frames carrying a MAC destination address (DA) within the range of 01-80-C2-00-00-00 through 01-80-C2-00-00-0F and 01-80-C2-00-00-20 through 01-80-C2-00-00-2F. Therefore, if a vendor defines L2CP frames outside the specified MAC DA ranges, the L2CP handling rules do not apply to these frames.



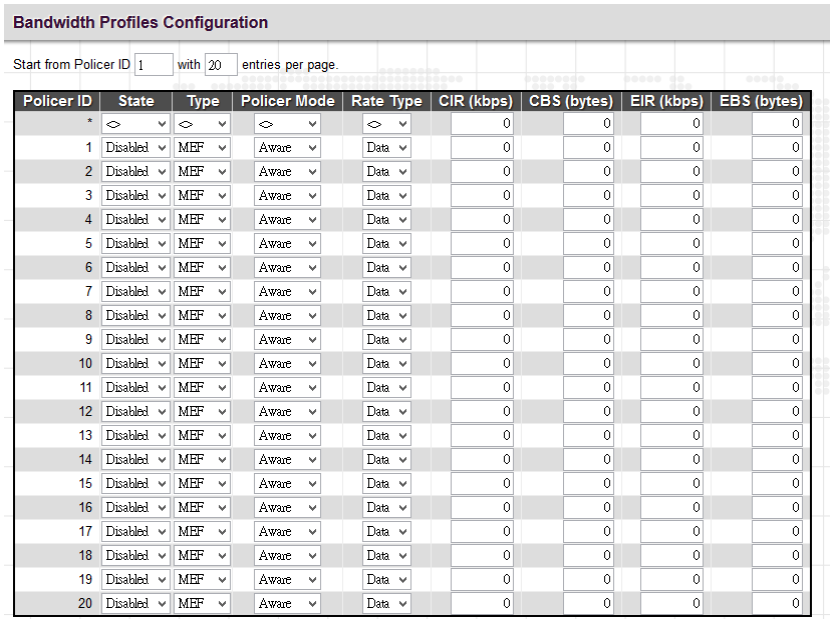
DMAC: The destination MAC address. The MAC DA range for Bridge block of protocol is 01-80-C2-00-00-00 through 01-80-C2-00-00-0F and for GARP block of protocol is 01-80-C2-00-00-20 through 01-80-C2-00-00-2F.

L2CP Mode: Select the L2CP frame handling mode for the corresponding destination MAC address (DMAC).

Peer: Redirect to CPU to allow peering/tunneling/discard depending on ECE and protocol configuration.

Forward: Allow peering/forwarding/tunneling/discarding depending on ECE and protocol configuration.

3.22.3 Bandwidth Profiles



Bandwidth Profiles Configuration

Start from Policer ID 1 with 20 entries per page.

Policer ID	State	Type	Policer Mode	Rate Type	CIR (kbps)	CBS (bytes)	EIR (kbps)	EBS (bytes)
*	<>	<>	<>	<>	0	0	0	0
1	Disabled	MEF	Aware	Data	0	0	0	0
2	Disabled	MEF	Aware	Data	0	0	0	0
3	Disabled	MEF	Aware	Data	0	0	0	0
4	Disabled	MEF	Aware	Data	0	0	0	0
5	Disabled	MEF	Aware	Data	0	0	0	0
6	Disabled	MEF	Aware	Data	0	0	0	0
7	Disabled	MEF	Aware	Data	0	0	0	0
8	Disabled	MEF	Aware	Data	0	0	0	0
9	Disabled	MEF	Aware	Data	0	0	0	0
10	Disabled	MEF	Aware	Data	0	0	0	0
11	Disabled	MEF	Aware	Data	0	0	0	0
12	Disabled	MEF	Aware	Data	0	0	0	0
13	Disabled	MEF	Aware	Data	0	0	0	0
14	Disabled	MEF	Aware	Data	0	0	0	0
15	Disabled	MEF	Aware	Data	0	0	0	0
16	Disabled	MEF	Aware	Data	0	0	0	0
17	Disabled	MEF	Aware	Data	0	0	0	0
18	Disabled	MEF	Aware	Data	0	0	0	0
19	Disabled	MEF	Aware	Data	0	0	0	0
20	Disabled	MEF	Aware	Data	0	0	0	0

Start Policer ID: The start Policer ID for displaying the table entries. The allowed range is from 1 through 2048.

Number of Entries per page: The number of entries per page. The allowed range is from 1through 999.

Policer ID: The Policer ID is used to identify one of the 2048 policers.

State: The administrative state of the bandwidth profile. The allowed values are:

Enabled: The bandwidth profile enabled.

Disabled: The bandwidth profile is disabled.

Type: The policer type of the bandwidth profile. The allowed values are:

MEF: MEF ingress bandwidth profile.

Single: Single bucket policer.

Policer Mode: The colour mode of the bandwidth profile. The allowed values are:

Coupled: Colour-aware mode with coupling enabled.

Aware: Colour-aware mode with coupling disabled.

Blind: Colour-blind mode.

Rate Type: The rate type of the bandwidth profile. The allowed values are:

Data: Specify that this bandwidth profile operates on data rate.

Line: Specify that this bandwidth profile operates on line rate.

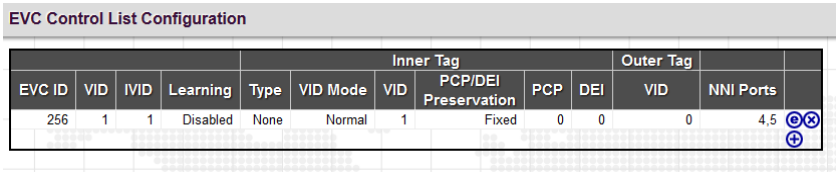
CIR: The Committed Information Rate (CIR) of the bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.

CBS: The Committed Burst Size (CBS) of the bandwidth profile. The allowed range is from 0 through 100000 bytes.

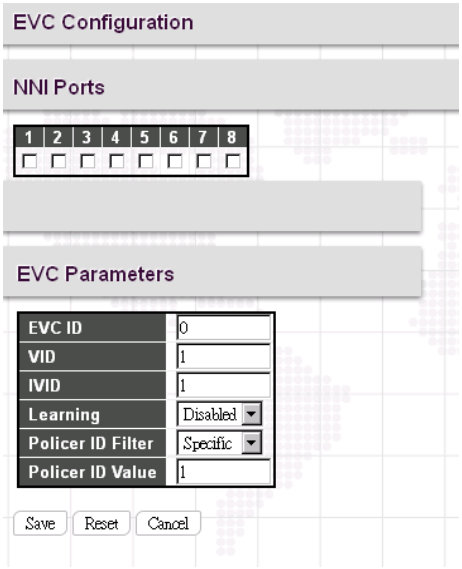
EIR: The Excess Information Rate (EIR) for MEF type bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.

EBS: The Excess Burst Size (EBS) for MEF type bandwidth profile. The allowed range is from 0 through 100000 bytes.

3.22.4 EVCs



Click on the plus sign ⊕ to add a new entry and configure its detailed settings.



NNI Ports: Select the network interface for EVC.

EVC Parameters

EVC ID: The EVC ID identifies the EVC. The allowed range is from 1 through 4096.

VID: The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The allowed range is from 1 through 4095.

IVID: The Internal/classified VLAN ID in the PB network. The allowed range is from 1 through 4095.

Learning: The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. The possible values are:

Enabled: Learning is enabled (MAC addresses are learned).

Disabled: Learning is disabled (MAC addresses are not learned).

Policer ID Filter: The ingress bandwidth profile mode for the EVC. The possible values are:

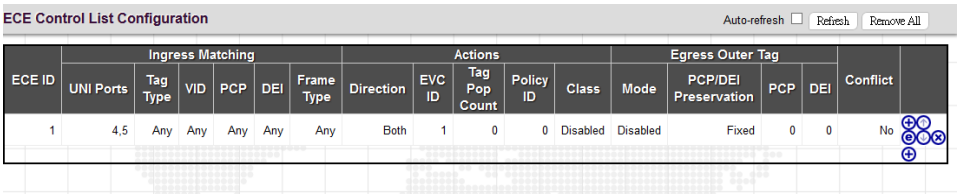
Specific: The allowed range is from 1 through 2048.

Discard: All received frames are discarded for the EVC.

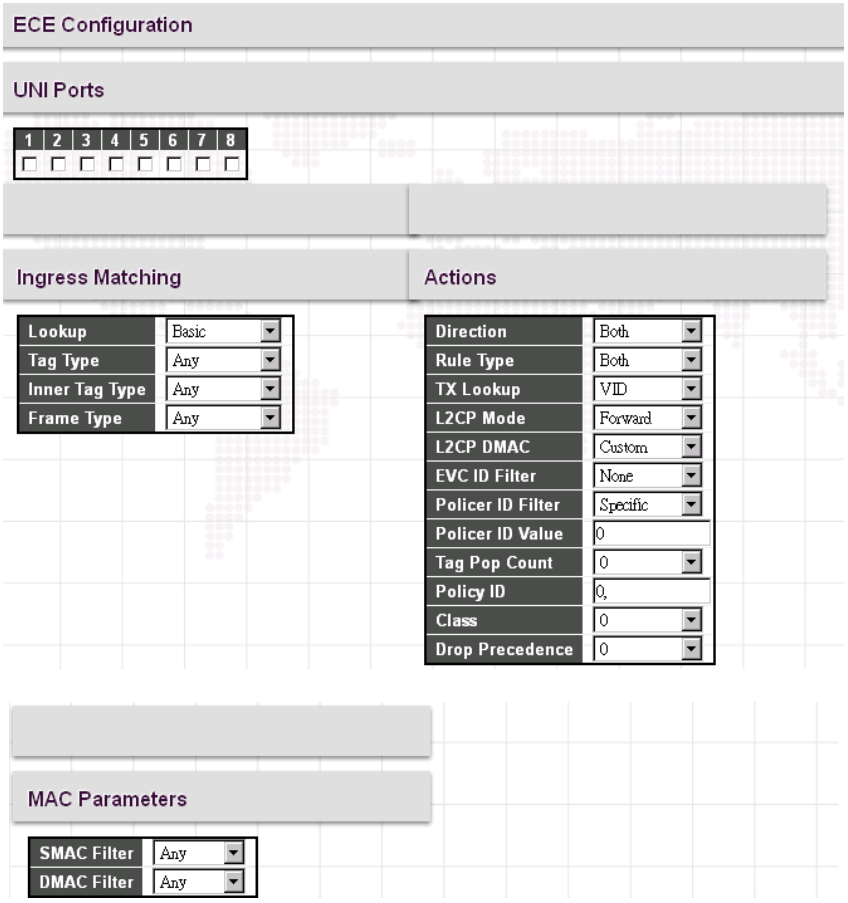
None: None bandwidth profile for the EVC.

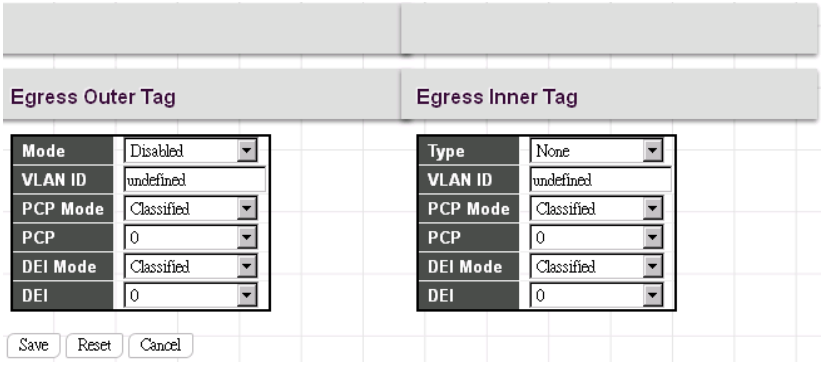
Policer ID Value: Specify a policer ID.

3.22.5 ECEs



Click on the plus sign to add a new entry and configure its detailed settings.





NNI Ports: Select the network interface for ECE.

Ingress Matching

Tag Type: The tag type for matching the ECE. The possible values are:

Any: The ECE will match both tagged and untagged frames.

Untagged: The ECE will match untagged frames only.

C-Tagged: The ECE will match custom tagged frames only.

S-Tagged: The ECE will match service tagged frames only.

Tagged: The ECE will match tagged frames only.

Frame Type: The frame type for the ECE. The possible values are:

Any: The ECE will match any frame type.

IPv4: The ECE will match IPv4 frames only.

IPv6: The ECE will match IPv6 frames only.

Actions

Direction: The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. The possible values are:

Both: Bidirectional.

UNI-to-NNI: Unidirectional from UNI to NNI.

NNI-to-UNI: Unidirectional from NNI to UNI.

EVC ID Filter: The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. The possible values are:

Any: No EVC ID filter is specified. (EVC ID filter status is "don't-care".)

Specific: If you want to filter a specific EVC ID with this ECE, choose this value. A field for entering a specific value appears.

EVC ID Value: When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 1 through 4096.

Tag Pop Count: The ingress tag pop count for the ECE. The allowed range is from 0 through 2.

Policy ID: The ACL Policy ID for the ECE for matching ACL rules. The allowed range is from 0 through 255.

Class: The traffic class for the ECE. The allowed range is from 0 to 7 and Disabled.

MAC Parameters

SMAC/DMAC Filter: The source and destination MAC address for matching ECE. This depends on the port address mode. When port address mode is set to “Source”, then the field is used for source MAC address. Similarly when port address mode is set to “Destination”, then the field is used for destination MAC address.

Any: No SMAC or DMAC file is specified.

Specific: Filter a specific SMAC or DMAC address with this ECE. When this option is selected, a field for entering a specific value appears. The legal format is “xx-xx-xx-xx-xx-xx” or “xxxxxxxxxxxx”.

DMAC Type: The destination MAC address for matching this ECE. The possible values are:

Any: No destination MAC is specified.

Unicast: Frames must be unicast.

Multicast: Frames must be multicast.

Broadcast: Frames must be broadcast.

Egress Outer Tag

Mode: The outer tag for nni-to-uni direction for the ECE. The possible values are:

Enable: Enable outer tag for nni-to-uni direction for the ECE.

Disable: Disable outer tag for nni-to-uni direction for the ECE.

PCP/DEI Preservation: The outer tag PCP and DEI preservation for the ECE. The possible values are:

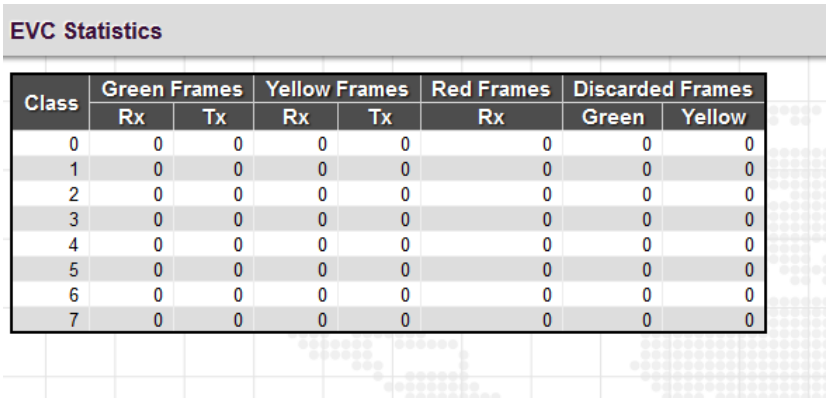
Preserved: The outer tag PCP and DEI is preserved.

Fixed: The outer tag PCP and DEI is fixed.

PCP: The outer tag PCP value for the ECE. The allowed range is from 0 through 7.

DEI: The outer tag DEI value for the ECE. The allowed value is 0 or 1.

3.22.6 EVC Statistics


EVC Statistics

Class	Green Frames		Yellow Frames		Red Frames	Discarded Frames	
	Rx	Tx	Rx	Tx	Rx	Green	Yellow
0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0

Class: List the traffic class for EVC.

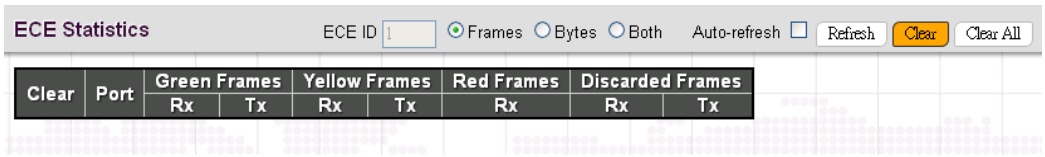
Green Frames Rx & Tx: The number of received and transmitted green frames.

Yellow Frames Rx & Tx: The number of received and transmitted yellow frames.

Red Frames Rx: The number of received red frames.

Discarded Frames Rx & Tx: The number of discarded frames in ingress and egress queue system.

3.22.7 ECE Statistics


ECE Statistics ECE ID 1 Frames Bytes Both Auto-refresh Refresh Clear Clear All

Clear	Port	Green Frames		Yellow Frames		Red Frames	Discarded Frames	
		Rx	Tx	Rx	Tx	Rx	Rx	Tx

Clear: Select the checkbox to mark an entry for clearance in next Clear operation.

Port: The UNI/NNI port number for the ECE.

Green Frames Rx & Tx: The number of received and transmitted green frames.

Yellow Frames Rx & Tx: The number of received and transmitted yellow frames.

Red Frames Rx: The number of received red frames.

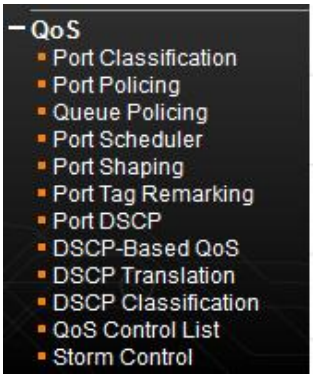
Discarded Frames Rx & Tx: The number of discarded frames in ingress and egress queue system.

3.23 QoS

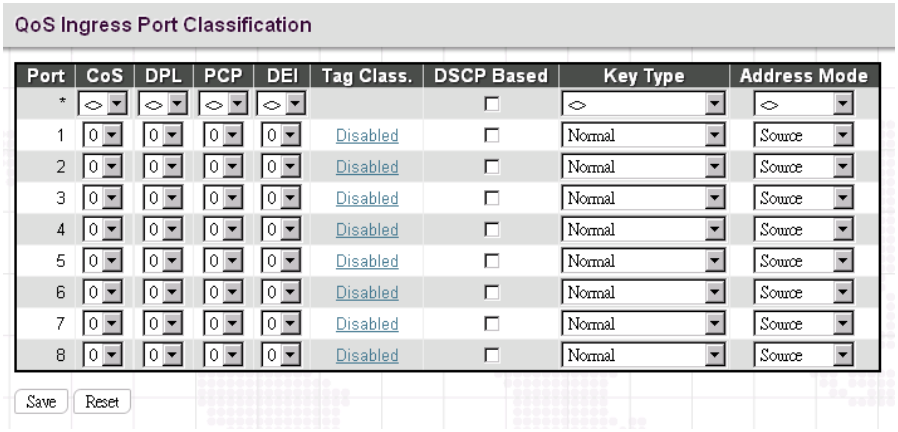
Network traffic is always unpredictable and the only basic assurance that can be offered is the best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria and receives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



3.23.1 Port Classification



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

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

DPL: Select the default Drop Precedence Level.

PCP: Select the appropriate value for the default Priority Code Point (or User Priority) for untagged frames.

DEI: Select the appropriate value for the default Drop Eligible Indicator for untagged frames.

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

Disabled: Use the default QoS class and DP level for tagged frames.

Enabled: Use the mapped versions of PCP and DEI for tagged frames.

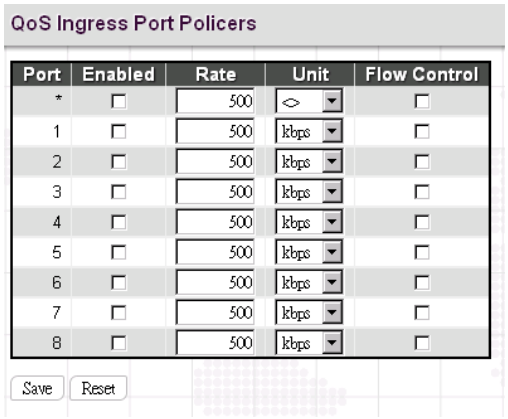
DSCP Based: Select the checkbox to enable DSCP based QoS (Ingress Port).

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

Source: Enable source IP/MAC matching.

Destination: Enable destination IP/MAC matching.

3.23.2 Port Policing



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

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

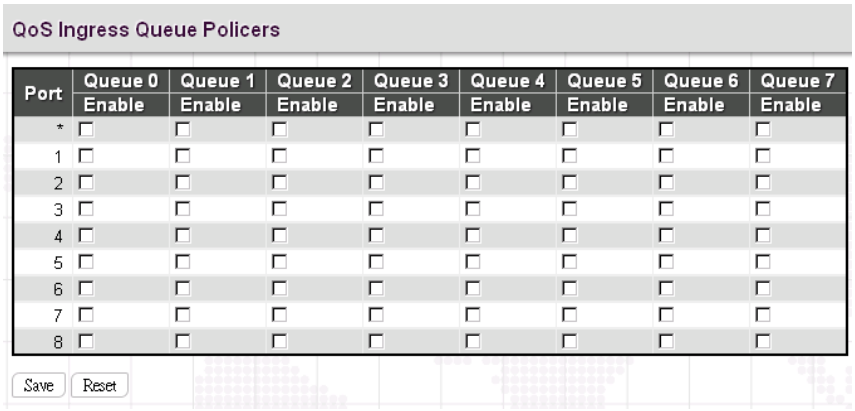
Enabled: Select the checkbox to enable port policing function on a port.

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.

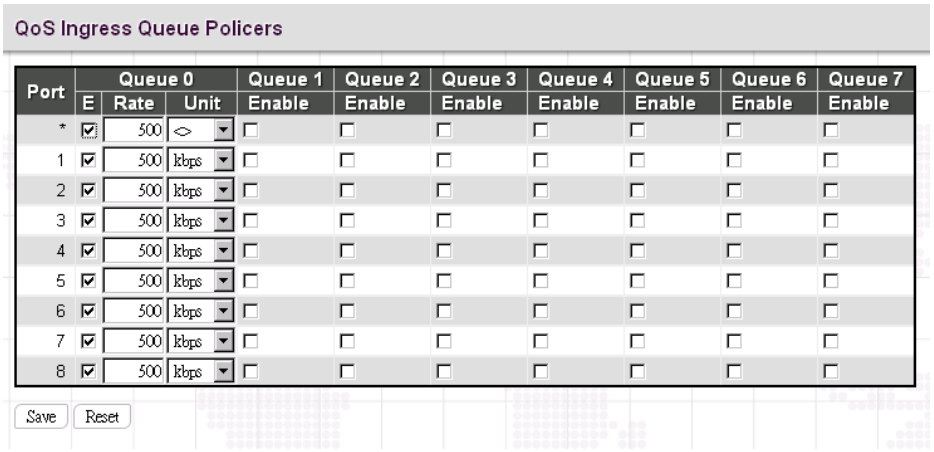
3.23.3 Queue Policing



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.

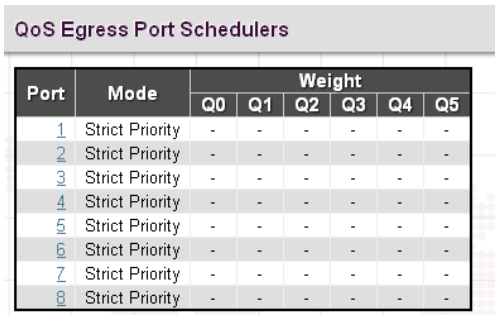
When enabled, the following image will appear:



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.

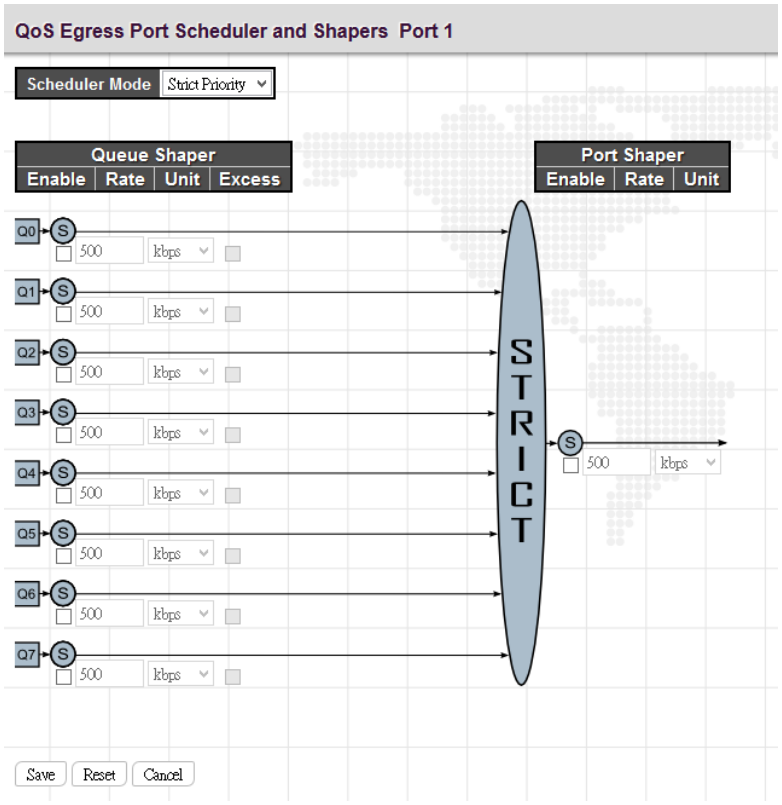
3.23.4 Port Scheduler

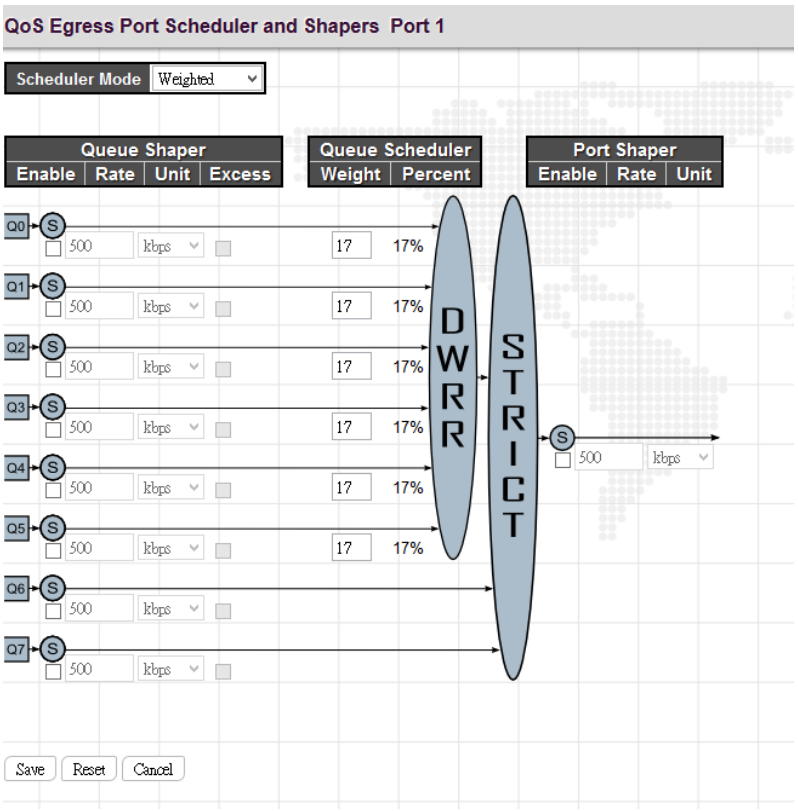


Port: Click the port to set up detailed settings for port scheduler.

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

3.23.5 Port Shaping

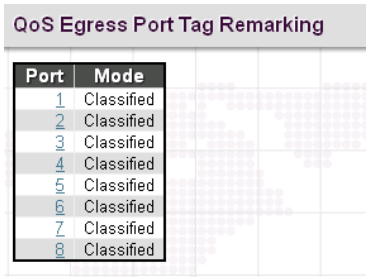
QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

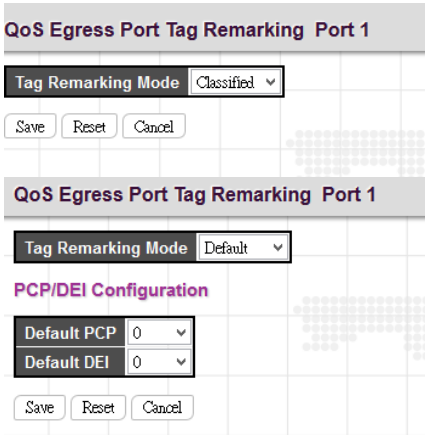
This displays each port's queue shaper and port shaper's rate.

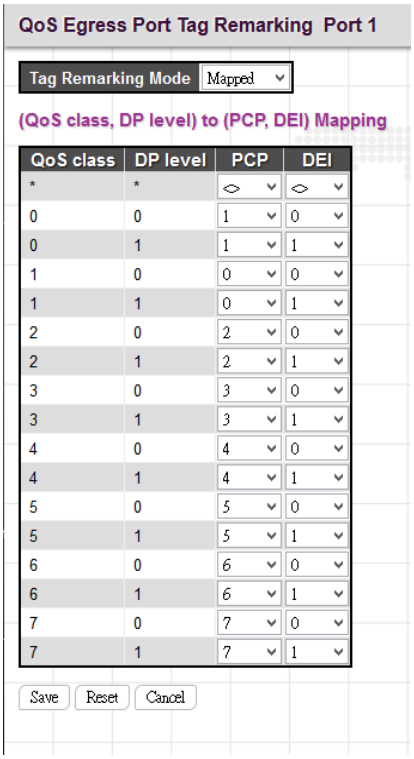
Click the port number to modify or reset queue shaper and port shaper's rates. See "Port Scheduler" for detailed explanation on each configuration option.

3.23.6 Port Tag Remarking



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





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

Classified: Use classified PCP/DEI values.

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

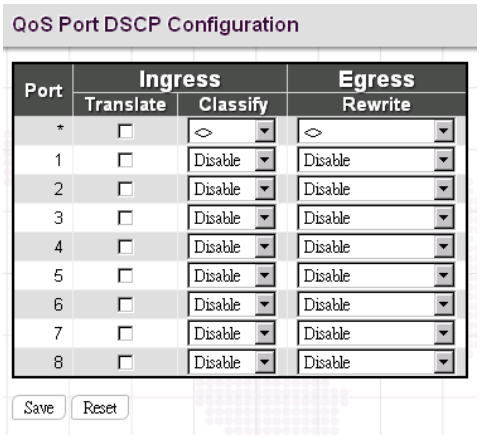
Mapped: Use the mapping of the classified QoS class values and DP levels to PCP/DEI values.

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

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

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

3.23.7 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.

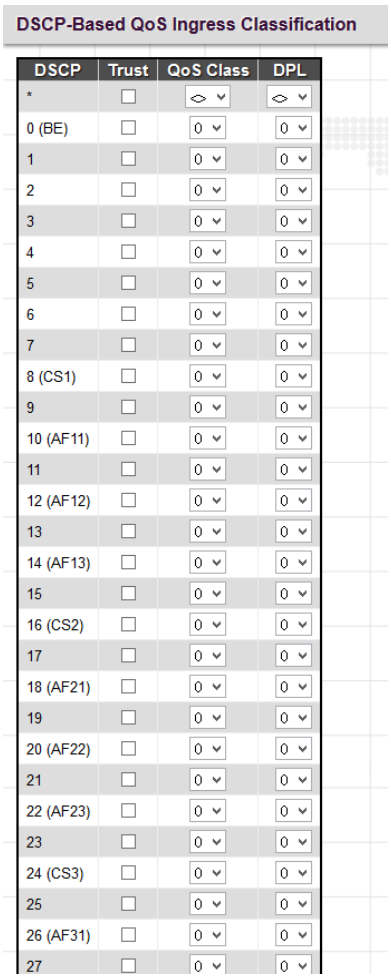
Disable: Egress rewriting is disabled.

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.

3.23.8 DSCP-Based QoS



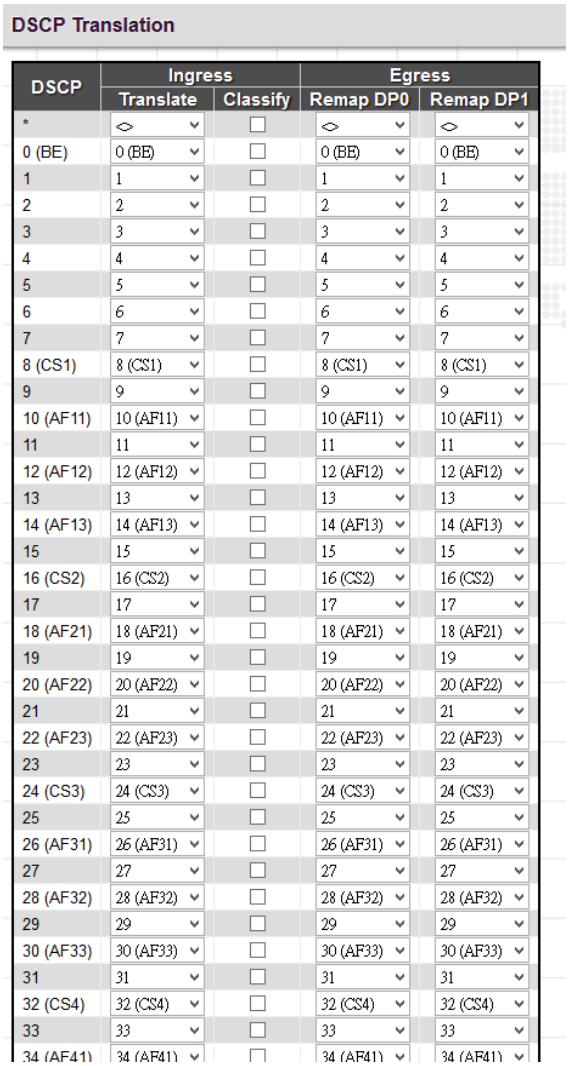
DSCP: DSCP value in ingress packet. DSCP range is from 0 to 63.

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.

3.23.9 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.

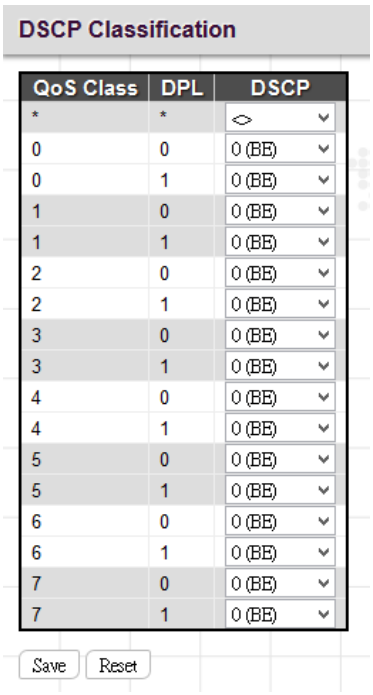
Ingress Translate: Enable Ingress Translation of DSCP values based on the specified classification method.

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.

3.23.10 DSCP Classification



Map DSCP values to QoS class and DPL value.

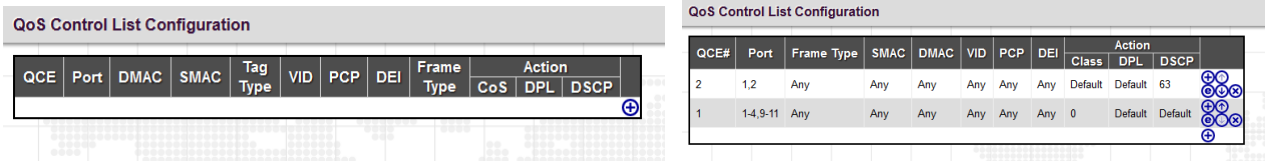
QoS Class: List of actual QoS class values.

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.

3.23.11 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.

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

SMAC: Source MAC address.

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

VID: Display VLAN ID (1~4095)

PCP: Display PCP value.

DEI: Display DEI value.

Frame Type: Display the frame type selected.

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

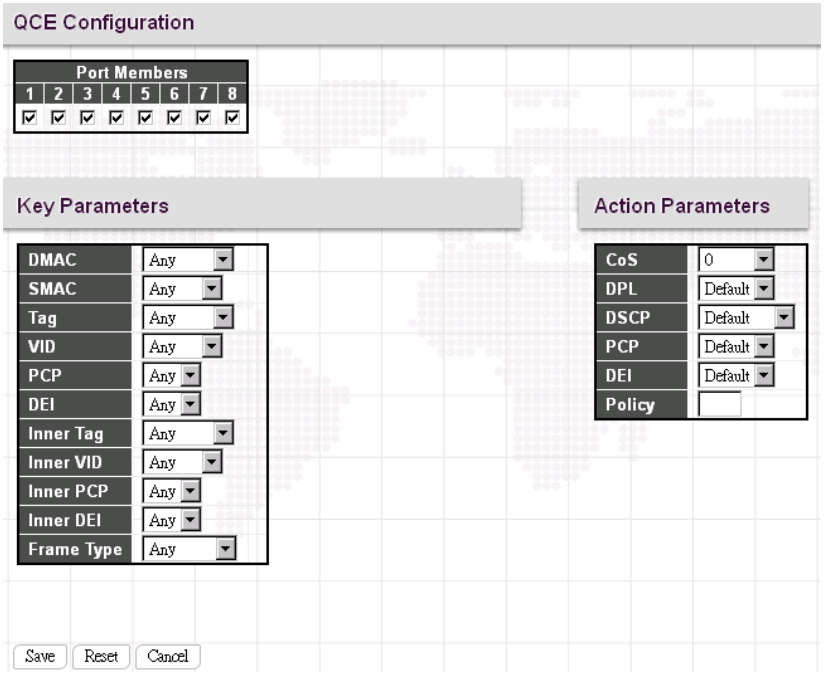
Class: If a frame matches the QCL, it will be put in the queue corresponding to the specified QoS class.

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

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

You can modify each QCE (QoS Control Entry) in the table using the following buttons:
: Insert a new QCE before the current row.
: Edit the QCE entry.
: Move the QCE up the list.
: Move the QCE down the list.
: Delete the QCE.
: The lowest plus sign add a new entry at the bottom of the QCE listings.

Once is clicked in display page, the following page will appear.



QCE Configuration

Port Members: Select ports that use this rule.

Key Parameters

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IPv4:

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

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

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

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

IPv6:

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

SIP 32 LSB: Select source IP type. By default, any is used. Select "Specific" to indicate self-defined source IP and submask format.

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

Action Parameters

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

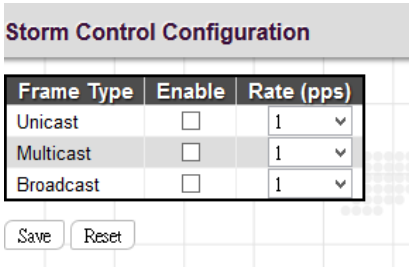
CoS: If a frame matches the QCE, it will be put in the queue corresponding to the specified QoS class or placed in a queue based on basic classification rules.

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

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

3.23.12 Storm Control

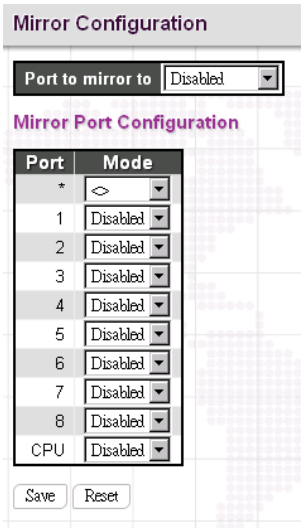
Storm Control is used to keep a network from downgraded performance or a complete halt by setting up a threshold for traffic like broadcast, unicast and multicast. When a device on the network is malfunctioning or application programs are not well designed or properly configured, storms may occur and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

3.24 Mirroring



Port to mirror: Select the mirror port to which rx or tx traffic will be mirrored. Or disable port mirroring function.

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

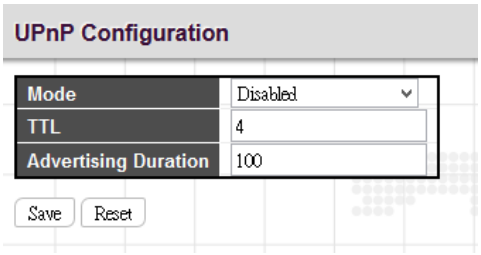
Disabled: Disable the port mirroring function on a given port.

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

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

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

3.25 UPnP



Mode: Enable or disable UPnP operation.

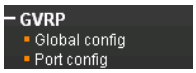
TTL: TTL (Time to live) is used to configure how many steps an UPnP advertisement can travel before it disappears.

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.

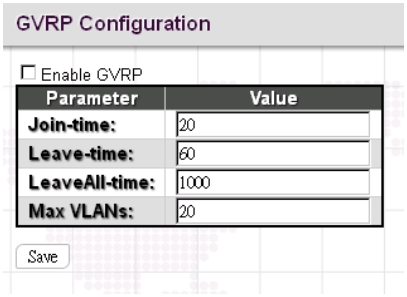
3.26 GVRP

GVRP (GVRP VLAN Registration Protocol) is defined in the IEEE 802.1Q standard and enables the switch to dynamically create IEEE 802.1Q compliant VLANs between GVRP-enabled devices. With GVRP, VLAN information can be automatically propagated from device to device so as to reduce errors when creating VLANs manually and provide VIDs consistency across network.

This section provides configuration pages for users to set up GVRP timers and enable GVRP on a per-port basis.



3.26.1 Global Config



Enable GVRP: Select the checkbox to globally enable GVRP function.

Join-time: Specify the amount of time in units of centi-seconds that PDUs are transmitted. The default value is 20 centi-seconds. The valid value is 1~20.

Note: *The "Leave-time" parameter must be three times greater than or equal to Join time.*

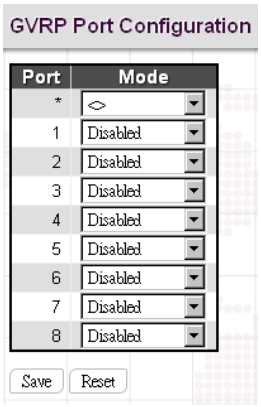
Leave-time: Specify the amount of time in units of centi-seconds that the device waits before deleting the associated etry. The leave time is activated by a "Leave All-time" message sent/received and cancelled by the Join message. The default value is 60 centi-seconds.

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

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

Max VLANs: The maximum number of VLANs can be learned via GVRP.

3.26.2 Port Config

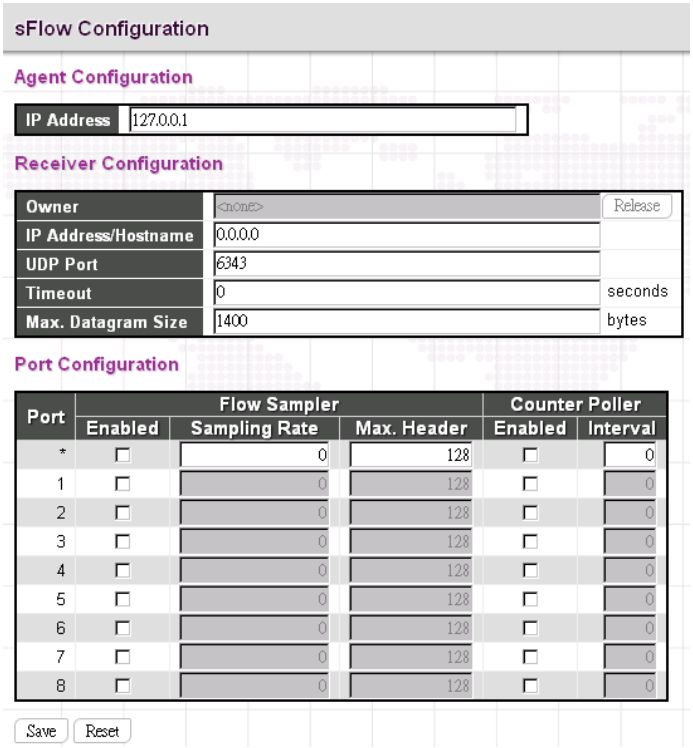


Port: The port number.

Mode: Enable GVRP on a per port basis.

3.27 sFlow

3.27.1 Configuration



Agent Configuration

IP Address: Specify an valid IPv4 or IPv6 address for sFlow agent.

Receiver Configuration

Owner: Basically, sFlow can be configured in two ways. One is through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

The button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

IP Address Hostname: Specify the IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

UDP Port: The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

Timeout: The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds.

Max. Datagram Size: The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration

Port: The port number for which the configuration below applies.

Flow Sampler Enabled: Enables flow sampling on this port. Uncheck the box will disable flow sampling on the this specific port.

Flow Sampler Sampling Rate: The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field. Valid range is 1 to 4294967295.

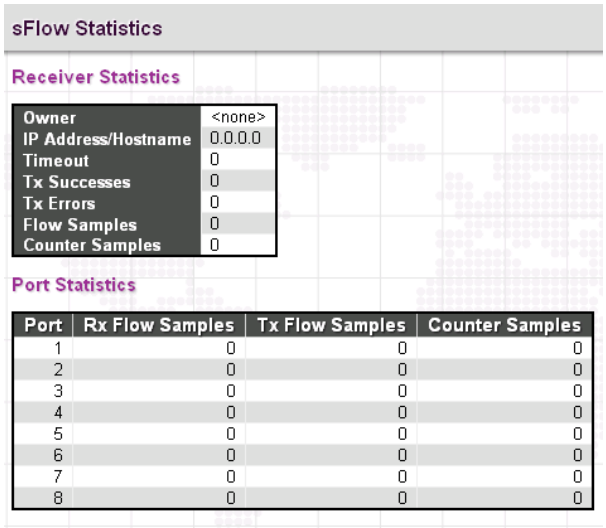
Flow Sampler Max. Header: The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

Counter Poller Enabled: Enable counter polling on this port. Uncheck the box to disable Counter Poller function on this port.

Counter Poller Interval: With counter polling enabled, this specifies the interval - in seconds - between counter poller samples. Valid range is 1 to 3600 seconds.

Save Button: Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.

3.27.2 Statistics



This page shows receiver and per-port sFlow statistics.

Receiver Statistics

Owner: This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:
- If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
- If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

IP Address/Hostname: This field shows the IP address or hostname of the sFlow receiver.

Timeout: This shows the number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes: The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors: The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6).

Flow Samples: The total number of flow samples sent to the sFlow receiver.

Counter Samples: The total number of counter samples sent to the sFlow receiver.

Port Statistics

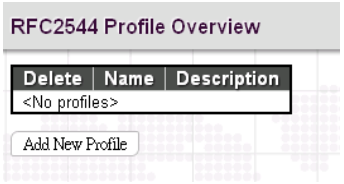
Port: The port number for which the following statistics applies.

Rx and Tx Flow Samples: The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

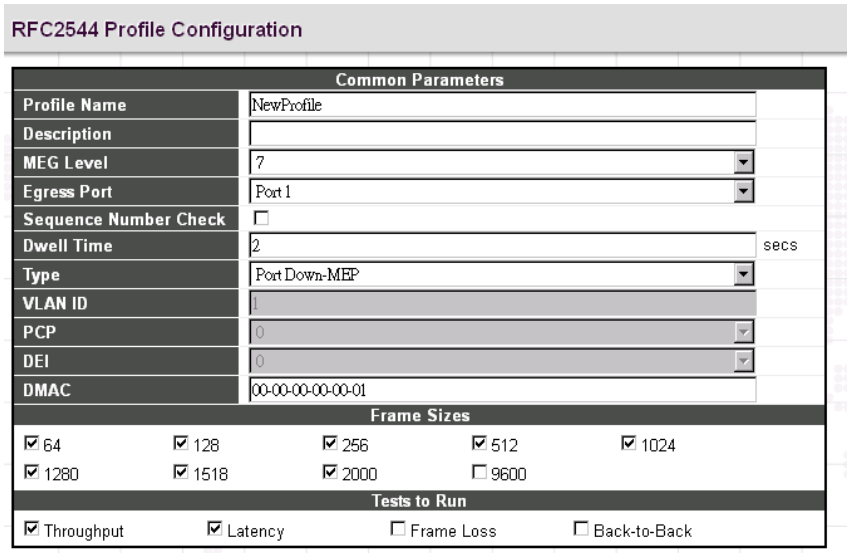
Counter Samples: The total number of counter samples sent to the sFlow receiver originating from this port.

3.28 RFC2544

3.28.1 Profiles



Click “Add New Profile” to create a new profile entry or click on the “Name” to mdoify the existing profile.



Profile Name: Enter a unique name for this profile. The profile name character must be from 1 to 32.

Description: Enter the descriptive text for this profile.

MEG Level: The frame types used in the various tests are Y.1731 TST and 1DM frames, both of which contain a MEG Level (MEL) field, which can be controlled with the value entered here. The MEG level ranges from 0 to 7 with 7 being the default.

Egress Port: Select the egress port that the generated frames are transmitted and expectedly received.

Sequence Number Check: When checked, looped Y.1731 TST frames are tested for out-of-order upon reception. Out-of-order frames are frames received in a different order than they were transmitted. If an out-of-order sequence is detected, the sub-test or trial is considered failing.

Dwell Time: When a trial is executed, Y.1731 TST frames are transmitted for a certain period of time. When that period has elapsed, the Dwell Time determines how long to wait before reading hardware counters and status in order to assess the status of the trial. The required dwell time must be at least the worst case roundtrip time, and therefore a.o. depends on the physical distance between the near and far ends. Valid range is from 1 to 10 with a default of 2 seconds.

Type: The RFC2544 test suite supports two types of tagging of frames on egress:

Port Down-MEP: All frames are transmitted untagged.

VLAN-based Down-MEP: All frames are transmitted with a VLAN tag. In order for this to work, the following manual VLAN configuration of the egress port is required:

- The VLAN Port Mode must be Trunk or Hybrid in order to get frames tagged upon transmission.
- The VLAN Port Type must be either of C-, S-, or S-Custom.
- VLAN Egress Tagging must be set to either tag all or untag Port VLAN. In the latter case the chosen VLAN ID for the profile must be different from the configured VLAN Port VLAN ID.
- The port must be member of the chosen VLAN ID.

Whether one or the other type is selected, frames are generated as close to the egress port as possible (hence the "Down-MEP" term) and therefore not sent through the queueing system, due to lack of integration with EVCs in this version of the software.

When VLAN-based Down-MEP is selected, the VLAN tag's ID, PCP, and DEI values are selected with the subsequent fields.

VLAN ID: When Type is set to VLAN-based Down-MEP, this field determines the VLAN ID used in the tag. Valid values are in the range 1 to 4095.

PCP: When Type is set to VLAN-based Down-MEP, this field determines the PCP value used in the VLAN tag.

DEI: When Type is set to VLAN-based Down-MEP, this field determines the DEI value used in the VLAN tag.

DMAC: This field determines the destination MAC address used in generation of the Y.1731 TST and 1DM frames. The source MAC address will automatically become the egress port's native MAC address. Note that it is important that the remote end swaps DMAC and SMAC while looping the frame.

Frame Sizes: Each sub-test is repeated for every selected frame size. At least one frame size must be checked. By default, all but the jumbo frame size are selected.

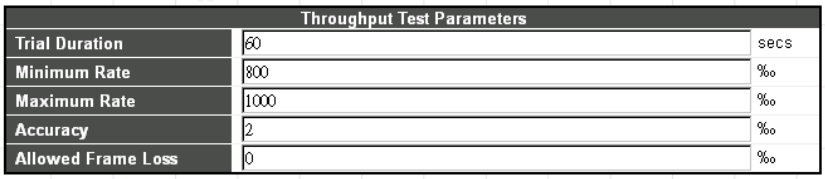
Tests to Run: One or more of the following sub-tests may be executed through the same profile.

Throughput: The throughput test searches for the maximum rate at which at most a certain percentage of the frames are lost. The throughput test starts at the maximum configured rate and uses a dichotomist algorithm (binary search) to find the optimum rate. The trials continue until the difference between a failing and succeeding rate is smaller than the configured accuracy.

Latency: The latency test measures the round-trip time of frames leaving the near-end until they get back to the near-end. Y.1731 TST frames are transmitted at the maximum rate determined by the throughput test less 200 Kbps. Every time, a Y.1731 1DM frame is transmitted and the time from this frame leaves the switch until it comes back is measured. If more than two 1DM frames are transmitted during a trial, also the delay variation will be part of the generated report. Selecting the latency test causes the throughput test to be selected automatically.

Frame Loss: The frame loss test measures frame loss at configurable transmission rates. It starts at the configured maximum rate and steps down by the configured step size and stops when two consecutive trials have zero frame loss (test succeeded in that case) or the minimum rate is reached (test failed in that case). For each trial, the report displays the frame loss ratio.

Back-to-Back: The back-to-back test aims to measure the network's ability to absorb bursty traffic. The test runs at line rate less 200 Kbps, and bursts of Y.1731 TST frames are generated a configurable number of times. The duration of a burst is configured in milliseconds, and the time from one burst ends until the next starts is configured through the Dwell Time.



Throughput Test Parameters		
Trial Duration	60	secs
Minimum Rate	800	‰
Maximum Rate	1000	‰
Accuracy	2	‰
Allowed Frame Loss	0	‰

Throughput Test Parameters

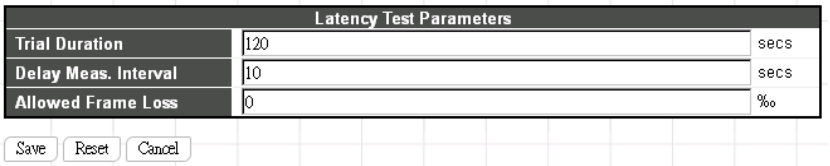
Trial Duration: The time - in seconds - to transmit Y.1731 TST frames at one given rate and frame size. This is known as a "trial". Valid range is from 1 to 1800 with a default of 60 seconds.

Minimum Rate: The minimum rate - in per mille of the egress port's line rate - to transmit Y.1731 TST frames at. If a trial fails at this rate, the test fails. Valid range is from 1 to 1000 with a default of 800 per mille of the line rate.

Maximum Rate: The maximum rate - in per mille of the egress port's line rate - transmit Y.1731 TST frames at while searching for maximum throughput. This is the rate that the search starts at. Valid range is from 1 to 1000 with a default of 1000 per mille of the line rate.

Accuracy: This specifies the stop criterion for the search for a maximum throughput rate. When the difference between a failing and succeeding rate is smaller than the accuracy, the search stops and the succeeding rate becomes the result. Valid range is from 1 to 1000 with a default of 2 per mille of the line rate.

Allowed Frame Loss: In some cases, it may be acceptable to have loss on a connection. The allowed loss can be specified with this parameter. The loss is measured in per mille of the number of transmitted frames during a trial, so if allowed loss is set to e.g. 1 per mille and 1000 frames are transmitted during a trial, the trial will be considered successful if 999 or 1000 frames return to the transmitter. Valid range is from 0 to 100 with a default of 0 per mille of the number of transmitted frames.



Latency Test Parameters		
Trial Duration	120	secs
Delay Meas. Interval	10	secs
Allowed Frame Loss	0	‰

Save Reset Cancel

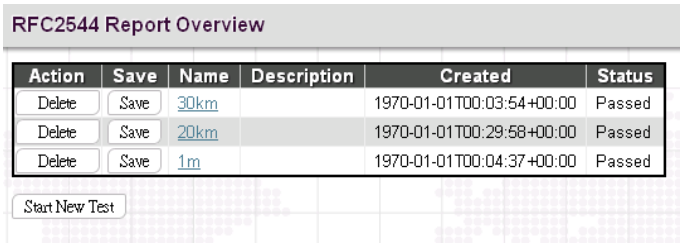
Latency Test Parameters

Trial Duration: The time - in seconds - to transmit Y.1731 TST frames at one given rate and frame size. This is known as a "trial". Valid range is from 10 to 1800 with a default of 120 seconds.

Delay Measurement Interval: This controls the period - in seconds - at which Y.1731 1DM frames are transmitted. The first 1DM frame is transmitted this number of seconds after the trial has started. The total number of transmitted 1DM frames in one trial therefore depends on the configured trial duration. Valid range is from 1 to 60 with a default of 10 seconds.

Allowed Frame Loss: In some cases, it may be acceptable to have loss on a connection. The allowed loss can be specified with this parameter. A trial is considered failing if more than this percentage of frames are lost. Valid range is from 0 to 100 with a default of 0 per mille of the number of transmitted frames.

3.28.2 Report



This page provides an overview of the currently stored reports along with options for deleting, downloading, and viewing them. Also initiation of execution of a profile is also handled through this page.
If no reports are currently stored, the table contains one line stating "<No test reports>". Otherwise there is a table row for each test report, each containing these elements:

Action: Click on the “Delete” button to remove the entry.

Save: Test reports can be downloaded and stored on the local computer with the use of the “Save” button. The suggested file name will be the report name concatenated with ".txt".

Name: A unique name identifying the report. Click the name to view the report.

Description: The description assigned to the report as entered on the test execution page.

Created: The date and time at which execution started.

Status: This field shows the current status of executing a test:

Inactive: Test just initiated, but not started. This is a transitional state that is unlikely to be noticed.

Executing: Test is currently executing. At most one test can execute at a time.

Cancelling: Test has just been stopped by the user. This is a transitional state that is unlikely to be noticed.

Cancelled: Test was stopped by the user and report is stored in non-volatile memory.

Passed: Test passed successfully and the report is stored in non-volatile memory.

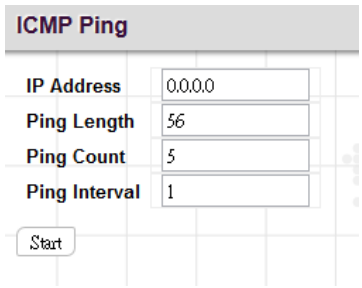
Failed: Test failed execution and report is stored in non-volatile memory. Details as to why the test failed are embedded in the report.

3.29 Diagnostics

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

3.29.1 Ping

This Ping function is for ICMPv4 packets.



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

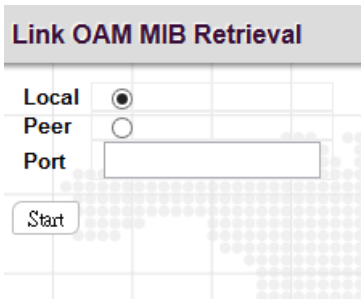
Ping Length: The size or length of echo packets.

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

Ping Interval: The time interval between each ping request.

3.29.2 Link OAM

3.29.2.1 MIB Retrieval

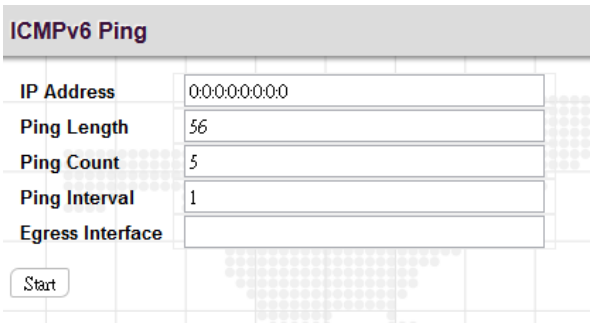


Local or Peer: Click on the radio button to select the location of MIB to be polled.

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

3.29.3 Ping6

This Ping function is for ICMPv6 packets.



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

Ping Length: The size or length of echo packets.

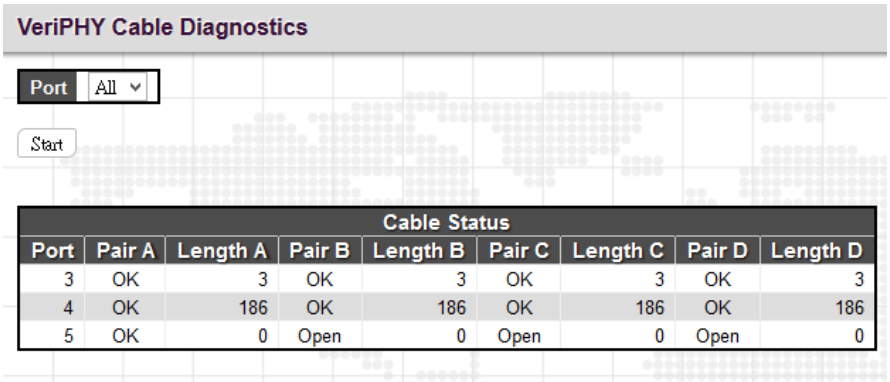
Ping Count: The number of echo packets will be sent.

Ping Interval: The time interval between each ping request.

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

3.29.4 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.

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

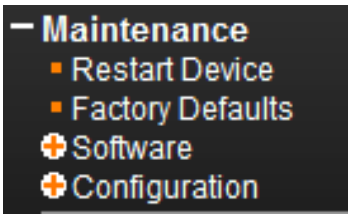
Cross D: Abnormal cross-pair coupling with pair D

Length: The length (in meters) of the cable pair. The resolution is ±3 meters.

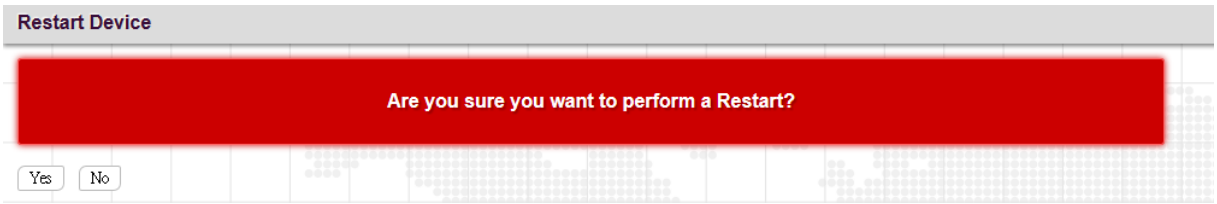
NOTE: *VeriPHY is only applicable to the electrical ports. It is not applicable to the optical ports.*

3.30 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.



3.30.1 Restart Device



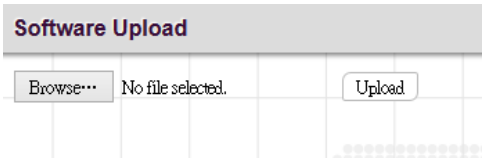
Click “Yes” button to reboot the switch.

3.30.2 Factory Defaults

Click “Yes” button to reset your device to factory defaults settings. Please note that all changed settings will be lost. It is recommended that a copy of the current configuration is saved to your local device.

3.30.3 Software

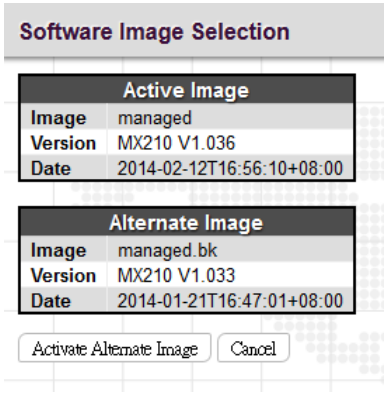
3.30.3.1 Upload



Update the latest Firmware file.

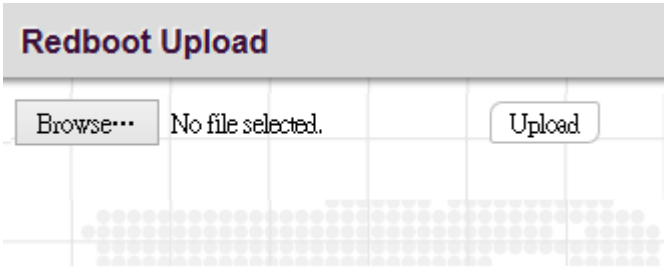
Select a Firmware file from your local device and then click “Upload” to start updating.

3.30.3.2 Image Select



Select the image file to be used in this device.

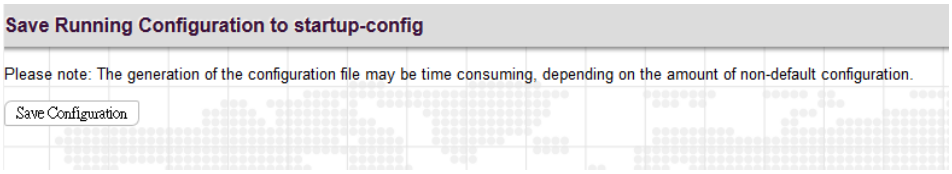
3.30.3.3 Upgrade boot code



Upgrade the latest redboot codes.

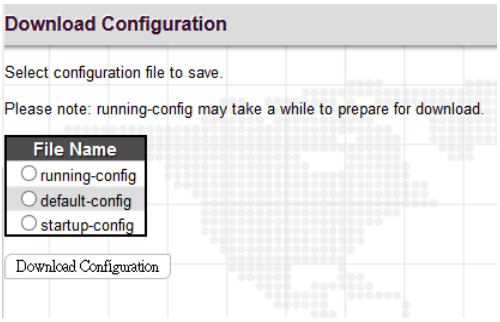
3.30.4 Configuration

3.30.4.1 Save



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

3.30.4.2 Download

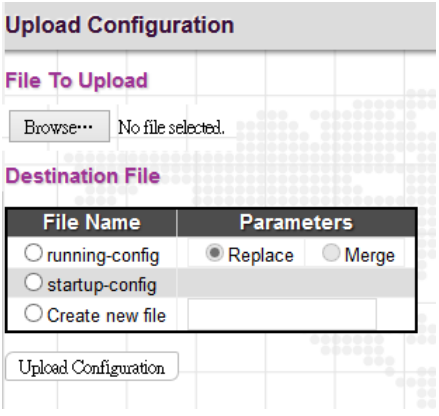


running-config: Download a copy of the current running configurations to your local device.

default-config: Download a copy of the factory default configurations to your local device.

startup-config: Download a copy of startup configurations to your local device.

3.30.4.3 Upload

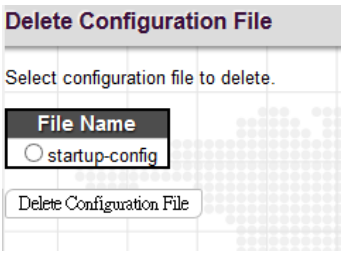


Select a file and then click “Upload Configuration” to start uploading the file.

3.30.4.4 Activate

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

3.30.4.5 Delete



Select the file that you would like to delete. Click on the “Delete Configuration File” to remove the file from the device.

This page is intentionally left blank.

CTC union®

www.ctcu.com

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