nivco professional

NGSME8H(x)(-AV)

8-(Rear)Port 10/100/1000Base-T PoE + 2 Gigabit SFP
Layer 2+ Full Management PoE Switch

NGSME16T2H(-AV)

16-(Rear)Port 10/100/1000Base-T(X) PoE + 2 Gigabit SFP Ports
Layer 2+ Full Management PoE Switch

NGSME24T2H(-AV)

24-(Rear)Port 10/100/1000Base-T PoE + 2 Gigabit SFP
Layer 2+ Full Management PoE Switch

User Manual

Version 2.2

FCC/CE Mark Warning

FCC Warning

This Equipment has been tested and found tocomply 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 in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark 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.

Table of Contents

Before Starting 10
Intended Readers 11
Icons for Note, Caution, and Warning 11
Chapter 1: Product Overview 12
1.1. Product Brief Description 13
1.2. Product Specification 15
1.3. Hardware Description 18
1.4. Hardware Installation 19
Chapter 2: Preparing for Management 20
2.1. Preparation for Serial Console 21
2.2. Preparation for Web Interface 23
2.3. Preparation for Telnet/SSH Interface 25
Chapter 3: Web Management 27
3.1. Web Management - Configure 28
3.1.1. Configuration - System 30
3.1.1.1. System - Information 30
3.1.1.2. System - IP 31
3.1.1.3. System - NTP 35
3.1.1.4. System - Time 36
3.1.1.5. System - Log 38
3.1.1.6. System - Virtual Stacking 39
3.1.2. Configuration - Green Ethernet 42
3.1.2.1. Green Ethernet - Port Power Savings 42
3.1.3. Configuration - Ports 44
3.1.4. Configuration - DHCP 46
3.1.4.1. DHCP - Server 46
3.1.4.1.1. DHCP - Server - Mode 46
3.1.4.1.2. DHCP - Server - Excluded IP 48
3.1.4.1.3. DHCP - Server - Pool 49
3.1.4.2. DHCP - Snooping 51
3.1.4.3. DHCP - Relay 52
3.1.5. Configuration - Security 54
3.1.5.1. Security - Switch - Users 54
3.1.5.2. Security - Switch - Privilege Level 56
3.1.5.3. Security - Switch - Authentication Method 58

Table of Contents

3.1.5.4. Security - Switch - SSH 59
3.1.5.5. Security - Switch - HTTPS 60
3.1.5.6. Security - Switch - Access Management 61
3.1.5.7. Security - Switch - SNMP 62
3.1.5.7.1. Security - Switch - SNMP - System 62
3.1.5.7.2. Security - Switch - SNMP - Trap 66
3.1.5.7.3. Security - Switch - SNMP - Community 68
3.1.5.7.4. Security - Switch - SNMP - User 69
3.1.5.7.5. Security - Switch - SNMP - Groups 71
3.1.5.7.5. Security - Switch - SNMP - Views 72
3.1.5.7.6. Security - Switch - SNMP - Access 73
3.1.5.8. Security - Switch - RMON 74
3.1.5.8.1. Security - Switch - RMON - Statistics 74
3.1.5.8.2. Security - Switch - RMON - History 75
3.1.5.8.3. Security - Switch - RMON - Alarm 76
3.1.5.8.4. Security - Switch - RMON - Event 78
3.1.5.9. Security - Network - Limit Control 79
3.1.5.10. Security - Network - NAS (Network Access Server) 82
3.1.5.11. Security - Network - ACL 93
3.1.5.11.1. Security - Network - ACL - Ports 93
3.1.5.11.2. Security - Network - ACL - Rate Limiter 95
3.1.5.11.3. Security - Network - ACL - Access Control List 96
3.1.5.12. Security - Network - IP Source Guard 112
3.1.5.12.1. Security - Network - IP Source Guard - Configuration 112
3.1.5.12.2. Security - Network - IP Source Guard - Static Table 113
3.1.5.13. Security - Network - ARP Inspection 114
3.1.5.13.1. Security - Network - ARP Inspection - Port Configuration 114
3.1.5.13.2. Security - Network - ARP Inspection - VLAN Configuration 116
3.1.5.13.3. Security - Network - ARP Inspection - Static Table 117
3.1.5.13.4. Security - Network - ARP Inspection - Dynamic Table 118
3.1.5.3. Security - AAA 120
3.1.5.3.1. Security - AAA - RADIUS 120
3.1.5.3.2. Security - AAA - TACACS+ 123
3.1.6. Configuration - Aggregation 125
3.1.6.1. Aggregation - Static 125
3.1.6.2. Aggregation - LACP 127
3.1.7. Configuration - Loop Protection 129

3.1.8. Configuration - Spanning Tree 131
3.1.8.1. Spanning Tree - Bridge Settings 131
3.1.8.2. Spanning Tree - MSTI Mapping 133
3.1.8.3. Spanning Tree - MSTI Priorities 135
3.1.8.4. Spanning Tree - CIST Ports 136
3.1.8.5. Spanning Tree - MSTI Ports 139
3.1.9. Configuration - IPMC Profile 141
3.1.9.1. IPMC Profile - Profile Table 141
3.1.9.2. IPMC Profile - Address Entry 143
3.1.10. Configuration - MVR 144
3.1.11. Configuration - IPMC 148
3.1.11.1. IPMC - IGMP Snooping 148
3.1.11.1.1. IPMC - IGMP Snooping - Basic Configuration 148
3.1.11.1.2. IPMC - IGMP Snooping - VLAN Configuration 150
3.1.11.1.3. IPMC - IGMP Snooping - Port Group Filtering 153
3.1.11.2. IPMC - MLD Snooping 154
3.1.11.2.1. IPMC - MLD Snooping - Basic Configuration 154
3.1.11.2.2. IPMC - MLD Snooping - VLAN Configuration 156
3.1.11.2.3. IPMC - MLD Snooping - Port Group Filtering 159
3.1.12. Configuration - LLDP 160
3.1.12.1. LLDP - LLDP 160
3.1.12.2. LLDP - LLDP-MED 163
3.1.13. Configuration - PoE 170
3.1.14. Configuration - MAC Table 174
3.1.15. Configuration - VLANs 176
3.1.16. Configuration - Private VLAN 181
3.1.16.1. Private VLAN - Membership 181
3.1.16.2. Private VLAN - Port Isolation 183
3.1.17. Configuration - VCL 184
3.1.17.1. VCL - MAC-based VLAN 184
3.1.17.2. VCL - Port-based VLAN 186
3.1.17.2.1. VCL - Port-based VLAN - Protocol to Group 186
3.1.17.2.2. VCL - Port-based VLAN - Group to VLAN 188
3.1.17.3. VCL - IP Subnet-based VLAN 189
3.1.18. Configuration - Voice VLAN 191
3.1.18.1. Voice VLAN - Configuration 191
3.1.18.2. Voice VLAN - OUI 193

Table of Contents

3.1.19. Configuration - QoS 194
3.1.19.1. QoS - Port Classification 194
3.1.19.2. QoS - Port Policing 197
3.1.19.3. QoS - Port Scheduler 198
3.1.19.4. QoS - Port Shaping 202
3.1.19.5. QoS - Port Tag Remarking 206
3.1.19.6. QoS - Port DSCP 209
3.1.19.7. QoS - DSCP-Based QoS 211
3.1.19.8. QoS - DSCP Translation 212
3.1.19.9. QoS - DSCP Classification 214
3.1.19.10. QoS - QoS Control List 215
3.1.19.11. QoS - Storm Control 217
3.1.20. Configuration - Mirroring 218
3.1.21. Configuration - UPnP 220
3.1.22. Configuration - GVRP 221
3.1.22.1. GVRP - Global Config 221
3.1.22.2. GVRP - Port Config 222
3.1.23. Configuration - sFlow 223
3.2. Web Management - Monitor 226
3.2.1. Monitor - System 226
3.2.1.1. System - Information 226
3.2.1.2. System - CPU Load 228
3.2.1.3. System - IP Status 229
3.2.1.4. System - Log 231
3.2.1.5. System - Detailed Log 232
3.2.3. Monitor - Green Ethernet 233
3.2.3.1. Green Ethernet - Port Power Savings Status 233
3.2.4. Monitor - Ports 234
3.2.4.1. Ports - Traffic Overview 234
3.2.4.2. Ports - QoS Statistics 235
3.2.4.3. Ports - QCL Status 236
3.2.4.4. Ports - Detailed Statistics 238
3.2.5. Monitor - DHCP 241
3.2.5.1. DHCP - Server 241
3.2.5.1.1. DHCP - Server - Statistics 241
3.2.5.1.2. DHCP - Server - Binding 243
3.2.5.1.3. DHCP - Server - Declined IP 244

3.2.5.2. DHCP - Snooping Table 245
3.2.5.3. DHCP - Relay Statistics 247
3.2.5.4. DHCP - Detailed Statistics 249
3.2.6. Monitor - Security 251
3.2.6.1. Security - Access Management Statistics 251
3.2.6.2. Security - Network 252
3.2.6.2.1. Security - Network - Port Security - Switch 252
3.2.6.2.2. Security - Network - Port Security - Port 254
3.2.6.2.3. Security - Network - NAS - Switch 255
3.2.6.2.5. Security - Network - NAS - Port 257
3.2.6.2.6. Security - Network - ACL Status 262
3.2.6.2.7. Security - Network - ARP Inspection 264
3.2.6.2.8. Security - Network - IP Source Guard 266
3.2.6.3. Security - AAA 270
3.2.6.3.1. Security - AAA - RADIUS Overview 270
3.2.6.3.2. Security - AAA - RADIUS Details 272
3.2.6.4. Security - Switch - RMON 276
3.2.6.4.1. Security - Switch - RMON - Statistics 276
3.2.6.4.2. Security - Switch - RMON - History 279
3.2.6.4.3. Security - Switch - RMON - Alarm 281
3.2.6.4.4. Security - Switch - RMON - Events 283
3.2.7. Monitor - LACP 284
3.2.7.1. LACP - System Status 284
3.2.7.2. LACP - Port Status 285
3.2.7.3. LACP - Port Statistics 286
3.2.8. Monitor - Loop Protection 287
3.2.9. Monitor - Spanning Tree 288
3.2.9.1. Spanning Tree - Bridge Status 288
3.2.9.2. Spanning Tree - Port Status 289
3.2.9.3. Spanning Tree - Port Statistics 290
3.2.10. Monitor - MVR 291
3.2.10.1. MVR - Statistics 291
3.2.10.2. MVR - MVR Channel Groups 292
3.2.10.3. MVR - MVR SFM Information 293
3.2.11. Monitor - IPMC 295
3.2.11.1. IPMC - IGMP Snooping 295
3.2.11.1.1. IPMC - IGMP Snooping - Status 295

3.2.11.1.2. IPMC - IGMP Snooping - Groups Information 297
3.2.11.1.3. IPMC - IGMP Snooping - IPv4 SFM Information 298
3.2.11.2. IPMC - MLD Snooping 300
3.2.11.2.1. IPMC - MLD Snooping - Status 300
3.2.11.2.2. IPMC - MLD Snooping - Groups Information 302
3.2.11.2.3. IPMC - MLD Snooping - IPv6 SFM Information 303
3.2.12. Monitor - LLDP 305
3.2.12.1. LLDP - Neighbours 305
3.2.12.2. LLDP - LLDP-MED Neighbours 307
3.2.12.3. LLDP - PoE 311
3.2.12.4. LLDP - EEE 313
3.2.12.5. LLDP - Port Statistics 315
3.2.13. Monitor - PoE 317
3.2.14. Monitor - MAC Table 319
3.2.15. Monitor - VLANs 321
3.2.15.1. VLANs - VLAN Membership 321
3.2.15.2. VLANs - VLAN Ports 323
3.2.16. Monitor - VCL 325
3.2.16.1. VCL - MAC-based VLAN 325
3.2.17. Monitor - sFlow 326
3.3. Web Management - Diagnostics 328
3.3.1. Diagnostics - Ping 328
3.3.2. Diagnostics - Ping6 330
3.3.3. Diagnostics - VeriPHY 332
3.4. Web Management - Maintenance 334
3.4.1. Maintenance - Restart Device 334
3.4.2. Maintenance - Factory Defaults 335
3.4.3. Maintenance - Software 336
3.4.3.1. Software - Upload 336
3.4.3.2. Software - Image Select 337
3.4.4. Maintenance - Configuration 338
3.4.4.1. Configuration - Save Startup-config 338
3.4.4.2. Configuration - Download 339
3.4.4.3. Configuration - Upload 340
3.4.4.4. Configuration - Activate 341
3.4.4.5. Configuration - Delete 342
Appendix A: Product Safety 343

Table of Contents

Appendix B: IP Configuration for Your PC 344
Appendix C: Glossary 347
Revision History 364

Before Starting

In Before Starting:

This section contains introductory information, which includes:

- **Intended Readers**
- **Icons for Note, Caution, and Warning**
- **Product Package Contents**

Intended Readers

This manual provides information regarding to all the aspects and functions needed to install, configure, use, and maintain the product you've purchased.

This manual is intended for technicians who are familiar with in-depth concepts of networking management and terminologies.

Icons for Note, Caution, and Warning

To install, configure, use, and maintain this product properly, please pay attention when you see these icons in this manual:



A **Note** icon indicates important information which will guide you to use this product properly.



A **Caution** icon indicates either a potential for hardware damage or data loss, including information that will guide you to avoid these situations.



A **Warning** icon indicates potentials for property damage and personal injury.

Chapter 1 :

Product Overview

In Product Overview:

This section will give you an overview of this product, including its feature functions and hardware/software specifications.

- **Product Brief Description**
- **Product Specification**
- **Hardware Description**
- **Hardware Installation**

1.1. Product Brief Description

Introduction

This switch is 8/16/24-port 10/100/1000M PoE + 2 Gigabit SFP Ports L2+ Full Managed Switch that is designed for small or medium network environment to strengthen its network connection. The 8/16/24 PoE ports support IEEE 802.3at/af PoE technology, up to 30W per port and maximum 100m transmission distance. The switch equipped with AC to DC power module to support 120W/235W/500W power budget for PoE power. The added 2 SFP/RJ45 combo ports support 100M and Gigabit Fiber transceiver for long distance transmission. The switch also supports Layer 2+ full management software features. These features are powerful to provide PoE Control, Network Control, Management, Monitor and Security features' requests. It is a superb choice to boost your network with better performance, efficiency and high PoE power consumption.

IEEE 802.3at/af Power over Ethernet (PoE) ports

This product can convert standard 100~240V/AC power into low-voltage DC that runs over existing LAN cable to power up IEEE 802.3at/af compliant network accessories. It also features PoE awareness to verify whether the network device receive power is IEEE 802.3at/af compliant, or only the data will be sent through LAN cable. By adding the switch to the existing networking, installing networking products such as Access Points and IP cameras can be easily managed and set up.

2 Gigabit SFP Open Slots

The switch supports 2 additional SFP open slots to uplink to servers, storage, or other switching devices for long reach applications. The 2 SFP slots support legacy 100M SFP transceiver. If the 100M fiber infrastructure is constructed and 100M bandwidth is enough, the 100M SFP transceiver can be an optional choice for the legacy 100M network environment.

Full Layer 2+ Management Features

The switch includes full Layer 2+ Management features. The software set includes up to 4K 802.1Q VLAN and advanced Protocol VLAN, Private VLAN, MVR…advanced VLAN features. There are 8 physical queues Quality of Service, IPv4/v6 Multicast filtering, Rapid Spanning Tree protocol to avoid network loop, Multiple Spanning Tree Protocol to integrate VLAN and Spanning Tree, LACP, LLDP; sFlow, port mirroring, cable diagnostic and advanced Network Security features. It also provides Console CLI for out of band management and SNMP, Web GUI for in band Management.

Advanced Security

The switch supports advanced security features. For switch management, there are secured HTTPS and SSH, the login password, configuration packets are secured. The port binding allows to bind specific MAC address to the port, only the MAC has the privilege to access the network. The 802.1X port based Access Control, every user should be authorized first when they want to access the network. AAA is the short of the Authentication, Authorization and Accounting with RADIUS, TACAS+ server. Layer 2+ Access Control List allows user to define the access privilege based on IP, MAC, Port number…etc.

PD Alive Check/Self healing

When this function is enabled, this switch will detect a network PoE powered device (for example, an IP CAM) with a set of IP address periodically. If the switch doesn't get any replies from the network PoE powered device, it will do a power cycle (PoE power OFF, and PoE power ON) to the port that connects the network PoE powered device, allowing that device to reboot. You can set the frequency of detecting, number of times of detecting, and the time period to perform power cycle when there's no reply via the switch's PoE configuration web page.

1.2. Product Specification

Interface		
10 Base-T/100 Base-TX/1000 Base-T RJ45 Ports		8/16/24
100/1000Base-SX/LX SFP Port		2
Console Port for CLI Management		1
System Performance		
Packet Buffer		4Mbits
MAC Address Table Size		8K
Switching Capacity		20Gbps/36Gbps/52Gbps
Forwarding Rate		14.88Mpps/26.78Mpps/38.7Mpps
PoE Features		
IEEE 802.3 af/at		IEEE 802.3 af/at
Number of PSE Ports		8/16/24
Max. Power Budget		120W/235W/500W
Max. System Power Consumption		10W
External/Internal Power		Internal Power
Power Feeding Detecting Capability on PD		•
PD Alive Check/Self healing		•
PD Classification		•
Power Management (per-port)	Enable/Disable PoE Per Port	•
	Priority Setting Per Port	•
	Power Level Setting Per Port	•
	Overloading Protection	•
L2 Features		
Auto-negotiation		•
Auto MDI/MDIX		•
Flow Control (duplex)	802.3x (Full)	•
	Back-Pressure (Half)	•
Spanning Tree	IEEE 802.1D (STP)	•
	IEEE 802.1w (RSTP)	•
	IEEE 802.1s (MSTP)	•
VLAN	VLAN Group	4K
	Tagged Based	•
	Port-based	•
	Voice VLAN	8 port: Voice VLAN with OUI
Link Aggregation	IEEE 802.3ad with LACP	•
	Static Trunk	•
	Max. LACP Link Aggregation Group	5/9/13
	Max. Port per Link Aggregation Group	8
IGMP Snooping	IGMP Snooping v1/v2/v3	Supports 1024 IGMP groups
	IGMP Static Multicast Addresses	Supports 1024 static multicast addresses
	IPv6 MLD Snooping	Supports 1024 MLD groups
	MLD Static Multicast Addresses	Supports 1024 static multicast addresses
	Querier, Immediate Leave	•
Storm Control (Broadcast/Multi-cast/Un-known Unicast)		•
Jumbo Frame Support		9.6KB

QoS Features		
Number of priority queue		8 queues/port
Rate Limiting	Ingress	Yes, 1KBps/1pps
	Egress	Yes, 1KBps/1pps
DiffServ (RFC2474 Remarking)		•
Scheduling (WRR, Strict, Hybrid)		•
CoS	IEEE 802.1p	•
	IP ToS precedence, IP DSCP	•
Security		
Management System User Name/Password Protection		•
User Privilege		Set user privilege up to 15 Level
Port Security (MAC-based)		•
IEEE 802.1x Port-based Access Control		•
ACL (L2/L3/L4)		•
IP Source Guard		•
RADIUS (Authentication, Authorization, Accounting)		•
TACACS+		•
HTTP & SSL (Secure Web)		•
SSH v2.0 (Secured Telnet Session)		•
MAC/IP Filter		•
Management		
Command Line Interface (CLI)		•
Web Based Management		•
Telnet		•
Access Management Filtering		SNMP/WEB/SSH/TELNET
Firmware Upgrade via HTTP		•
Dual Firmware Images		•
Configuration Download/Upload		•
SNMP (v1/v2c/v3)		•
RMON (1,2,3,&9 groups)		•
DHCP (Client/Relay/Option82/Snooping)		•
System Event/Error Log		•
NTP/LLDP		•
Cable Diagnostics		•
IPv6 Configuration		•
Port Mirroring		•
Mechanical		
Power Input		100~240VAC
Dimension (H*W*D)		44*330*210 mm/44*330*210 mm/44*440*331 mm
LED		Power, PoE, Link/Act, SFP
Operating Temperature		0~45°C
Storage Temperature		-20~80°C
Operating Humidity		5~90% (non-condensing)
Weight		2.2 KG/2.5 KG/4.8 KG
Certification		VCCI, CE, FCC Class A/CE, FCC Class A, cULus
Standard		
IEEE 802.3 – 10Base-T		•
IEEE 802.3u - 100Base-TX		•
IEEE 802.3ab - 1000Base-T		•
IEEE 802.3z - 1000 Base-SX/LX		•
IEEE 802.3af - Power over Ethernet (PoE)		•
IEEE 802.3at - Power over Ethernet (PoE+)		•
IEEE 802.3az - Energy Efficient Ethernet (EEE)		•
IEEE 802.3x - Flow Control		•
IEEE 802.1Q - VLAN		•

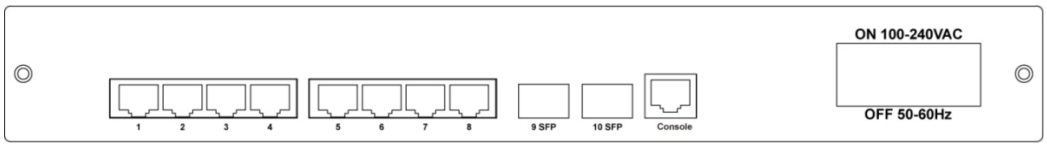
IEEE 802.1v - Protocol VLAN	•
IEEE 802.1p - Class of Service	•
IEEE 802.1D - Spanning Tree	•
IEEE 802.1w - Rapid Spanning Tree	•
IEEE 802.1s - Multiple Spanning Tree	•
IEEE 802.3ad - Link Aggregation Control Protocol (LACP)	•
IEEE 802.1AB - LLDP (Link Layer Discovery Protocol)	•
IEEE 802.1X - Access Control	•

1.3. Hardware Description

This section mainly describes the hardware of Full-Management PoE switch and gives a physical and functional overview on the certain switch.

Rear Panel

The front panel of the Full-Management PoE switch consists of 8/16/24 10/100/1000 Base-TX RJ-45 ports, 2 gigabit uplink SFP/RJ45 combo ports, and a power switch, and an IEC 60320 plug for power supply.



LED Indicators

The LED Indicators present real-time information of systematic operation status. The following table provides description of LED status and their meaning.

LED	Color / Status	Description
Power	Amber On	Power on
10/100/1000M	Green On	Link Up
	Green Blinking	Data Activating
PoE	Amber On	PD is connected
SFP	Green On	linked to Power Device
	Green Blinking	Data Activating

1.4. Hardware Installation

To install the Full-Management PoE switch, please place it on a large flat surface with a power socket close by. This surface should be clean, smooth, and level. Also, please make sure that there is enough space around the Full-Management PoE switch for RJ45 cable, power cord and ventilation.

If you're installing this Full-Management PoE switch on a 19-inch rack, please make sure to use the rack-mount kit (L brackets) and screws come with the product package. All screws must be fastened so the rack-mount kit and your product are tightly conjoined before installing it on your 19-inch rack.

Ethernet cable Request

The wiring cable types are as below:

- 10 Base-T: 2-pair UTP/STP CAT. 3, 4, 5 cable, EIA/TIA-568 100-ohm (Max. 100m)
- 100 Base-TX: 2-pair UTP/STP CAT. 5 cable, EIA/TIA-568 100-ohm (Max. 100m)
- 1000 Base-T: 4-pair UTP/STP CAT. 5 cable, EIA/TIA-568 100-ohm (Max. 100m)
- PoE: To delivery power properly, it is recommended to use CAT 5e and CAT 6 cable. Ethernet cables of higher qualities can reduce the power lost during transmission.

SFP Installation

While install the SFP transceiver, make sure the SFP type of the 2 ends is the same and the transmission distance, wavelength, fiber cable can meet your request. It is suggested to purchase the SFP transceiver with the switch provider to avoid any incompatible issue.

The way to connect the SFP transceiver is to Plug in SFP fiber transceiver fist. The SFP transceiver has 2 plug for fiber cable, one is TX (transmit), the other is RX (receive). Cross-connect the transmit channel at each end to the receive channel at the opposite end.

For more information regarding to the product safety and maintenance guide, please refer to **Appendix A: Product Safety**.

Chapter 2:

Preparing for Management

In Preparing for Management:
This section will guide your how to manage this product via serial console, management web page, and Telnet/SSH interface.

The switch provides both *out-of-band* and *in-band* managements.

Out-of-band Management: You can configure the switch via RS232 console cable without having the switch or your PC connecting to a network. Out-of-band management provides a dedicated and secure way for switch management.

In-Band Management: In-band management allows you to manage your switch with a web browser (such as Microsoft IE, Mozilla Firefox, or Google Chrome) as long as your PC and the switch are connected to the same network.

- **Preparation for Serial Console**
- **Preparation for Web Interface**
- **Preparation for Telnet/SSH Interface**

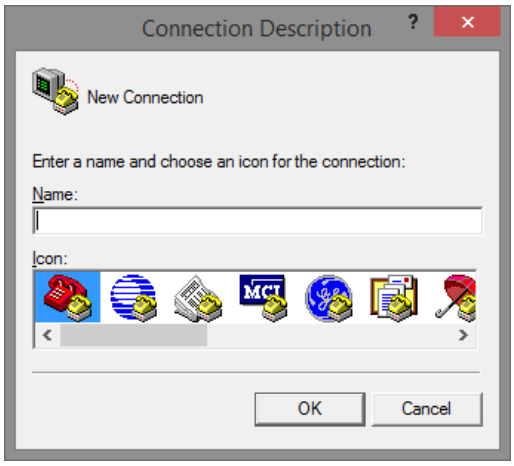
2.1. Preparation for Serial Console

Inside the product package, you can find an RS-232 console cable. Before managing your switch via out-of-band management, please attach this cable's RJ45 connector to your switch's console port and its RS-232 female connector to your PC's COM port.

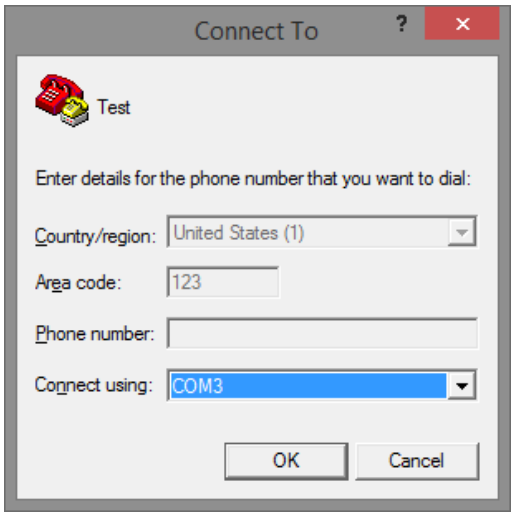
To access this switch's out-of-band management CLI (Command Line Interface), your PC must have terminal emulator software such as HyperTerminal or PuTTY installed. Some operating systems (such as Microsoft Windows XP) have HyperTerminal already installed. If your PC does not have any terminal emulator software installed, please download and install a terminal emulator software on your PC.

The following section will use HyperTerminal as an example.

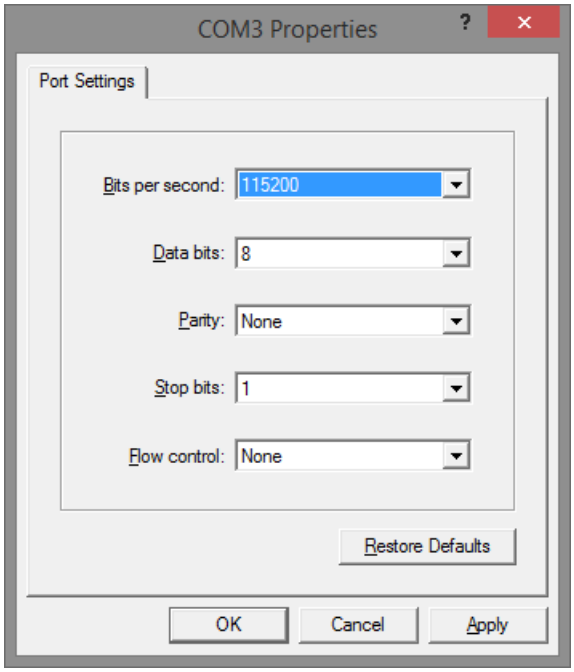
1. Run HyperTerminal on your PC.
2. Give a name to the new console connection.



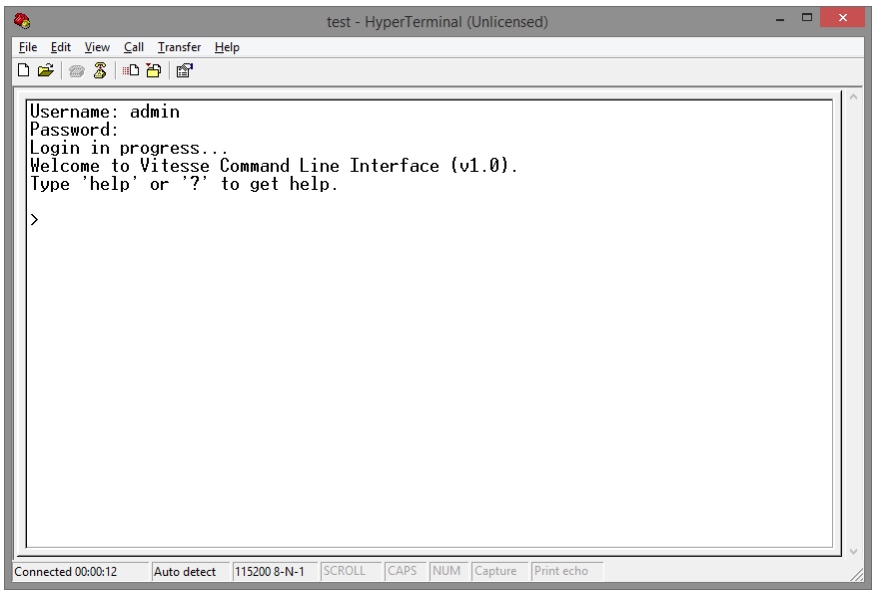
3. Choose the COM port that is connected to the switch.



4. Set the serial port settings as: **Baud Rate:** 115200, **Data Bit:** 8, **Parity:** None, **Stop Bit:** 1, **Row Control:** None.



5. The system will prompt you to login the out-of-band management CLI. The default username/password is **admin/admin**.

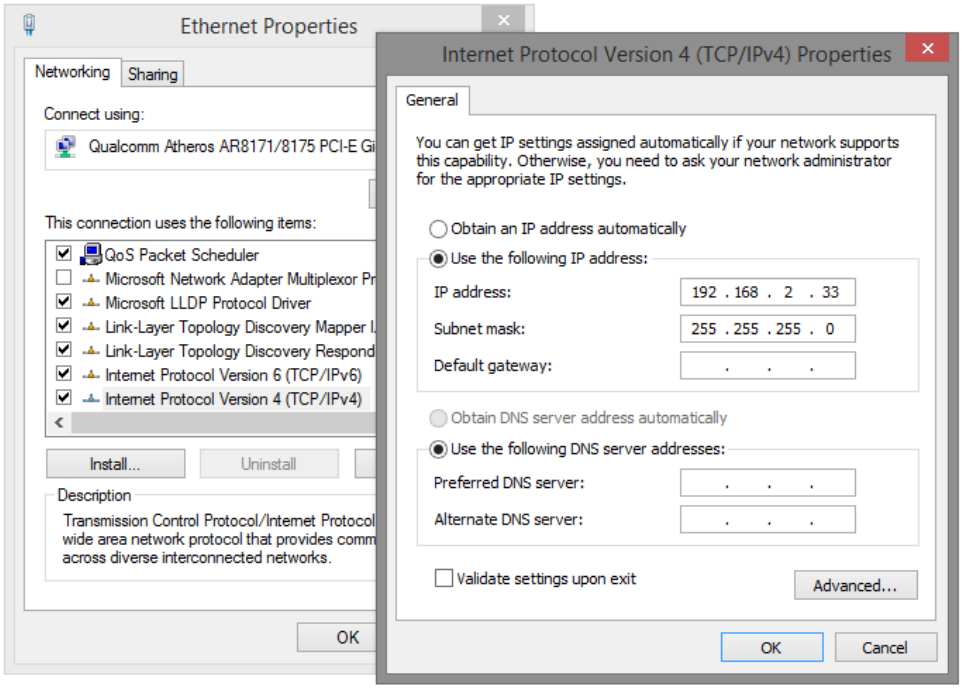


2.2. Preparation for Web Interface

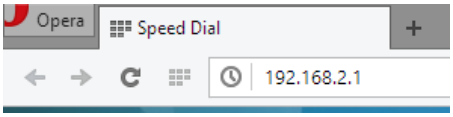
The management web page allows you to use a web browser (such as Microsoft IE, Google Chrome, or Mozilla Firefox) to configure and monitor the switch from anywhere on the network.

Before using the web interface to manage your switch, please verify that your switch and your PC are on the same network. Please follow the steps down below to configure your PC properly:

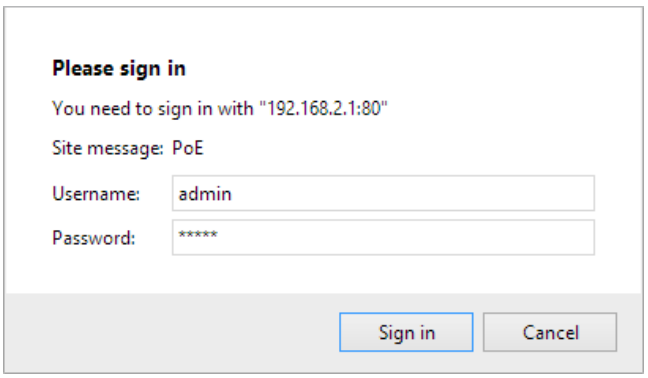
1. Verify that the network interface card (NIC) of your PC is operational and properly installed, and that your operating system supports TCP/IP protocol.
2. Connect your PC with the switch via an RJ45 cable.
3. The default IP address of the switch is **192.168.2.1**. The switch and your PC should locate within the same IP Subnet. Change your PC's IP address to 192.168.2.X, where X can be any number from 2 to 254. Please make sure that the IP address you've assigned to your PC cannot be the same with the switch.



4. Launch the web browser (IE, Firefox, or Chrome) on your PC.
5. Type **192.168.2.1** (or the IP address of the switch) in the web browser's URL field, and press Enter.



6. The web browser will prompt you to sign in. The default username/password for the configuration web page is **admin**/**admin**.



For more information, please refer to **Appendix B: IP Configuration for Your PC**.

2.3. Preparation for Telnet/SSH Interface

Both telnet and SSH (Secure Shell)are network protocols that provide a text-based command line interface (CLI) for in-band system management. However, only SSH provides a secure channel over an un-secured network, where all transmitted data are encrypted.

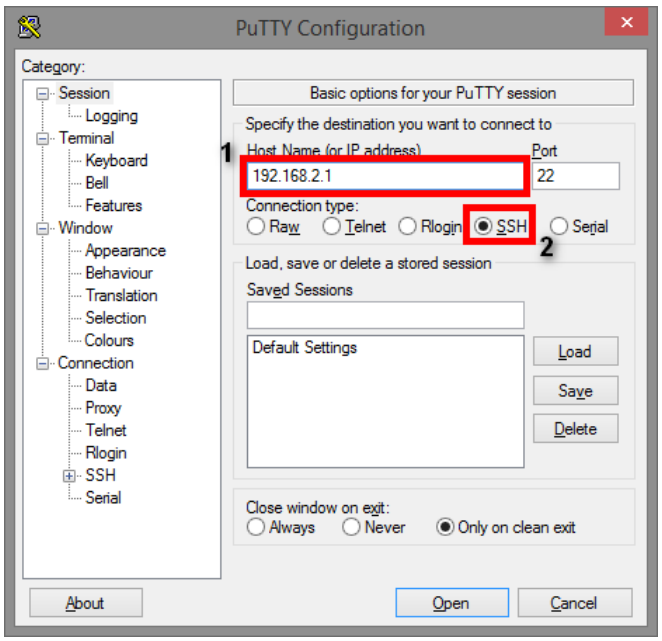
This switch support both telnet and SSH management CLI. In order to access the switch's CLI via telnet or SSH, both your PC and the switch must be in the same network. Before using the switch's telnet/SSH management CLI, please set your PC's network environment according to the previous chapter (**2.2. Preparation for Web Interface**).

Telnet interface can be accessed vi a Microsoft "CMD" command . However, SSH interface can only be accessed via dedicated SSH terminal simulator. The following section will use *PuTTY* as an example to demonstrate how to connect to the switch's SSH CLI, since both telnet and SSH uses the same way (though using different terminal simulator software) to access in-band management CLI.

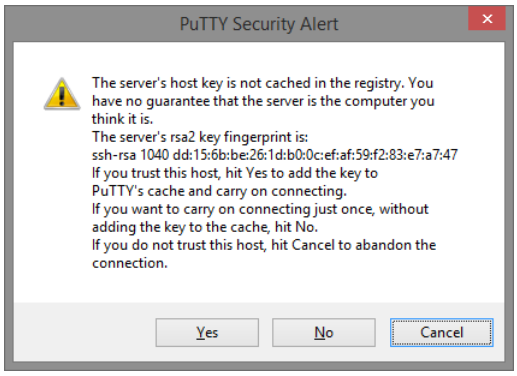
Access SSH via Putty:

A "PuTTY Configuration" window will pop up after you run PuTTY.

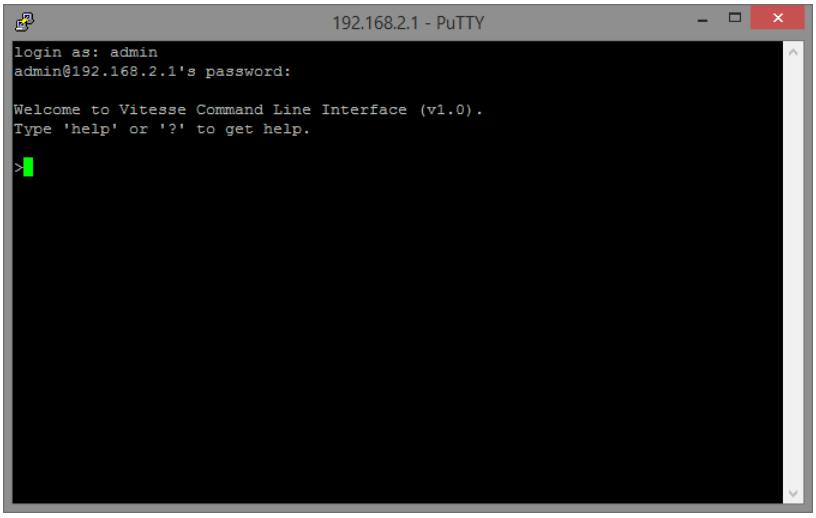
1. Input the IP address of the switch in the "**Host Name (or IP address)**" field. The default IP address of the switch if **192.168.2.1**.
2. Choose "SSH" on the "**Connection type**" section, then press "Enter".



3. If you're connecting to the switch via SSH for the first time, a "**PuTTY Security Alert**" window will pop up. Please press "**Yes**" to continue. This window won't pop up if you're using telnet to connect to the in-band management CLI.



4. PuTTY will prompt you to login after the telnet/SSH connection is established. The default username/password is **admin/admin**.



Chapter 3:

Web Management

In Web Management:

As mentioned in *Chapter 2.2. Preparation for Web Interface*, This switch provides a web-based management interface. You can make all settings and monitor system status with this management web page.

Configuration/Monitor options included in the management web page can be divided into the following 4 categories, which will be discussed in detail in this chapter:

- **Web Management - Configure**
- **Web Management - Monitor**
- **Web Management - Diagnostic**
- **Web Management - Maintenance**

3.1. Web Management - Configure

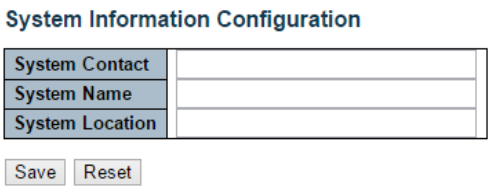
In here you can access all the configuration options of the switch. The configuration options here include:

- **System:** Here you can configure basic system settings such as system information, switch IP, NTP, system time and log.
- **Green Ethernet:** You can configure EEE (Energy Efficient Ethernet) function here on each port to conserve and save power used by the switch.
- **Ports:** You can view the connection status of all the ports on the switch, as well as set port connection speed, flow control, maximum frame length, and power control mode.
- **DHCP:** Here you can set DHCP server, DHCP snooping and DHCP relay.
- **Security:** The Security option allows you to make settings that secures both the switch itself or your network.
- **Aggregation:** Aggregation allows you to combine multiple physical ports into a logical port, thus allows the transmitting speed exceeding the limit of a single port.
- **Loop Protection:** A network loop might cause broadcast storm and paralyze your entire network. You can enable loop protection function here to prevent network loop.
- **Spanning Tree:** Spanning Tree Protocol is a network designed to ensure a loop-free network and provide redundant links that serve as automatic backup paths if an active link fails. This switch supports STP, RSTP (Rapid STP), and MSTP (Multiple STP).
- **IPMC Profile:** IPMC Profile is an acronym for IP Multicast Profile. The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.
- **MVR:** MVR stands for Multiple VLAN Registration, a protocol that allows sharing multicast VLAN information and configuring it dynamically when needed.
- **IPMC:** Here you can set IGMP snooping (for IPv4) or MLD snooping (for IPv6). These protocols can reduce the network loading while running band-width demanding applications such as streaming videos by eliminating excessive data transmitting.
- **LLDP:** LLDP stands for Link Layer Discovery Protocol, a protocol that allows the switch to advertise its identity, capabilities, and neighbors on the network.
- **PoE:** Here you can enable/disable the PoE function on each port or assign the power (in Watt) for each port.
- **MAC Table:** When a network device is connected to the switch, the switch will keep its MAC address on the MAC table. This section provides settings for the switch's MAC address table.

- **VLANs:** VLAN stands for Virtual LAN, which allows you to separate ports into different VLAN groups. Only member of the same VLAN group can transmit/receive packets among each other, while other ports in different VLAN group can't. Here you can set port-based VLAN.
- **Private VLANs:** Also known as port isolation. Only the same member in the private VLAN can communicate with each other.
- **VCL:** Here you can set MAC-based VLAN, Protocol-based VLAN, and IP Subnet-based VLAN.
- **Voice VLAN:** Voice VLAN is a specific VLAN for voice communication (such as VoIP phones) that can ensure the transmission priority of voice traffic and voice quality.
- **QoS:** QoS stands for Quality of Service, which allows you to control the network priority (which packet gets top priority to transmit and which gets low priority) via IEEE 802.1p or DSCP.
- **Mirroring:** For purposes such as network diagnostics, you can direct packets transmitted/received to/from a port (or multiple ports) to a designated port.
- **UPnP:** UPnP stands for Universal Plug and Play, a protocol that allows all the devices on the same network can discover each other and establishing network services such as data sharing. You can set UPnP here in this management page.
- **GVRP:** GVRP stands for GARP VLAN Registration Protocol, a protocol that allows switches exchanging VLAN information automatically.
- **sFlow:** sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets will be sent to the designated sFlow receiver (host) for system administrator for analysis.

3.1.1. Configuration - System

3.1.1.1. System - Information



The switch system information is provided here.

System Contact

The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

System Name

You can input an assigned name for this switch. By convention, this is the switch's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z & a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.

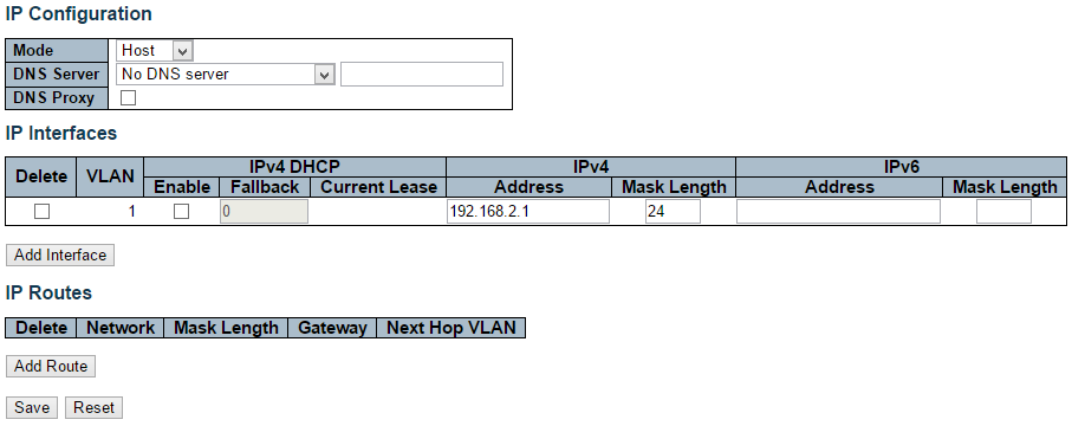
System Location

The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.1.2. System - IP



Configure IP basic settings, control IP interfaces and IP routes.

The maximum number of interfaces supported is 128 and the maximum number of routes is 32.

Basic Settings

Mode

Configure 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.

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, 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 Interfaces

Delete
Select this option to delete an existing IP interface.

VLAN
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 an new interface.

IPv4 DHCP Enabled
Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

IPv4 DHCP Fallback Timeout
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 the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.

IPv4 DHCP Current Lease
For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

IPv4 Address
The IPv4 address of the interface in dotted decimal notation.

If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

IPv4 Mask
The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for an IPv4 address.

If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

IPv6 Address
The IPv6 address of the interface. A 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.

System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address.

The field may be left blank if IPv6 operation on the interface is not desired.

IPv6 Mask

The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a IPv6 address.

The field may be left blank if IPv6 operation on the interface is not desired.

IP Routes

Delete

Select this option to delete an existing IP route.

Network

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

Mask Length

The 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

The IP address of the IP gateway. Valid format is dotted decimal notationor a valid IPv6 notation. Gateway and Network must be of the same type.

Next Hop VLAN (Only for IPv6)

The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.

The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.

If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.

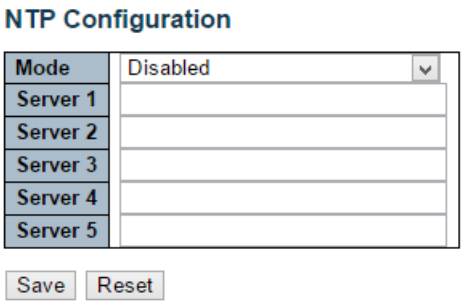
If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

Buttons

- **Add Interface:** Click to add a new IP interface. A maximum of 128 interfaces is supported.
- **Add Route:** Click to add a new IP route. A maximum of 32 routes is supported.

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.1.3. System - NTP



NTP stands for Network Time Protocol, which allows switch to perform clock synchronization with the NTP server.

Mode

You can enable or disable NTP function on this switch:

- **Enabled:** Enable NTP client mode.
- **Disabled:** Disable NTP client mode.

Server 1~5

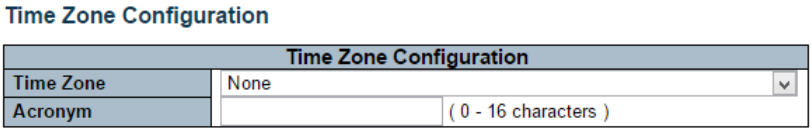
Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Also, you can just input NTP server's URL here as well.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

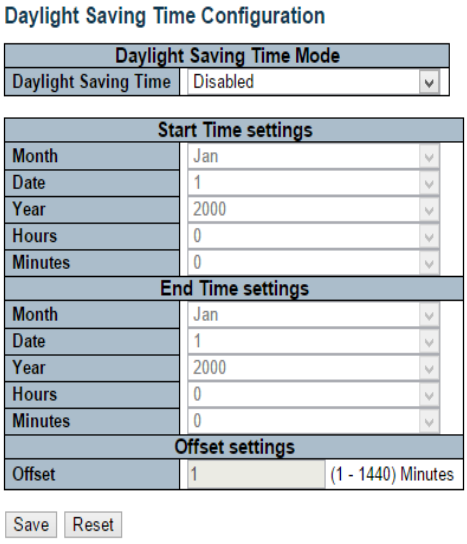
3.1.1.4. System - Time



This page allows you to configure the Time Zone and daylight saving time.

Time Zone Configuration

- **Time Zone:** Lists various Time Zones world wide. Select appropriate Time Zone from the drop down and click Save to set.
- **Acronym:** User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. You can use up to 16 alphanumeric characters and punctuations such as "-", "_", and ".".



Daylight Saving Time Configuration

When enabled, the switch will set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration.

- **Disable:** Disable the Daylight Saving Time configuration. This is the default setting.
- **Recurring:** The configuration of the daylight saving time duration will be applied every year.
- **Non-Recurring**: The configuration of the daylight saving time duration will be applied only once.

Start time settings

- **Week** - Select the starting week number.
- **Day** - Select the starting day.
- **Month** - Select the starting month.
- **Hours** - Select the starting hour.
- **Minutes** - Select the starting minute.

End time settings

- **Week** - Select the ending week number.
- **Day** - Select the ending day.
- **Month** - Select the ending month.
- **Hours** - Select the ending hour.
- **Minutes** - Select the ending minute.

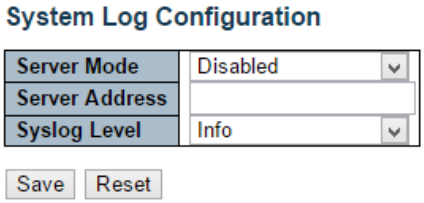
Offset settings

- **Offset** - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.1.5. System - Log



Configure System Log on this page.

Server Mode

When enabled, the system log message will be sent out to the system log server you set here. The system log protocol is based on UDP communication and received on UDP port 514 and the system log server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The system log packet will always send out even if the system log server does not exist. Possible modes are:

- **Enabled:** Enable server mode operation.
- **Disabled:** Disable server mode operation.

Server Address

Indicates the IPv4 host address of system log server. If the switch provide DNS feature, it also can be a host name.

System log Level

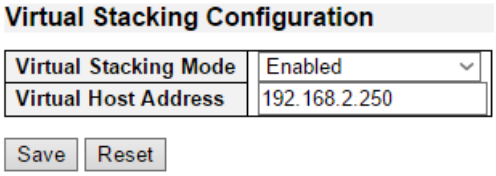
Indicates what kind of message will send to system log server. Possible modes are:

- **Info:** Send information, warnings and errors.
- **Warning:** Send warnings and errors.
- **Error:** Send errors.

Buttons

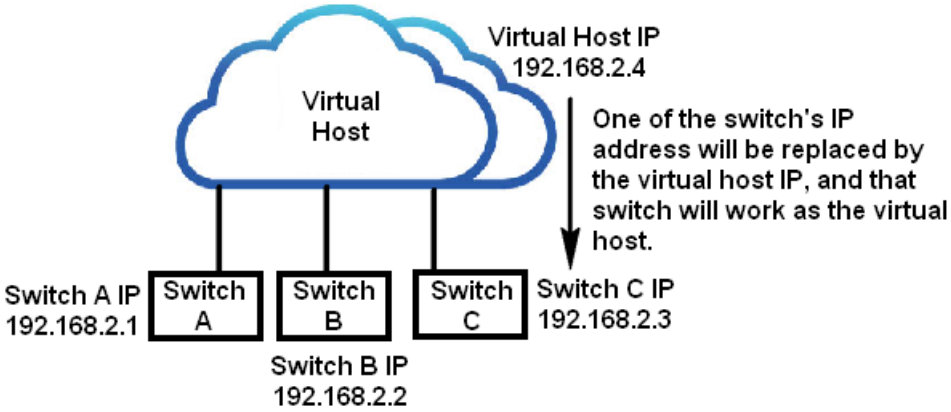
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.1.6. System - Virtual Stacking



Here you can enable the virtual stacking function.

Virtual stacking allows you to set a "virtual host", allowing all the switches with the same virtual host to be access via the virtual host's configuration web page, as shown in the figure down below:



The figure above is an example of the virtual stacking structure. One of the switch's IP address will be replaced by the virtual host IP, and that switch will work as the virtual host.

Virtual Stacking Mode

You can enable or disable the virtual stacking function here with the scroll-down menu:

- **Enable:** Enable the virtual stacking function.
- **Disable:** Disable the virtual stacking function.

Virtual Host Address

Enter the IP address of the virtual host here. When entering the virtual host IP address, please note that:

1. The IP address of the virtual host must be unique in the network, meaning that no other network devices shall have the same IP address.
2. In virtual stacking mode, switches communicate with each other via broadcast, allowing all the switches located in the same physical network (even in different network segment) to be included under the same virtual host.
3. To centralize system management, it is highly recommended to have only 1 virtual host in a network.
4. As mentioned above, one of the switch's IP address will be replaced by the virtual host IP

you've inputted here. That switch will work as the virtual host.

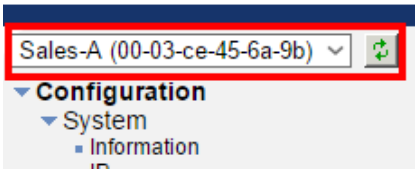
5. When a virtual host is removed from the virtual stacking, a new virtual host will be re-elected as the new virtual host and assume the virtual host's IP address. Please note that adding a new switch to the virtual stack with an existing virtual host won't change the existing virtual host. You can only change the virtual host via its configuration page's scroll-down menu as mentioned down below.
6. After enabling and setting virtual stacking function, it is necessary to go to go to Maintenance -> Configuration -> Save startup-config and save all the settings you've made in order to have the virtual stacking function working properly.

Buttons

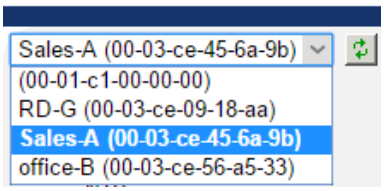
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

After the virtual stacking function is enabled and set the virtual host IP address properly, you can access the virtual host's configuration web page via its IP address.

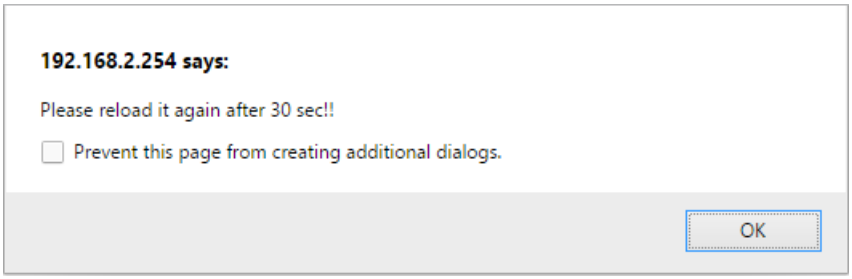
The configuration web page of the virtual host and the ordinary switch configuration web page are quite the same, with the exception of the switch selecting scroll-down menu located on the upper-left part of the configuration web page.



You can choose which switch's configuration web page by this scroll-down menu:



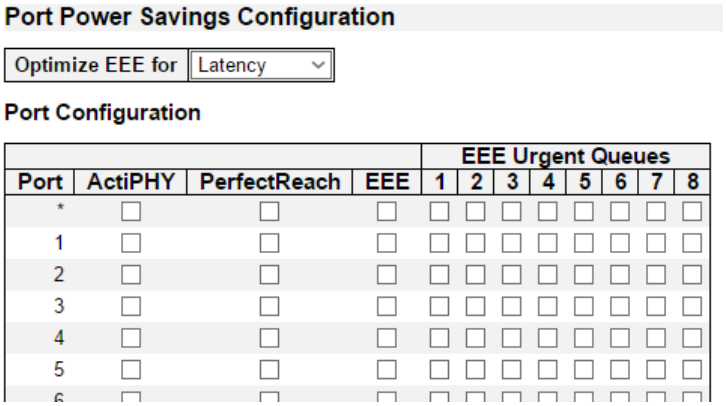
The switch list goes by the format of "<Switch Device Name> (Switch MAC Address)" for identification. After you've selected the switch that you would like to manage, press the "" button to apply.



A window will pop up, reminding you to reload the web browser after 30 seconds. Please press the "OK" button, and reload the web browser after 30 seconds. The virtual host will be changed to the switch that you've chose in the scroll-down menu, and the previous virtual host will resume its previous IP address.

3.1.2. Configuration - Green Ethernet

3.1.2.1. Green Ethernet - Port Power Savings



EEE is a power saving option that reduces the power usage when there is low or no traffic utilization.

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode.

For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.

Port Power Savings Configuration

Optimize EEE for

Here you can set the EEE optimization option:

- **Latency:** When choosing this option, the switch will focus more on reducing network latency.
- **Power:** When choosing this option, the switch will focus more on saving power.

Port Configuration

Port

The switch port number of the logical port.

ActiPHY

Link down power savings enabled.

ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted.

PerfectReach

Cable length power savings enabled.

PerfectReach works by determining the cable length and lowering the power for ports with short cables.

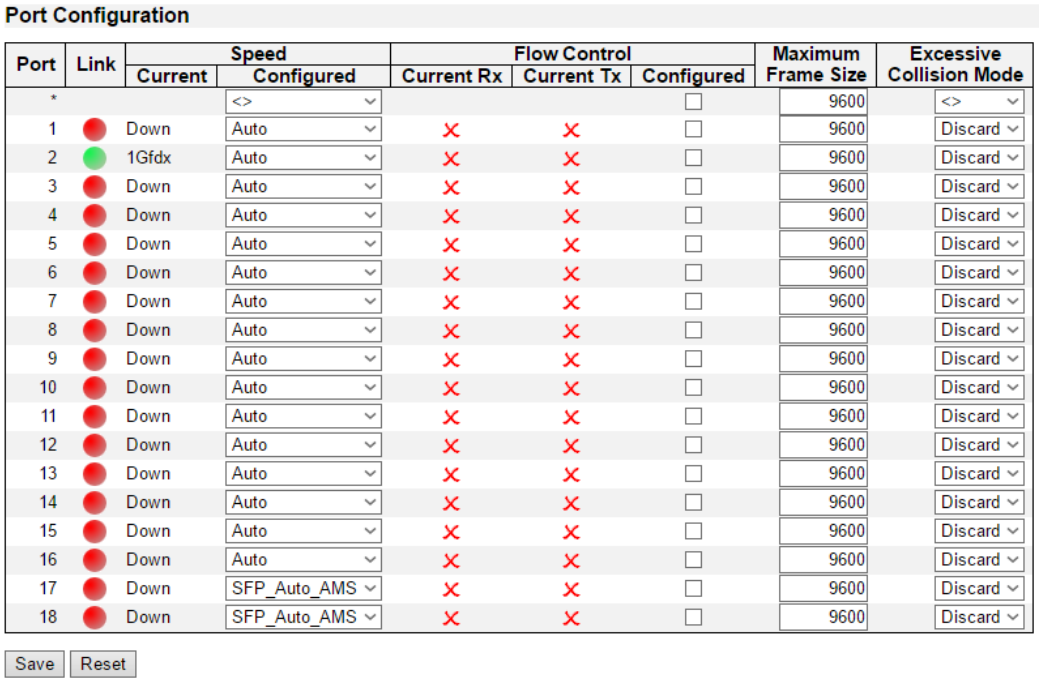
EEE

Enable or disable the EEE functions by check or un-check the check box.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.3. Configuration - Ports



Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>			☐	9600	<>
1		Down	Auto	✕	✕	☐	9600	Discard
2		1Gfdx	Auto	✕	✕	☐	9600	Discard
3		Down	Auto	✕	✕	☐	9600	Discard
4		Down	Auto	✕	✕	☐	9600	Discard
5		Down	Auto	✕	✕	☐	9600	Discard
6		Down	Auto	✕	✕	☐	9600	Discard
7		Down	Auto	✕	✕	☐	9600	Discard
8		Down	Auto	✕	✕	☐	9600	Discard
9		Down	Auto	✕	✕	☐	9600	Discard
10		Down	Auto	✕	✕	☐	9600	Discard
11		Down	Auto	✕	✕	☐	9600	Discard
12		Down	Auto	✕	✕	☐	9600	Discard
13		Down	Auto	✕	✕	☐	9600	Discard
14		Down	Auto	✕	✕	☐	9600	Discard
15		Down	Auto	✕	✕	☐	9600	Discard
16		Down	Auto	✕	✕	☐	9600	Discard
17		Down	SFP_Auto_AMS	✕	✕	☐	9600	Discard
18		Down	SFP_Auto_AMS	✕	✕	☐	9600	Discard

Save Reset

This page displays current port configurations. Ports can also be configured here.

The port settings relate to the currently selected stack unit, as reflected by the page header.

Port

This is the logical port number for this row.

Link

The current link state is displayed graphically. Green indicates the link is up and red that it is down.

Current Link Speed

The current link speed of the port.

Configured Link Speed

Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:

- **Disabled** - Disables the switch port operation.
- **Auto** - Cu port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.
- **10Mbps HDX** - Forces the cu port in 10Mbps half duplex mode.
- **10Mbps FDX** - Forces the cu port in 10Mbps full duplex mode.
- **100Mbps HDX** - Forces the cu port in 100Mbps half duplex mode.
- **100Mbps FDX** - Forces the cu port in 100Mbps full duplex mode.
- **1Gbps FDX** - Forces the cu port in 1Gbps full duplex mode.

Flow Control

When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.

When a fixed-speed setting is selected, that is what is used. 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 related to the setting for Configured Link Speed.

Maximum Frame Size

Enter the maximum frame size allowed for the switch port, including FCS.

Excessive Collision Mode

Configure port transmit collision behavior.

- **Discard:** Discard frame after 16 collisions (default).
- **Restart:** Restart backoff algorithm after 16 collisions.

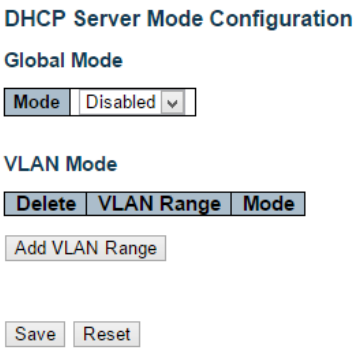
Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Refresh:** Click to refresh the page. Any changes made locally will be undone.

3.1.4. Configuration - DHCP

3.1.4.1. DHCP - Server

3.1.4.1.1. DHCP - Server - Mode



This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.

Global Mode

Configure operation mode to enable/disable DHCP server per system.

Mode

Configure the operation mode per system. Possible modes are:

- **Enabled:** Enable DHCP server per system.
- **Disabled:** Disable DHCP server pre system.

VLAN Mode

Configure operation mode to enable/disable DHCP server per VLAN.

VLAN Range

Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both.

On the other hand, if you want to disable existed VLAN range, then you can follow the steps.

1. Press “Add VLAN Range” to add a new VLAN range.
2. Input the VLAN range that you want to disable.
3. Choose Mode to be Disabled.
4. Press “Save” to apply the change.

Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.

Mode

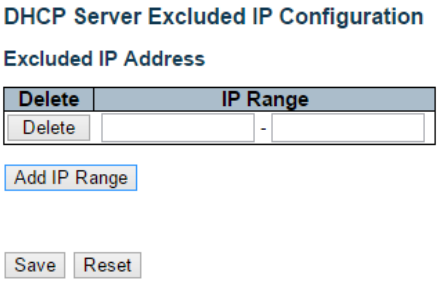
Indicate the operation mode per VLAN. Possible modes are:

- **Enabled:** Enable DHCP server per VLAN.
- **Disabled:** Disable DHCP server pre VLAN.

Buttons

- **Add VLAN Range:** Click to add a new VLAN range.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.4.1.2. DHCP - Server - Excluded IP



This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.

Excluded IP Address

Configure excluded IP addresses.

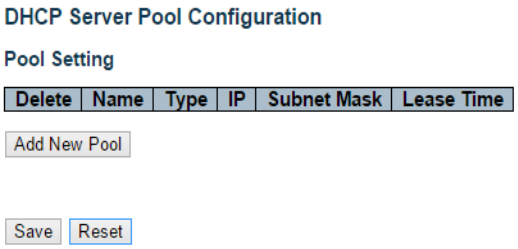
IP Range

Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first and second excluded IP or both.

Buttons

- **Add IP Range:** Click to add a new excluded IP range.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.4.1.3. DHCP - Server - Pool



This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.

Pool Setting

Add or delete pools.

Adding a pool and giving a name is to create a new pool with "default" configuration. If you want to configure all settings including type, IP subnet mask and lease time, you can click the pool name to go into the configuration page.

Name

Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.

Type

Display which type of the pool is.

- **Network:** the pool defines a pool of IP addresses to service more than one DHCP client.
- **Host:** the pool services for a specific DHCP client identified by client identifier or hardware address.

If "-" is displayed, it means not defined.

IP

Display network number of the DHCP address pool.

If "-" is displayed, it means not defined.

Subnet Mask

Display subnet mask of the DHCP address pool.

If "-" is displayed, it means not defined.

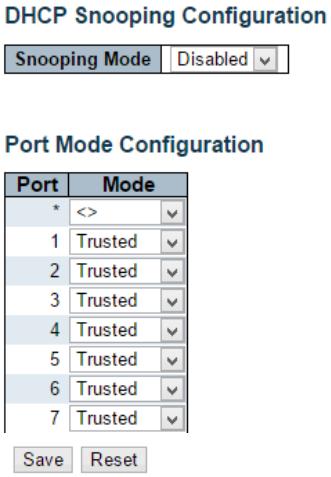
Lease Time

Display lease time of the pool.

Buttons

- **Add New Pool:** Click to add a new DHCP pool.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.4.2. DHCP - Snooping



Configure DHCP Snooping on this page.

Snooping Mode

Indicates the DHCP snooping mode operation. Possible modes are:

- **Enabled:** Enable DHCP snooping mode operation. 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.
- **Disabled:** Disable DHCP snooping mode operation.

Port Mode Configuration

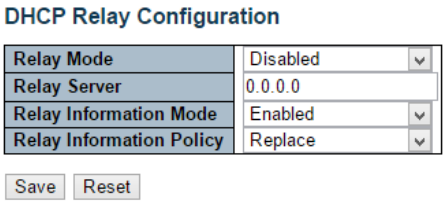
Indicates the DHCP snooping port mode. Possible port modes are:

- **Trusted:** Configures the port as trusted source of the DHCP messages.
- **Untrusted:** Configures the port as untrusted source of the DHCP messages.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.4.3. DHCP - Relay



A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID(Port VLAN ID) correctly.

Relay Mode

Indicates the DHCP relay mode operation.

Possible modes are:

- **Enabled:** Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.
- **Disabled:** Disable DHCP relay mode operation.

Relay Server

Indicates the DHCP relay server IP address.

Relay Information Mode

Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

Possible modes are:

- **Enabled:** Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

- **Disabled:** Disable DHCP relay information mode operation.

Relay Information Policy

Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:

- **Replace:** Replace the original relay information when a DHCP message that already contains it is received.
- **Keep:** Keep the original relay information when a DHCP message that already contains it is received.
- **Drop:** Drop the package when a DHCP message that already contains relay information is received.

Buttons

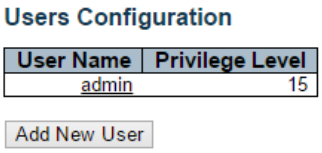
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5. Configuration - Security

This section provides settings regarding to the switch's security functions. Settings provided here can be divided into 3 categories:

- **Switch:** Here you can make security setti ngs regarding to the switch itself.
- **Network:** Providing security settings regarding to the network.
- **AAA:** Here you can set RADIUS and TACACS+ authentication settings.

3.1.5.1. Security - Switch - 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.

User Name

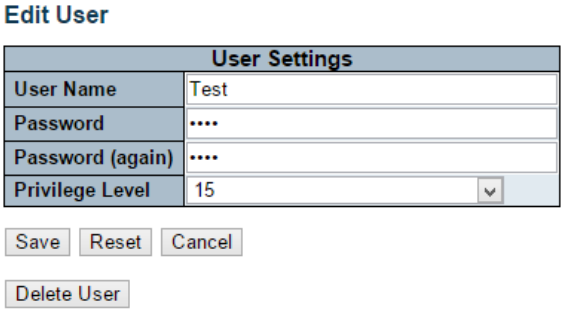
The name of the user. You can also click on the link to configure user account.

Privilege Level

The privilege level of the user. 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 others value 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.

Buttons

- **Add New User:** Click to add a new user.



This page configures a user.

User Name

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31. The valid user name is a combination of letters, numbers and underscores.

Password

The password of the user. The allowed string length is 0 to 31.

Privilege Level

The privilege level of the user. 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 others value 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.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Click to undo any changes made locally and return to the Users.
- **Delete User:** Delete the current user. Please note that the default user (admin) cannot be deleted.

3.1.5.2. Security - Switch - Privilege Level

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
Diagnostics	5	10	5	10
EEE	5	10	5	10
IP	5	10	5	10
IPMC_LIB	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
LLDP_MED	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
MVR	5	10	5	10
Maintenance	15	15	15	15
Mirroring	5	10	5	10
PHY	5	10	5	10
POE	5	10	5	10
Port_Security	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
SNMP	5	10	5	10
Security	5	10	5	10
Spanning_Tree	5	10	5	10
Stack	5	10	1	10
System	5	10	1	10
Timer	5	10	5	10
UPnP	5	10	5	10
VCL	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
sFlow	5	10	5	10

Save Reset

This page provides an overview of the privilege levels.

Group Name

The name identifying 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.

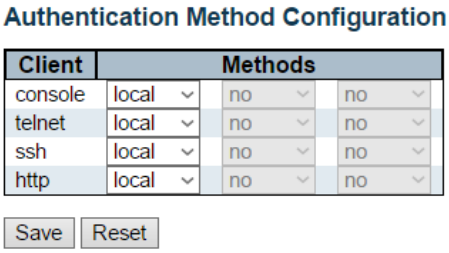
Privilege Levels

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

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.3. Security - Switch - Authentication Method



This page allows you to configure how a user is authenticated when helogs into the stack via one of the management client interfaces.

Client

The management client for which the configuration below applies.

Method

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.

Methods that involve remote servers are timed 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.

Fallback

Enable fallback to local authentication by checking this box.

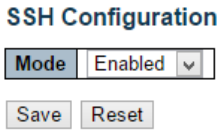
If none of the configured authentication servers are alive, the local user database is used for authentication.

This is only possible if the Authentication Method is set to a value other than 'none' or 'local'.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.4. Security - Switch - SSH



Configure SSH on this page.

Mode

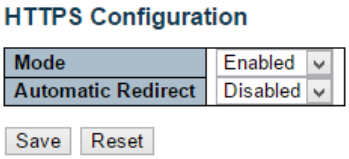
Indicates the SSH mode operation. Possible modes are:

- **Enabled:** Enable SSH mode operation.
- **Disabled:** Disable SSH mode operation.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.5. Security - Switch - HTTPS



Configure HTTPS on this page.

Mode

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

- **Enabled:** Enable HTTPS mode operation.
- **Disabled:** Disable HTTPS mode operation.

Automatic Redirect

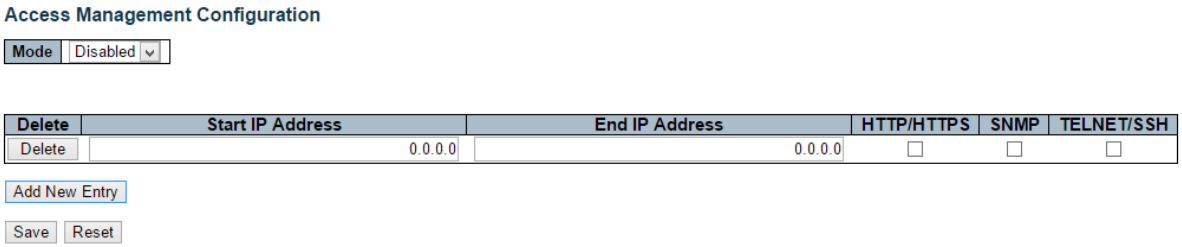
Indicates the HTTPS redirect mode operation. Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled. Possible modes are:

- **Enabled:** Enable HTTPS redirect mode operation.
- **Disabled:** Disable HTTPS redirect mode operation.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.6. Security - Switch - Access Management



Configure access management table on this page. The maximum number of entries is 16. If the application's type match any one of the access management entries, it will allow 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.

Delete

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

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

Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP

Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

TELNET/SSH

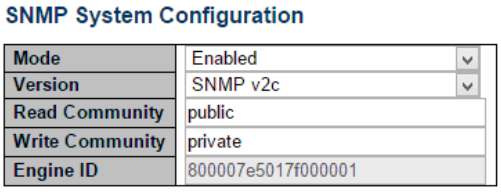
Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons

- **Add New Entry:** Click to add a new access management entry.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.7. Security - Switch - SNMP

3.1.5.7.1. Security - Switch - SNMP - System



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 SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It 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.

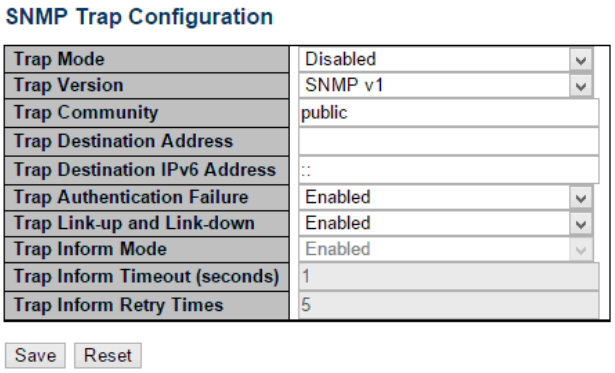
Write Community

Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It 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. Change of the Engine ID will clear all original local users.



SNMP Trap Configuration

Configure SNMP trap on this page.

Trap Mode

Indicates the SNMP trap mode operation. Possible modes are:

- **Enabled:** Enable SNMP trap mode operation.
- **Disabled:** Disable SNMP trap mode operation.

Trap Version

Indicates the SNMP trap supported version. Possible versions are:

- **SNMP v1:** Set SNMP trap supported version 1.
- **SNMP v2c:** Set SNMP trap supported version 2c.
- **SNMP v3:** Set SNMP trap supported version 3.

Trap Community

Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.

Trap Destination Address

Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').

And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

Trap Destination IPv6 Address

Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Trap Authentication Failure

Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are:

- **Enabled:** Enable SNMP trap authentication failure.
- **Disabled:** Disable SNMP trap authentication failure.

Trap Link-up and Link-down

Indicates the SNMP trap link-up and link-down mode operation. Possible modes are:

- **Enabled:** Enable SNMP trap link-up and link-down mode operation.
- **Disabled:** Disable SNMP trap link-up and link-down mode operation.

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 using 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.

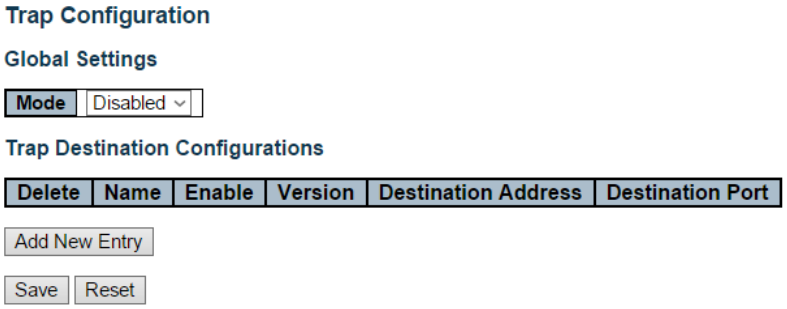
Trap Security Name

Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.7.2. Security - Switch - SNMP - Trap



Configure SNMP trap on this page.

Global Settings

Mode

Indicates the trap mode operation. Possible modes are:

- **Enabled**: Enable SNMP trap mode operation.
- **Disabled**: Disable SNMP trap mode operation.

Trap Destination Configurations

Name

Indicates the trap Configuration's name. Indicates the trap destination's name.

Enable

Indicates the trap destination mode operation. Possible modes are:

- **Enabled**: Enable SNMP trap mode operation.
- **Disabled**: Disable SNMP trap mode operation.

Version

Indicates the SNMP trap supported version. Possible versions are:

- **SNMPv1**: Set SNMP trap supported version 1.
- **SNMPv2c**: Set SNMP trap supported version 2c.
- **SNMPv3**: Set SNMP trap supported version 3.

Destination Address

Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').

And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records

represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

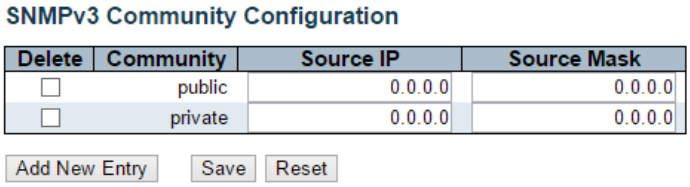
Destination port

Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

Buttons

- **Add New Entry:** Click to add a new user.
- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

3.1.5.7.3. Security - Switch - SNMP - Community



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 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

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.

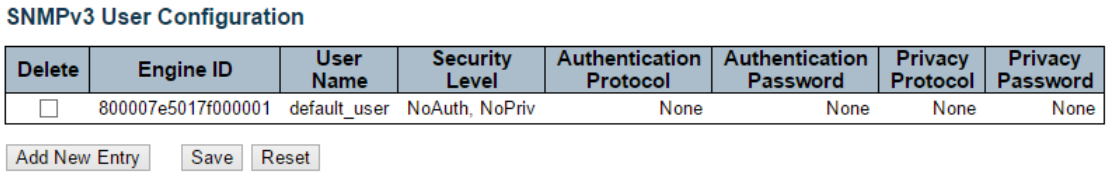
Source Mask

Indicates the SNMP access source address mask.

Buttons

- **Add New Entry:** Click to add a new community entry.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.7.4. Security - Switch - SNMP - User



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

Delete

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

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's remote user.

User Name

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level

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

- **NoAuth, NoPriv:** No authentication and no privacy.
- **Auth, NoPriv:** Authentication and no privacy.
- **Auth, Priv:** Authentication and privacy.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol

Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

- **None:** No authentication protocol.
- **MD5:** An optional flag to indicate that this user uses MD5 authentication protocol.
- **SHA:** An optional flag to indicate that this user uses SHA authentication protocol.

The value of security level cannot be modified if entry already exists. That means must first ensure 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. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

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.

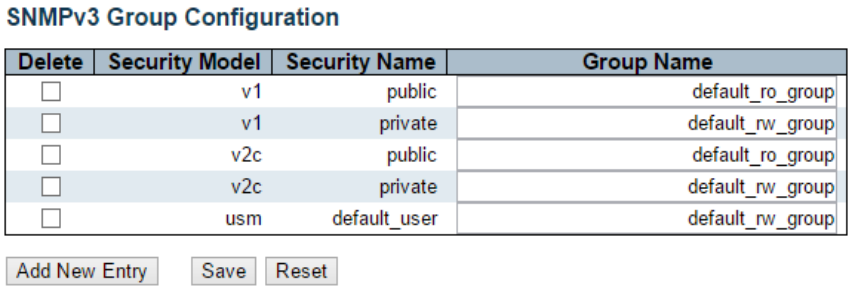
Privacy Password

A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

- **Add New Entry:** Click to add a new community entry.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.7.5. Security - Switch - SNMP - Groups



SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	usm	default_user	default_rw_group

Add New Entry Save Reset

Configure SNMPv3 group table on this page.

Delete

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

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).

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 33 to 126.

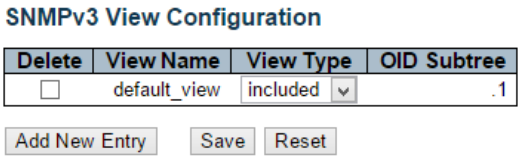
Group Name

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 33 to 126.

Buttons

- **Add New Entry:** Click to add a new community entry.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.7.5. Security - Switch - SNMP - Views



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

Delete

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

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 33 to 126.

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.

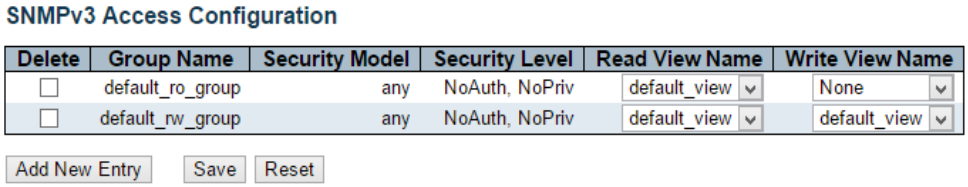
OID Subtree

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 asterisk(*).

Buttons

- **Add New Entry:** Click to add a new community entry.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.7.6. Security - Switch - SNMP - Access



Configure SNMPv3 access table on this page.

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 33 to 126.

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).

Security Level

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

- **NoAuth, NoPriv:** No authentication and no privacy.
- **Auth, NoPriv:** Authentication and no privacy.
- **Auth, Priv:** Authentication and privacy.

Read View Name

The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Write View Name

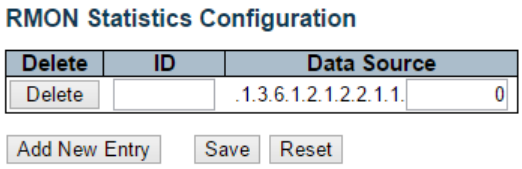
The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

- **Add New Entry:** Click to add a new community entry.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.8. Security - Switch - RMON

3.1.5.8.1. Security - Switch - RMON - Statistics



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. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

Buttons

- **Add New Entry:** Click to add a new community entry.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.8.2. Security - Switch - RMON - History

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1. 0	1800	50	

Add New Entry | Save | Reset

Configure RMON History 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. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005.

Interval

Indicates the interval in seconds for sampling the historystatistics data. The range is from 1 to 3600, default value is 1800 seconds.

Buckets

Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.

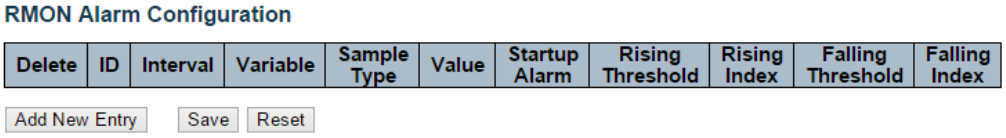
Buckets Granted

The number of data shall be saved in the RMON.

Buttons

- **Add New Entry:** Click to add a new community entry.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.8.3. Security - Switch - RMON - Alarm



Configure RMON Alarm 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.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.

Variable

Indicates the particular variable to be sampled, the possible variables are:

- **InOctets:** The total number of octets received on the interface, including framing characters.
- **InUcastPkts:** The number of uni-cast packets delivered to a higher-layer protocol.
- **InNUcastPkts:** The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.
- **InDiscards:** The number of inbound packets that are discarded even the packets are normal.
- **InErrors:** The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- **InUnknownProtos:** the number of the inbound packets that were discarded because of the unknown or un-support protocol.
- **OutOctets:** The number of octets transmitted out of the interface , including framing characters.
- **OutUcastPkts:** The number of uni-cast packets that request to transmit.
- **OutNUcastPkts:** The number of broad-cast and multi-cast packets that request to transmit.
- **OutDiscards:** The number of outbound packets that are discarded event the packets are normal.
- **OutErrors:** The The number of outbound packets that could not be transmitted because of errors.
- **OutQLen:** The length of the output packet queue (in packets).

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

- **Absolute:** Get the sample directly.
- **Delta:** Calculate the difference between samples (default).

Value

The value of the statistic during the last sampling period.

Startup Alarm

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

- RisingTrigger alarm when the first value is larger than the rising threshold.
- FallingTrigger alarm when the first value is less than the falling threshold.
- RisingOrFallingTrigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

Rising Threshold

Rising threshold value (-2147483648-2147483647).

Rising Index

Rising event index (1-65535).

Falling Threshold

Falling threshold value (-2147483648-2147483647)

Falling Index

Falling event index (1-65535).

Buttons

- **Add New Entry:** Click to add a new community entry.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.8.4. Security - Switch - RMON - Event



Configure RMON Event 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.

Desc

Indicates this event, the string length is from 0 to 127, default is a null string.

Type

Indicates the notification of the event, the possible types are:

- **None:** The total number of octets received on the interface, including framing characters.
- **Log:** The number of uni-cast packets delivered to a higher-layer protocol.
- **snmptrap:** The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.
- **logandtrap:** The number of inbound packets that are discarded even the packets are normal.

Community

Specify the community when trap is sent, the string length is from 0 to 127, default is "public".

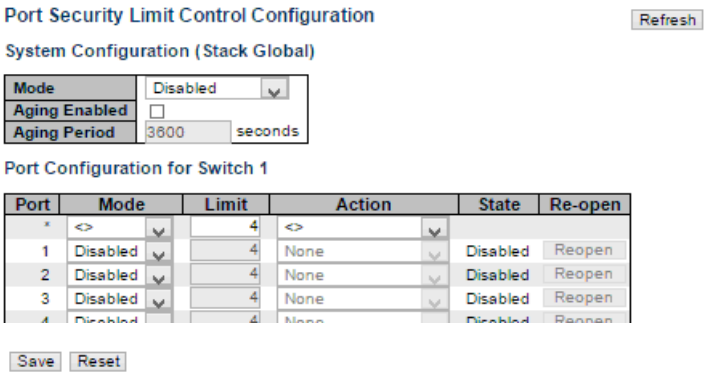
Event Last Time

Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

- **Add New Entry:** Click to add a new community entry.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.9. Security - Network - Limit Control



This page allows you to configure the Port Security Limit Control system and port settings.

Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learnt on the port.

The Limit Control configuration consists of two sections, a system- and a port-wide.

System Configuration

Mode

Indicates if Limit Control is globally enabled or disabled on the stack. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled

If checked, secured MAC addresses are subject to aging as discussed under Aging Period .

Aging Period

If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The Aging Period can be set to a number between 10 and 10,000,000 seconds.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is

not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. 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.

Port Configuration

The table has one row for each port on the selected switch in the stack and a number of columns, which are:

Port

The port number to which the configuration below applies.

Mode

Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

Limit

The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.
The stack is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Action

If Limit is reached, the switch can take one of the following actions:

- **None:** Do not allow more than Limit MAC addresses on the port, but take no further action.
- **Trap:** If Limit + 1 MAC addresses is 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 gets 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 address 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:
    1. Boot the stack or elect a new master,
    2. Disable and re-enable Limit Control on the port or the stack,

3. 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

This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:

- **Disabled:** Limit Control is either globally disabled or disabled on the port.
- **Ready:** The limit is not yet reached. This can be shown for all actions.
- **Limit Reached:** Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.
- **Shutdown:** Indicates that 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.

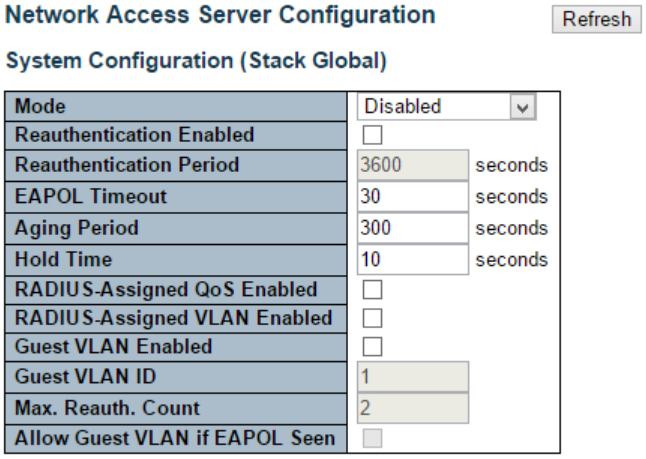
Re-open Button

If a port is shutdown 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.

Buttons

- **Add New Entry:** Click to add a new community entry.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.10. Security - Network - NAS (Network Access Server)



This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration→Security→AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

The NAS configuration consists of two sections, a system- and a port-wide.

System Configuration

Mode

Indicates if NAS is globally enabled or disabled on the stack. If globally disabled, all ports are allowed forwarding of frames.

Re-authentication Enabled

If checked, successfully authenticated supplicants/clients are re-authenticated after the interval specified by the Re-authentication Period. Re-authentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, re-authentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

Re-authentication Period

Determines the period, in seconds, after which a connected client must be re-authenticated. This is only active if the Re-authentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.

EAPOL Timeout

Determines the time for retransmission of Request Identity EAPOL frames.

Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

Aging Period

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

If re-authentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next re-authentication, which will fail. But if re-authentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, re-authentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Hold Time

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the

"Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.

In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.

The Hold Time can be set to a number between 10 and 1000000 seconds.

RADIUS-Assigned QoS Enabled

RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).

The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

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 (see RADIUS-Assigned VLAN Enabled below for a detailed description).

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 determine 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 - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. 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 is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.

Valid values are in the range [1; 4095].

Max. Reauth. Count

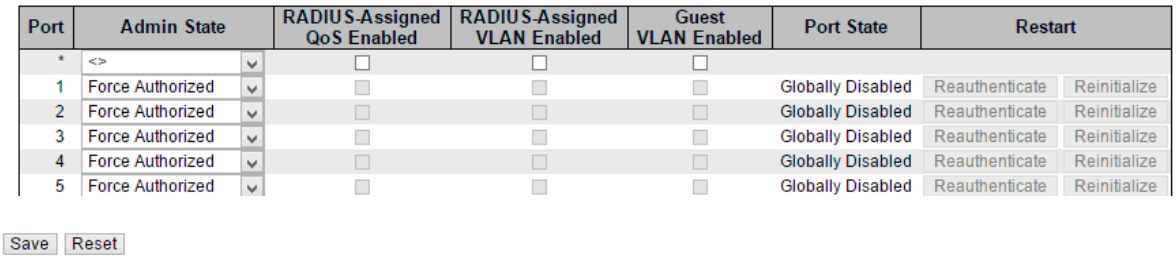
The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting.The value can only be changed if the Guest VLAN option is globally enabled.

Valid values are in the range [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	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

Save Reset

Port Configuration

The table has one row for each port on the selected switch in the stack and a number of columns, which are:

Port

The port number for which the configuration below applies.

Admin State

If NAS is globally enabled, this selection controls the port's authentication mode. 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

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Single 802.1X

In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 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

Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. 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.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC

address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

MAC-based Auth.

Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and 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.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

RADIUS-Assigned QoS Enabled

When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If

(re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class:

The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

RADIUS-Assigned VLAN Enabled

When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID:

RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.
- The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
  - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
  - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
  - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

Guest VLAN Enabled

When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN **configuration**.

Guest VLAN Operation:

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port State

The current state of the port. It can undertake one of the following values:

- **Globally Disabled:** NAS is globally disabled.
- **Link Down:** NAS is globally enabled, but there is no link on the port.
- **Authorized:** The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.
- **Unauthorized:** The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.
- **X Auth/Y Unauth:** The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

Restart

Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect.

- **Re-authenticate:** Schedules a re-authentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, re-authentication 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.

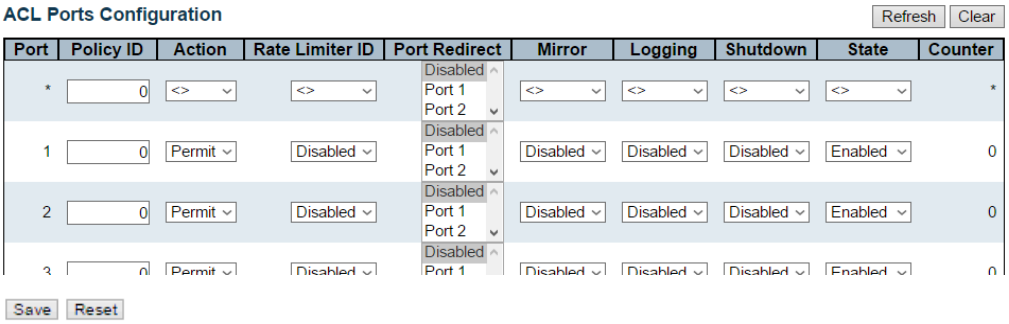
- **Reinitialize:** Forces a reinitialization of the clients on the port and thereby a re-authentication immediately. The clients will transfer to the unauthorized state while the re-authentication is in progress.

Buttons

- **Add New Entry:** Click to add a new community entry.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.11. Security - Network - ACL

3.1.5.11.1. Security - Network - ACL - Ports



Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

The settings relate to the currently selected stack unit, as reflected by the page header.

Port

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

Policy ID

Select the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.

Action

Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID

Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".

Port Redirect

Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value 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".

Logging

Specify the logging operation of this port. The allowed values are:

- **Enabled:** Frames received on the port are stored in the System Log.
- **Disabled:** Frames received on the port are not logged.

The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.

Shutdown

Specify the port shut down operation of this port. The allowed values are:

- **Enabled:** If a frame is received on the port, the port will be disabled.
- **Disabled:** Port shut down is disabled.

The default value is "Disabled".

State

Specify the port state of this port. The allowed values are:

- **Enabled:** To reopen ports by changing the volatile port configuration of the ACL user module.
- **Disabled:** To close ports by changing the volatile port configuration of the ACL user module.

The default value is "Enabled".

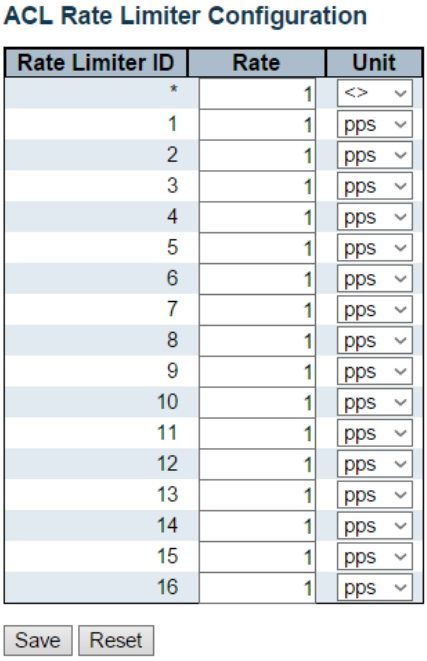
Counter

Counts the number of frames that match this ACE.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Refresh:** Click to refresh the page; any changes made locally will be undone.
- **Clear:** Click to clear the counters.

3.1.5.11.2. Security - Network - ACL - Rate Limiter



Configure the rate limiter for the ACL of the switch.

Rate Limiter ID

The rate limiter ID for the settings contained in the same row.

Rate

The allowed values are: 0-131071 in pps

Unit

Specify the rate unit. The allowed values are:

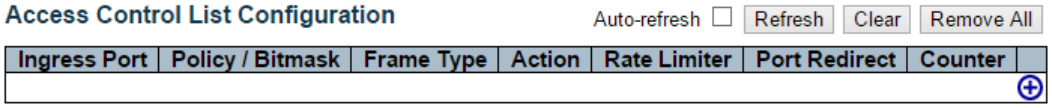
pps: packets per second.

kbps: Kbits per second.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.11.3. Security - Network - ACL - Access Control List



This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 512 on each switch.

Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

Notice: the ACE won't apply to any stacking or none existing port.

Ingress Port

Indicates the ingress port of the ACE. Possible values are:

- **All:** The ACE will match all ingress port.
- **Port:** The ACE will match a specific ingress port.

Policy / Bitmask

Indicates the policy number and bitmask of the ACE.

Frame Type

Indicates 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

Indicates the forwarding action of the ACE.

- **Permit:** Frames matching the ACE may be forwarded and learned.
- **Deny:** Frames matching the ACE are dropped.

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.

Counter

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

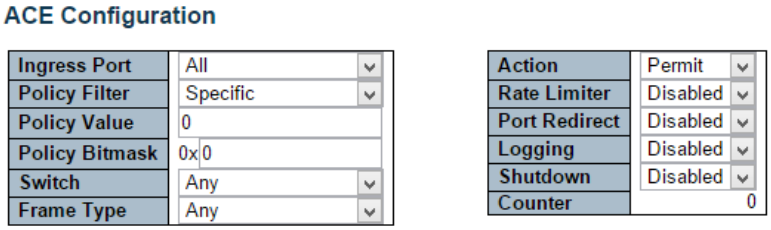
Modification Buttons

You can modify each ACE (Access Control Entry) in the table using the following buttons:

- : Inserts a new ACE before the current row.
- : Edits the ACE row.
- : Moves the ACE up the list.
- : Moves the ACE down the list.
- : Deletes the ACE.
- : The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page; any changes made locally will be undone.
- **Clear:** Click to clear the counters.
- **Remove All:** Click to remove all ACEs.



Configure an ACE (Access Control Entry) on this page.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

A frame that hits this ACE matches the configuration that is defined here.

Ingress Port

Select the ingress port for which this ACE applies.

- **All:** The ACE applies to all port.
- **Port n:** The ACE applies to this port number, where n is the number of the switch port.

Policy Filter

Specify the policy number filter for this ACE.

- **Any:** No policy filter is specified. (policy filter status is "don't-care".)
- **Specific:** If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.

Policy Value

When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255.

Policy Bitmask

When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff.

Switch

Select the switch to which this ACE applies.

- **Any:** The ACE applies to any port.
- **Switch n:** The ACE applies to this switch number, where n is the number of the switch.

Frame Type

Select the frame type for this ACE. These frame types are mutually exclusive.

- **Any:** Any frame can match this ACE.
- **Ethernet Type:** Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).
- **ARP:** Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.
- **IPv4:** Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.
- **IPv6:** Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.

Action

Specify the action to take with a frame that hits this ACE.

- **Permit:** The frame that hits this ACE is granted permission for the ACE operation.
- **Deny:** The frame that hits this ACE is dropped.

Rate Limiter

Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.

Port Redirect

Frames that hit the ACE are redirected to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.

Logging

Specify the logging operation of the ACE. The allowed values are:

- **Enabled:** Frames matching the ACE are stored in the System Log.
- **Disabled:** Frames matching the ACE are not logged.

Please note that the System Log memory size and logging rate is limited.

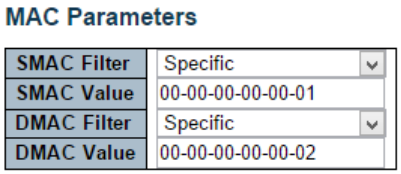
Shutdown

Specify the port shut down operation of the ACE. The allowed values are:

- **Enabled:** If a frame matches the ACE, the ingress port will be disabled.
- **Disabled:** Port shut down is disabled for the ACE.

Counter

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



MAC Parameters

SMAC Filter

(Only displayed when the frame type is Ethernet Type or ARP.)

Specify the source MAC filter for this ACE.

- **Any:** No SMAC filter is specified. (SMAC filter status is "don't-care".)
- **Specific:** If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

SMAC Value

When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.

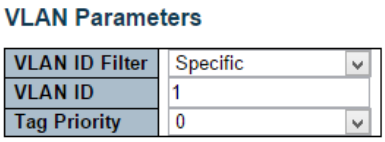
DMAC Filter

Specify the destination MAC filter for this ACE.

- **Any:** No DMAC filter is specified. (DMAC filter status is "don't-care".)
- **MC:** Frame must be multicast.
- **BC:** Frame must be broadcast.
- **UC:** Frame must be unicast.
- **Specific:** If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

DMAC Value

When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.



VLAN Parameters

VLAN ID Filter

Specify the VLAN ID filter for this ACE.

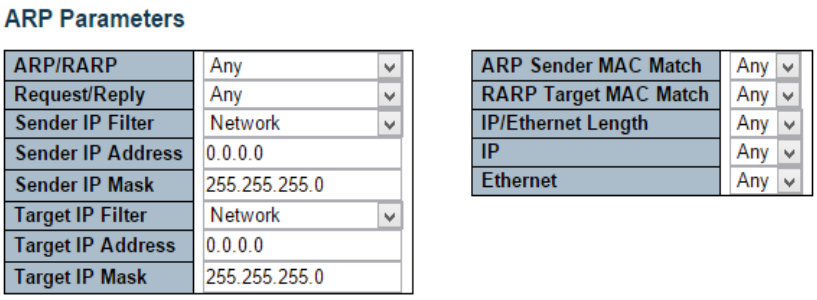
- **Any:** No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)
- **Specific:** If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.

VLAN ID

When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.

Tag Priority

Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)



ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

ARP/RARP

Specify the available ARP/RARP opcode (OP) flag for this ACE.

- **Any:** No ARP/RARP OP flag is specified. (OP is "don't-care".)
- **ARP:** Frame must have ARP opcode set to ARP.
- **RARP:** Frame must have RARP opcode set to RARP.
- **Other:** Frame has unknown ARP/RARP Opcode flag.

Request/Reply

Specify the available Request/Reply opcode (OP) flag for this ACE.

- **Any:** No Request/Reply OP flag is specified. (OP is "don't-care".)
- **Request:** Frame must have ARP Request or RARP Request OP flag set.
- **Reply:** Frame must have ARP Reply or RARP Reply OP flag.

Sender IP Filter

Specify the sender IP filter for this ACE.

- **Any:** No sender IP filter is specified. (Sender IP filter is "don't-care".)
- **Host:** Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.
- **Network:** Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

Sender IP Address

When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.

Sender IP Mask

When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.

Target IP Filter

Specify the target IP filter for this specific ACE.

- **Any:** No target IP filter is specified. (Target IP filter is "don't-care".)
- **Host:** Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

Target IP Address

When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.

Target IP Mask

When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.

ARP Sender MAC Match

Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.

- **0:** ARP frames where SHA is not equal to the SMAC address.
- **1:** ARP frames where SHA is equal to the SMAC address.
- **Any:** Any value is allowed ("don't-care").

RARP Target MAC Match

Specify whether frames can hit the action according to their target hardware address field (THA) settings.

- **0:** RARP frames where THA is not equal to the target MAC address.
- **1:** RARP frames where THA is equal to the target MAC address.
- **Any:** Any value is allowed ("don't-care").

IP/Ethernet Length

Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

- **0:** ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).
- **1:** ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).
- **Any:** Any value is allowed ("don't-care").

IP

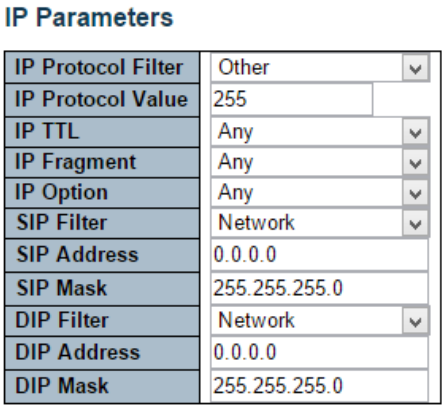
Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

- **0:** ARP/RARP frames where the HLD is not equal to Ethernet (1).
- **1:** ARP/RARP frames where the HLD is equal to Ethernet (1).
- **Any:** Any value is allowed ("don't-care").

Ethernet

Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

- **0:** ARP/RARP frames where the PRO is not equal to IP (0x800).
- **1:** ARP/RARP frames where the PRO is equal to IP (0x800).
- **Any:** Any value is allowed ("don't-care").



IP Parameters

The IP parameters can be configured when Frame Type "IPv4" is selected.

IP Protocol Filter

Specify the IP protocol filter for this ACE.

- **Any:** No IP protocol filter is specified ("don't-care").
- **Specific:** If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.
- **ICMP:** Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.
- **UDP:** Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.
- **TCP:** Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

IP Protocol Value

When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.

IP TTL

Specify the Time-to-Live settings for this ACE.

- **zero:** IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.
- **non-zero:** IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

IP Fragment

Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.
No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero

must not be able to match this entry.

- **Yes:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

IP Option

Specify the options flag setting for this ACE.

- **No:** IPv4 frames where the options flag is set must not be able to match this entry.
- **Yes:** IPv4 frames where the options flag is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

SIP Filter

Specify the source IP filter for this ACE.

- **Any:** No source IP filter is specified. (Source IP filter is "don't-care".)
- **Host:** Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.
- **Network:** Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

SIP Address

When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.

SIP Mask

When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.

DIP Filter

Specify the destination IP filter for this ACE.

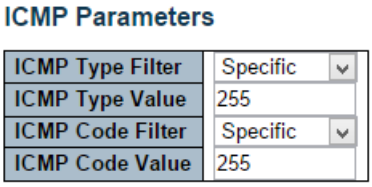
- **Any:** No destination IP filter is specified. (Destination IP filter is "don't-care".)
- **Host:** Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.
- **Network:** Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

DIP Address

When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.

DIP Mask

When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.



ICMP Parameters

ICMP Type Filter

Specify the ICMP filter for this ACE.

- **Any:** No ICMP filter is specified (ICMP filter status is "don't-care").
- **Specific:** If you want to filter a specific ICMP filter with thisACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.

ICMP Type Value

When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.

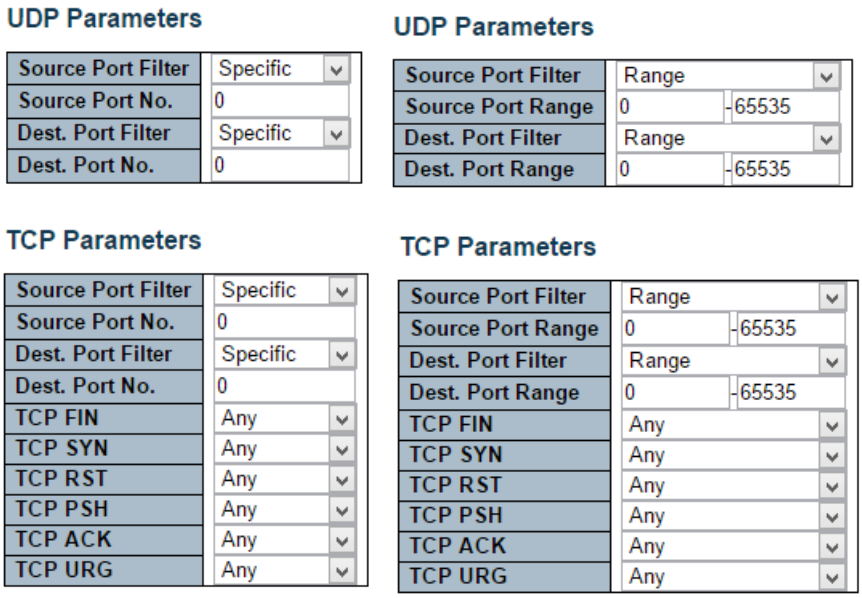
ICMP Code Filter

Specify the ICMP code filter for this ACE.

- **Any:** No ICMP code filter is specified (ICMP code filter status is "don't-care").
- **Specific:** If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

ICMP Code Value

When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.



TCP/UDP Parameters

TCP/UDP Source Filter

Specify the TCP/UDP source filter for this ACE.

- **Any:** No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").
- **Specific:** If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.
- **Range:** If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

TCP/UDP Source No.

When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Source Range

When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Destination Filter

Specify the TCP/UDP destination filter for this ACE.

- **Any:** No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").

- **Specific:** If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.
- **Range:** If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

TCP/UDP Destination Number

When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP/UDP Destination Range

When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP FIN

Specify the TCP "No more data from sender" (FIN) value for this ACE.

- **0:** TCP frames where the FIN field is set must not be able to match this entry.
- **1:** TCP frames where the FIN field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP SYN

Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.

- **0:** TCP frames where the SYN field is set must not be able to match this entry.
- **1:** TCP frames where the SYN field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP RST

Specify the TCP "Reset the connection" (RST) value for this ACE.

- **0:** TCP frames where the RST field is set must not be able to match this entry.
- **1:** TCP frames where the RST field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP PSH

Specify the TCP "Push Function" (PSH) value for this ACE.

- **0:** TCP frames where the PSH field is set must not be able to match this entry.
- **1:** TCP frames where the PSH field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP ACK

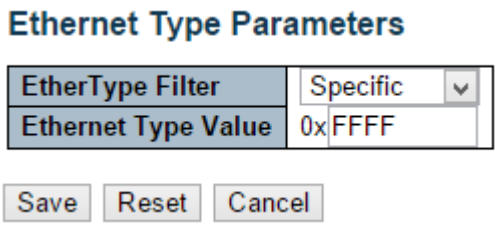
Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.

- **0:** TCP frames where the ACK field is set must not be able to match this entry.
- **1:** TCP frames where the ACK field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP URG

Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.

- **0:** TCP frames where the URG field is set must not be able to match this entry.
- **1:** TCP frames where the URG field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").



Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

EtherType Filter

Specify the Ethernet type filter for this ACE.

- **Any:** No EtherType filter is specified (EtherType filter status is "don't-care").
- **Specific:** If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.

Ethernet Type Value

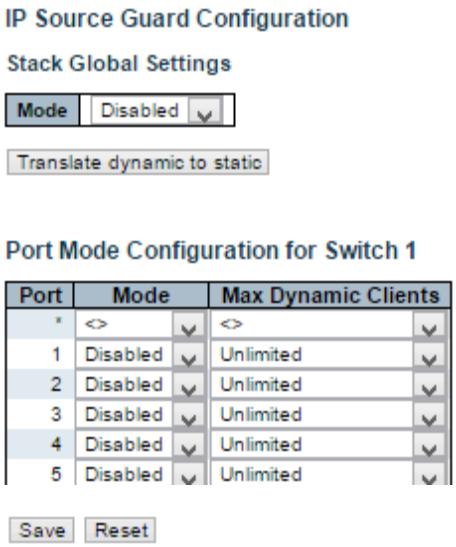
When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Return to the previous page.

3.1.5.12. Security - Network - IP Source Guard

3.1.5.12.1. Security - Network - IP Source Guard - Configuration



This page provides IP Source Guard related configuration.

Mode of IP Source Guard Configuration

Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration

Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

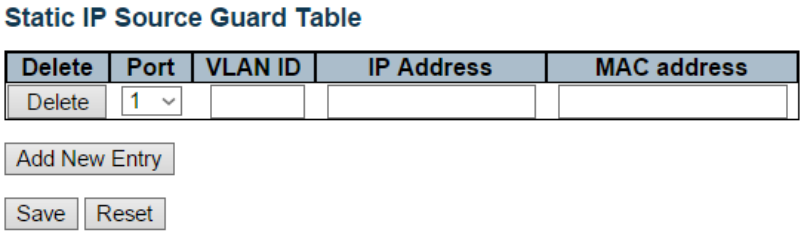
Max Dynamic Clients

Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Translate Dynamic to Static**: Click to translate all dynamic entries to static entries.

3.1.5.12.2. Security - Network - IP Source Guard - Static Table



Delete

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

Port

The logical port for the settings.

VLAN ID

The vlan id for the settings.

IP Address

Allowed Source IP address.

MAC Address

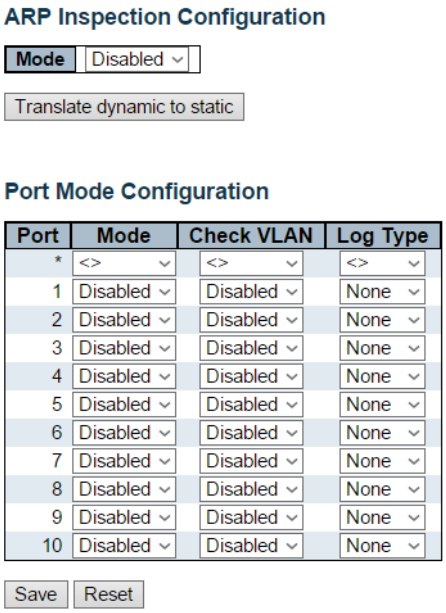
Allowed Source MAC address.

Buttons

- **Add New Entry:** Click to add a new entry to the Static IP Source Guard table.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.13. Security - Network - ARP Inspection

3.1.5.13.1. Security - Network - ARP Inspection - Port Configuration



This page provides ARP Inspection related configuration.

Mode

Enable the Global ARP Inspection or disable the Global ARP Inspection.

Port Mode Configuration

Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:

- **Enabled**: Enable ARP Inspection operation.
- **Disabled**: Disable ARP Inspection operation.

If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:

- **Enabled**: Enable check VLAN operation.
- **Disabled**: Disable check VLAN operation.

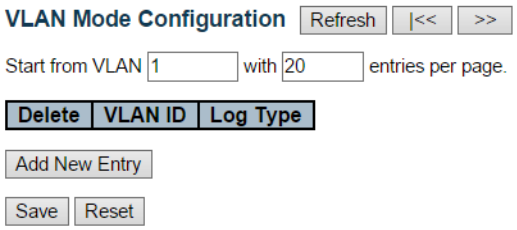
Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are:

- **None**: Log nothing.
- **Deny**: Log denied entries.
- **Permit**: Log permitted entries.
- **ALL**: Log all entries.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Translate Dynamic to Static**: Click to translate all dynamic entries to static entries.

3.1.5.13.2. Security - Network - ARP Inspection - VLAN Configuration



This page provides ARP Inspection related configuration.

Navigating the VLAN Configuration

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the closest next VLAN Table match. The >> button will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the << button to start over.

VLAN Mode Configuration

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.

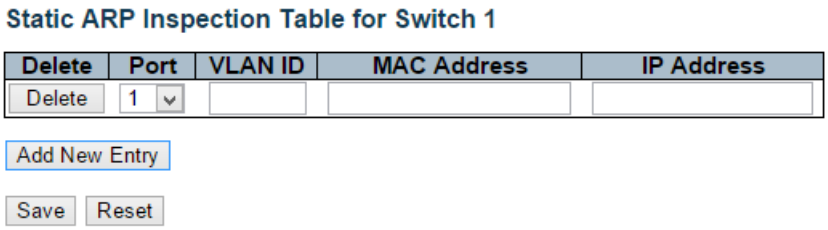
Possible types are:

- **None:** Log nothing.
- **Deny:** Log denied entries.
- **Permit:** Log permitted entries.
- **ALL:** Log all entries.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Add New Entry**: Click to add a new VLAN to the ARP Inspection VLAN table.

3.1.5.13.3. Security - Network - ARP Inspection - Static Table



Delete

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

Port

The logical port for the settings.

VLAN ID

The vlan id for the settings.

MAC Address

Allowed Source MAC address in ARP request packets.

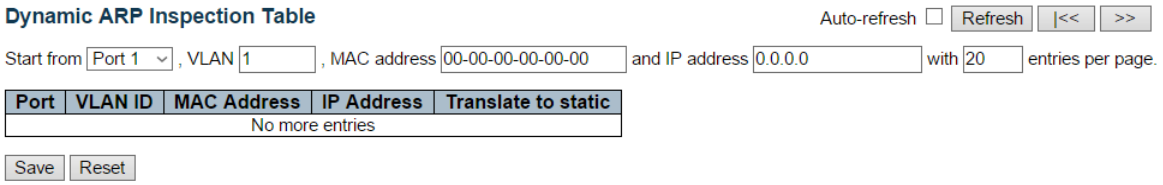
IP Address

Allowed Source IP address in ARP request packets.

Buttons

- **Add New Entry:** Click to add a new entry to the Static IP Source Guard table.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.5.13.4. Security - Network - ARP Inspection - Dynamic Table



Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

ARP Inspection Table Columns

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the ARP traffic is permitted.

MAC Address

User MAC address of the entry.

IP Address

User IP address of the entry.

Translate to static

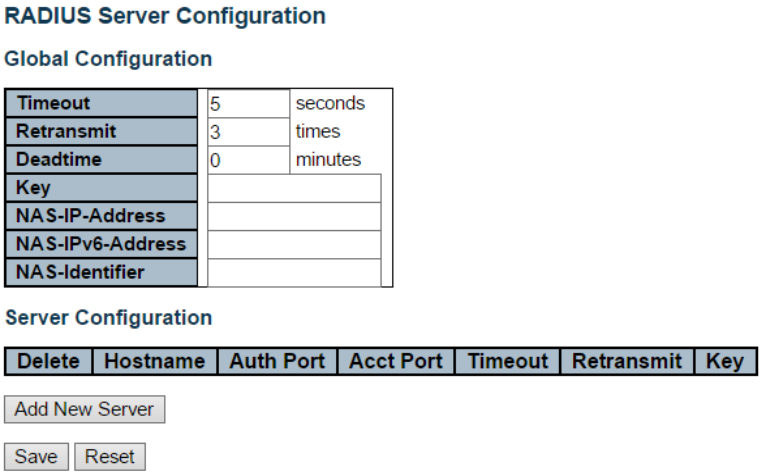
Select the checkbox to translate the entry to static entry.

Buttons

- **Auto-refresh**: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh**: Refreshes the displayed table starting from the input fields.
- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.
- **<<:** Updates the table starting from the first entry in the Dynamic ARP Inspection Table.
- >>: Updates the table, starting with the entry after the last entry currently displayed.

3.1.5.3. Security - AAA

3.1.5.3.1. Security - AAA - RADIUS



This page allows you to configure the RADIUS servers.

Global Configuration

Timeout

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit

Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key

The secret key - up to 63 characters long - shared between the RADIUS server and the switch.

NAS-IP-Address (Attribute 4)

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

NAS-IPv6-Address (Attribute 95)

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

NAS-Identifier (Attribute 32)

The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration

The table has one row for each RADIUS server and a number of columns, which are:

Delete

To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

Hostname

The IP address or hostname of the RADIUS server.

Auth Port

The UDP port to use on the RADIUS server for authentication.

Acct Port

The UDP port to use on the RADIUS server for accounting.

Timeout

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Retransmit

This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

Key

This optional setting overrides the global key. Leaving it blank will use the global key.

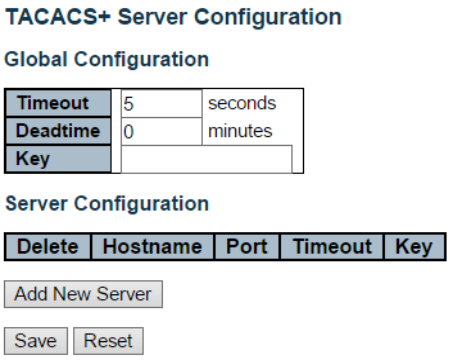
Adding a New Server

Click Add New Server button to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported. The Delete button can be used to undo the addition of the new server.

Buttons

- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

3.1.5.3.2. Security - AAA - TACACS+



This page allows you to configure the TACACS+ servers.

Global Configuration

These setting are common for all of the TACACS+ servers.

Timeout

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key

The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

The table has one row for each TACACS+ server and a number of columns, which are:

Delete

To delete a TACACS+ server entry, check this box. The entry will be deleted during the next **Save.**

Hostname

The IP address or hostname of the TACACS+ server.

Port

The TCP port to use on the TACACS+ server for authentication.

Timeout

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Key

This optional setting overrides the global key. Leaving it blank will use the global key.

Adding a New Server

Click Add New Server button to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.

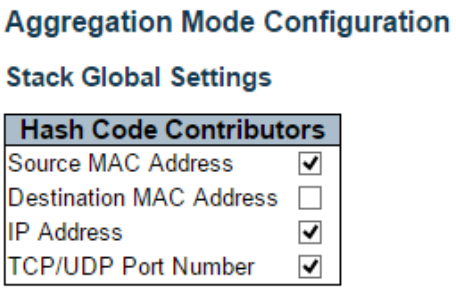
The Delete button can be used to undo the addition of the new server.

Buttons

- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

3.1.6. Configuration - Aggregation

3.1.6.1. Aggregation - Static



This page is used to configure the Aggregation hash mode and the aggregation group.

Hash Code Contributors

Source MAC Address

The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.

Destination MAC Address

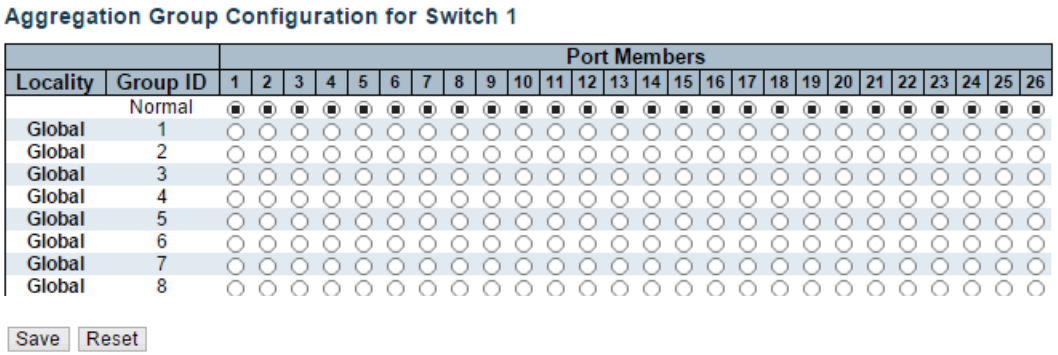
The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.

IP Address

The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.

TCP/UDP Port Number

The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.



Aggregation Group Configuration

Locality

Indicates the aggregation group type. This field is only valid for stackable switches.

- **Global:** The group members may reside on different units in the stack. Each global aggregation may consist of up to 8 members.
- **Local:** The group members reside on the same unit. Each local aggregation may consist of up to 16 members.

Group ID

Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

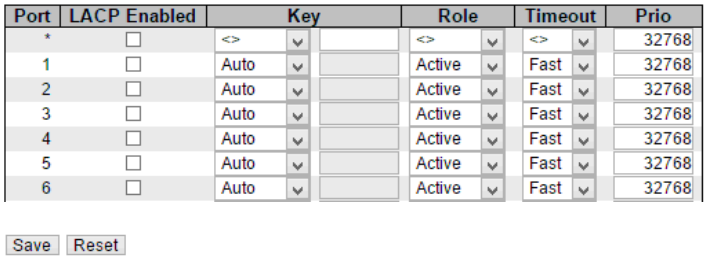
Port Members

Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. 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.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.6.2. Aggregation - LACP



Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☐	Auto		Active	Fast	32768
2	☐	Auto		Active	Fast	32768
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768

Save Reset

This page allows the user to inspect the current LACP port configurations, and possibly change them as well.

The LACP port settings relate to the currently selected stack unit, as reflected by the page header.

Port

The switch port number.

LACP Enabled

Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form max 12 LLAGs per switch and 2 GLAGs per stack.

Key

The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.

Role

The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).

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.

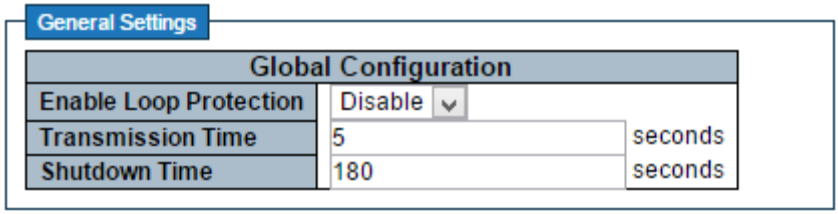
Prio

The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.7. Configuration - Loop Protection



This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well.

General Settings

Enable Loop Protection

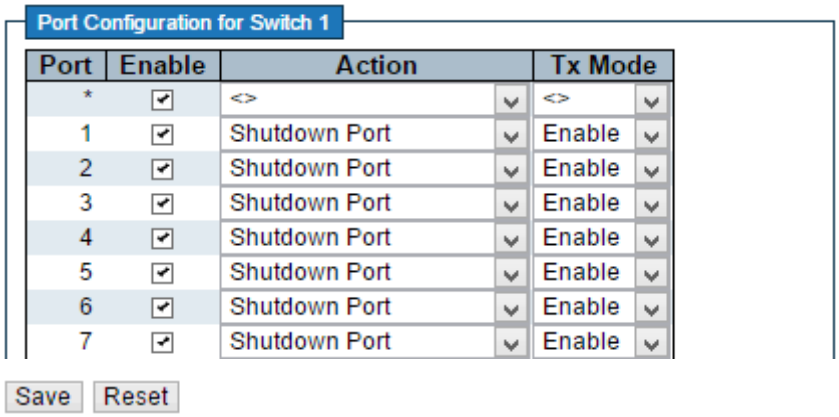
Controls whether loop protections is enabled (as a whole).

Transmission Time

The interval between each loop protection PDU sent on each port. valid values are 1 to 10 seconds.

Shutdown Time

The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).



Port Configuration

Port

The switch port number of the port.

Enable

Controls whether loop protection is enabled on this switch port.

Action

Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.

Tx Mode

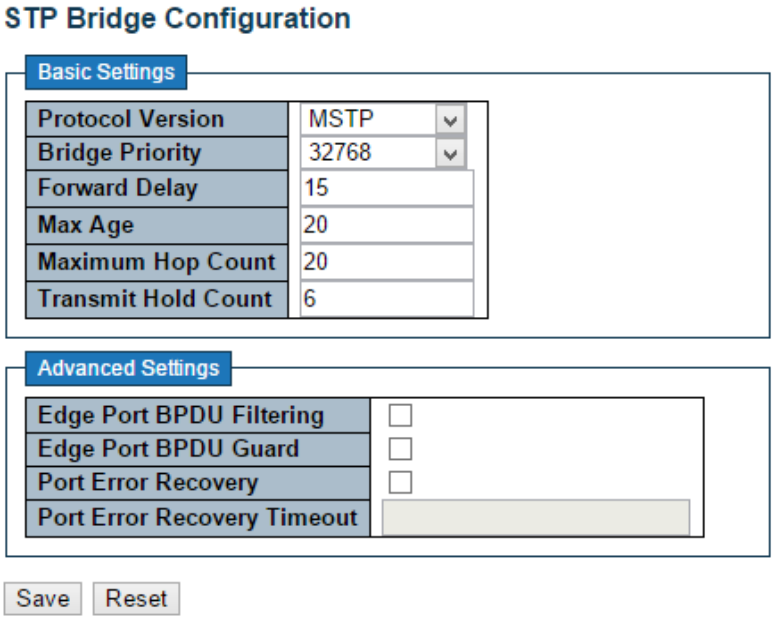
Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.8. Configuration - Spanning Tree

3.1.8.1. Spanning Tree - Bridge Settings



This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch Stack.

Basic Settings

Protocol Version

The MSTP / RSTP / STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a **Bridge Identifier.**

For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Forward Delay

The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age

The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count

This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count

The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering

Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard

Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Port Error Recovery

Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

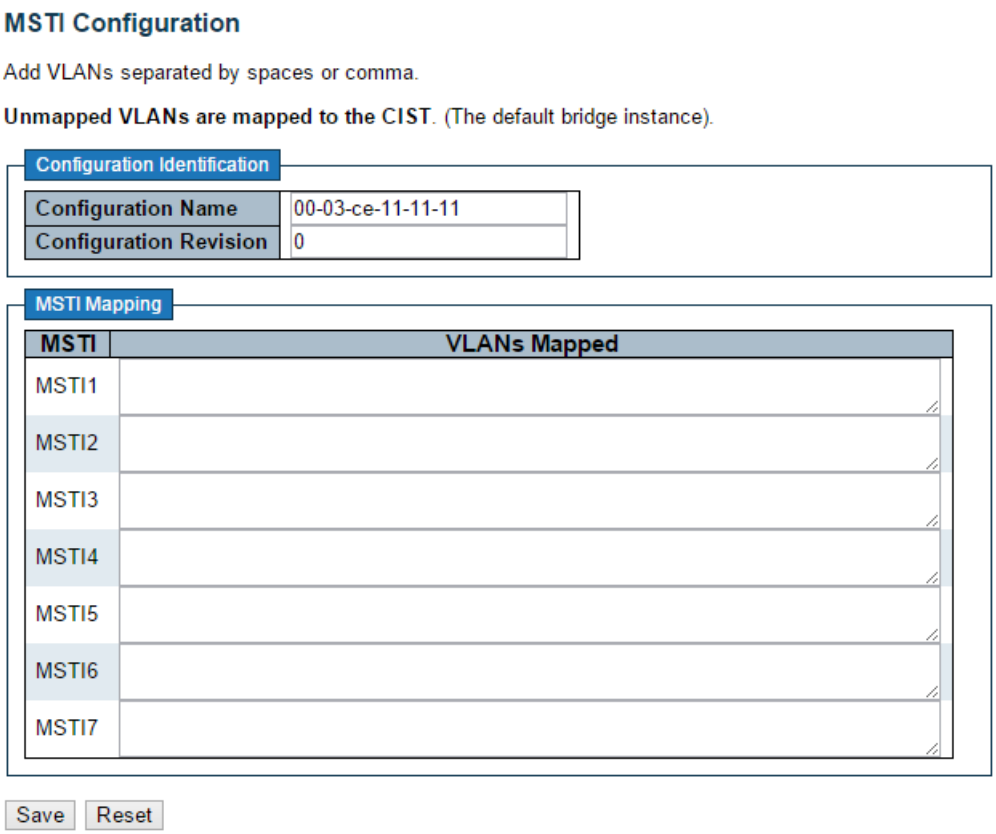
Port Error Recovery Timeout

The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.8.2. Spanning Tree - MSTI Mapping



This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Configuration Identification

Configuration Name

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

MSTI

The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

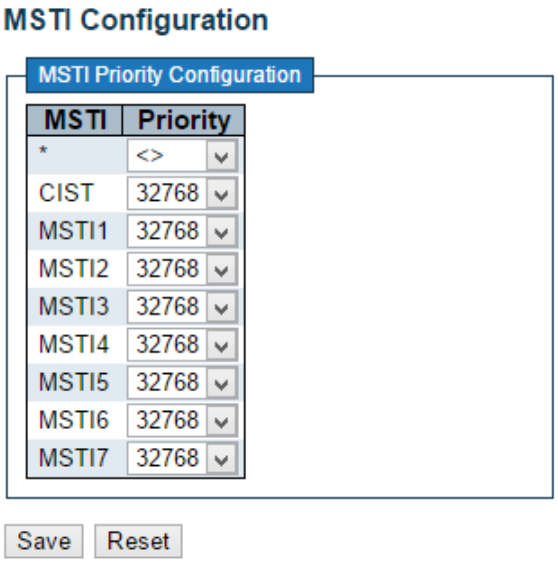
VLANs Mapped

The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2,5,20-40.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.8.3. Spanning Tree - MSTI Priorities



This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

MSTI

The bridge instance. The CIST is the default instance, which is always active.

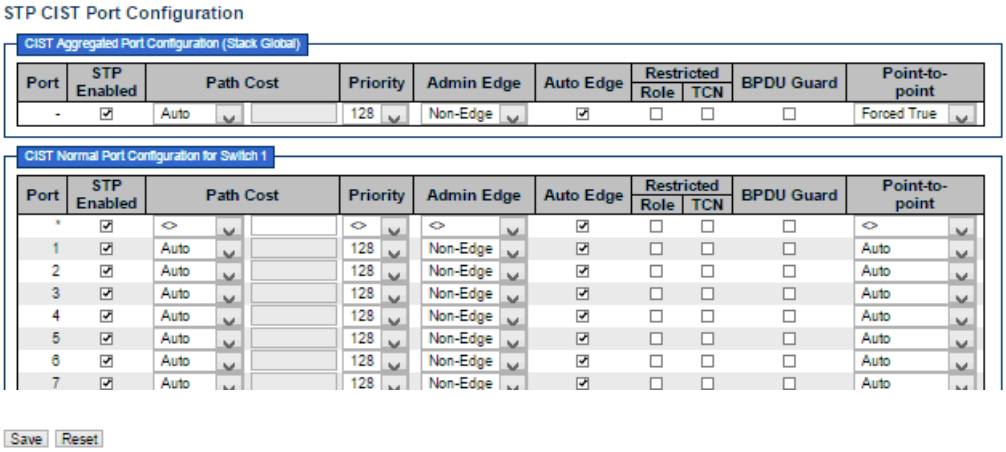
Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.8.4. Spanning Tree - CIST Ports



This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well.

This page contains settings for physical and aggregated ports. The aggregation settings are stack global.

The STP port settings relate to the currently selected stack unit, as reflected by the page header.

Port

The switch port number of the logical STP port.

STP Enabled

Controls whether STP is enabled on this switch port.

Path Cost

Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority

Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

operEdge (state flag)

Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

AdminEdge

Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

AutoEdge

Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role

If enabled, 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 vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN

If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard

If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting.
A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

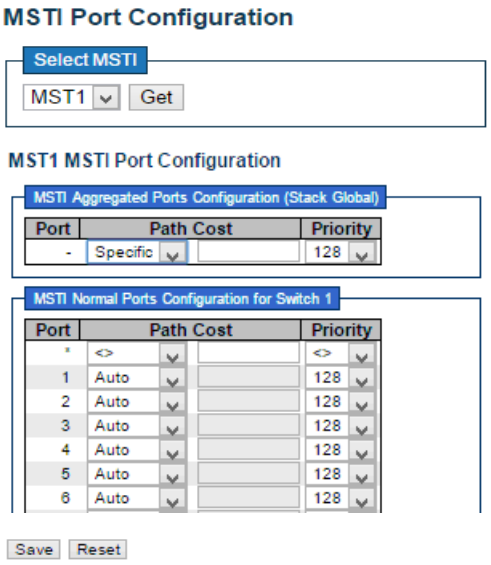
Point-to-Point

Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.8.5. Spanning Tree - MSTI Ports



This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well.

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are stack global.

Apart from the selected MSTI, the STP MSTI port settings also relate to thecurrently selected stack unit, as reflected by the page header.

Port

The switch port number of the corresponding STP CIST (and MSTI) port.

Path Cost

Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority

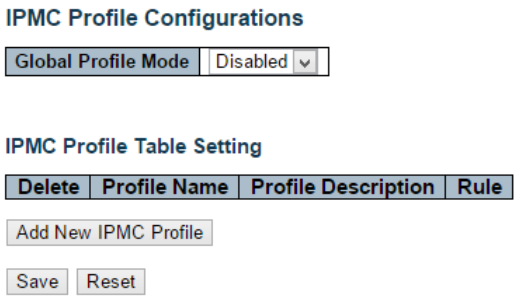
Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

Buttons

- **Get:** Click to retrieve settings for a specific MSTI.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.9. Configuration - IPMC Profile

3.1.9.1. IPMC Profile - Profile Table



This page provides IPMC Profile related configurations.

The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64Profiles with at maximum 128 corresponding rules for each.

Global Profile Mode

Enable/Disable the Global IPMC Profile.

System starts to do filtering based on profile settings only when the global profile mode is enabled.

Delete

Check to delete the entry.

The designated entry will be deleted during the next save.

Profile Name

The name used for indexing the profile table.

Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

Profile Description

Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile.

No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.

Rule

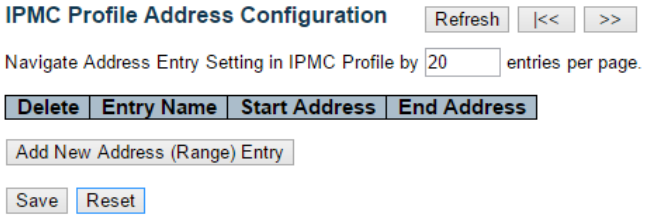
When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:

-  **Navigate:** List the rules associated with the designated profile.
-  **Edit:** Adjust the rules associated with the designated profile.

Buttons

- **Add New IPMC Profile:** Click to add new IPMC profile. Specify the name and configure the new entry. Click "Save".
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.9.2. IPMC Profile - Address Entry



This page provides address range settings used in IPMC profile.

The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create at maximum 128 address entries in the system.

Delete

Check to delete the entry.

The designated entry will be deleted during the next save.

Entry Name

The name used for indexing the address entry table.

Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

Start Address

The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

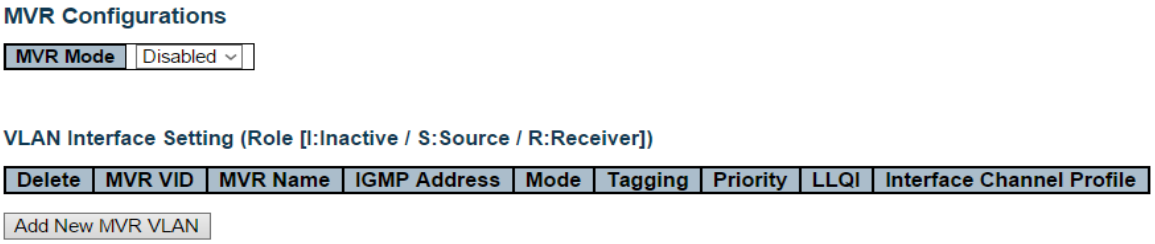
End Address

The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons

- **Add New Address (Range) Entry:** Click to add new address range. Specify the name and configure the addresses. Click "Save"
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table starting from the first entry in the IPMC Profile Address Configuration.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.1.10. Configuration - MVR



This page provides MVR related configurations.

Most of the settings are global, whereas the Immediate Leave and MVR Port-Role configuration is related to the current selecting stack unit, as reflected by the page header.

The MVR feature enables multicast traffic forwarding on the Multicast VLANs. In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports. It is allowed to create at maximum 8 MVR VLANs with corresponding channel settings for each Multicast VLAN. There will be totally at maximum 256 group addresses for channel settings.

MVR Mode

Enable/Disable the Global MVR.

The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping.

It is suggested to enable Unregistered Flooding control when the MVR group table is full.

Delete

Check to delete the entry. The designated entry will be deleted during the next save.

MVR VID

Specify the Multicast VLAN ID.

Note: MVR source ports are not recommended to be overlapped with management VLAN ports.

MVR Name

MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

Mode

Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.

Tagging

Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.

Priority

Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

LLQI

Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.

Interface Channel Setting

When the MVR VLAN is created, click the Edit symbol to expand the corresponding multicast channel settings for the specific MVR VLAN. Summary about the Interface Channel Setting (of the MVR VLAN) will be shown besides the Edit symbol.

Detail information regarding to the Interface Channel Setting will be covered on page 122.

Port

The logical port for the settings.

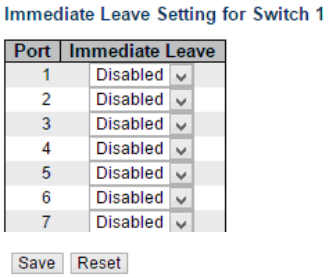
Port Role

Configure an MVR port of the designated MVR VLAN as one of the following roles.

- **Inactive (I):** The designated port does not participate MVR operations.
- **Source (S):** Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.
- **Receiver (R):** Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

Note: MVR source ports are not recommended to be overlapped with management VLAN ports.

Select the port role by clicking the Role symbol to switch the setting.

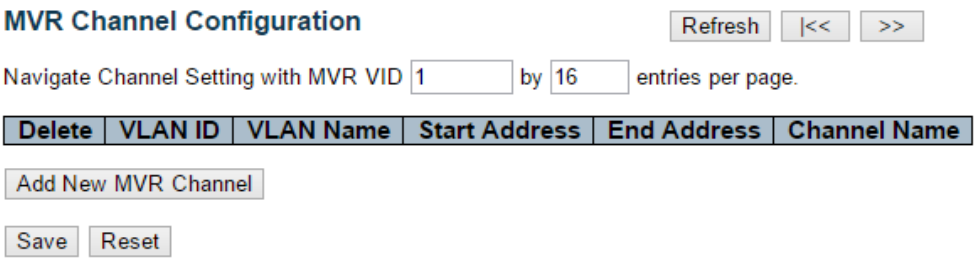


Immediate Leave

Enable the fast leave on the port.

Buttons

- **Add New NVR VLAN:** Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Save".
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.



This page provides MVR channel settings for a specific MVR VLAN.

Delete

Check to delete the entry. The designated entry will be deleted during the next save.

VLAN ID

Display the specific Multicast VLAN ID. This field is not editable.

VLAN Name

Display the name of the specific Multicast VLAN. This field is not editable.

Start Address

The starting IPv4/IPv6 Multicast Group Address that will be used as a streaming channel.

End Address

The ending IPv4/IPv6 Multicast Group Address that will be used as a streaming channel.

Channel Name

Indicate the name of the Channel of the specific Multicast VLAN. Maximum length of the Channel Name string is 32. Channel Name can only contain alphabets or numbers. Channel name should contain at least one alphabet. Channel name can be edited for the existing Channel entries or it can be added to the new entries.

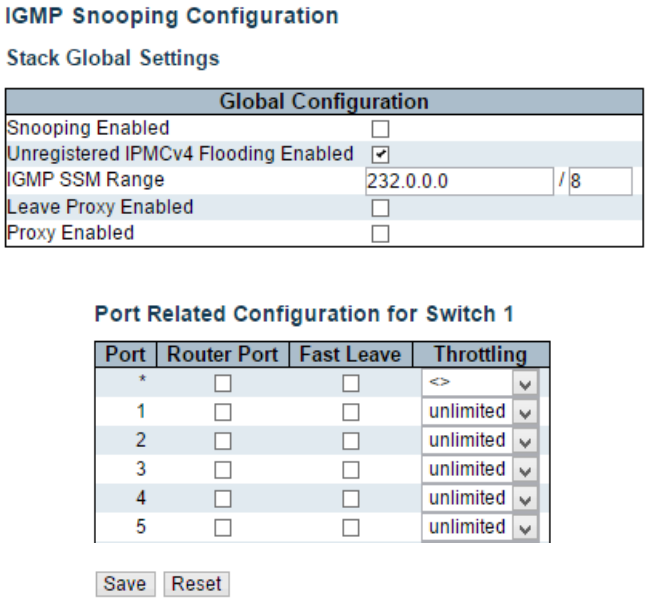
Buttons

- **Add New MVR Channel:** Click to add new Channel for a given MVR VLAN. Specify the Address and configure the new entry. Click "Save"
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table starting from the first entry in the MVR Channel Configuration for a specific MVR VLAN.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.1.11. Configuration - IPMC

3.1.11.1. IPMC - IGMP Snooping

3.1.11.1.1. IPMC - IGMP Snooping - Basic Configuration



This page provides IGMP Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the currently selected stack unit, as reflected by the page header.

Snooping Enabled

Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding Enabled

Enable unregistered IPMCv4 traffic flooding.

The flooding control takes effect only when IGMP Snooping is enabled.

When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.

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

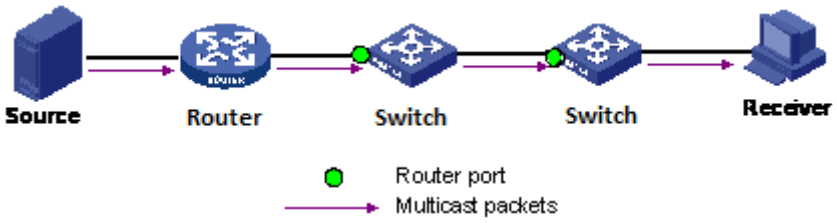
Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.



If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

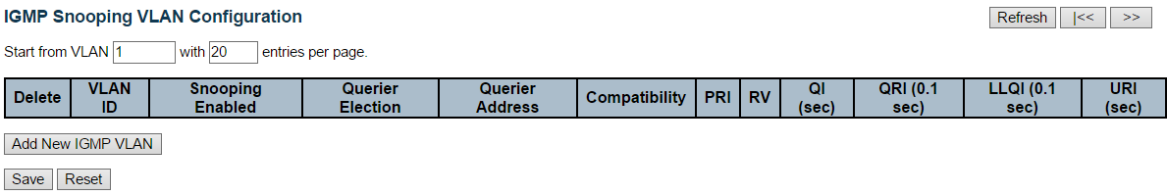
Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.11.1.2. IPMC - IGMP Snooping - VLAN Configuration



Navigating the IGMP Snooping VLAN Table

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match.

The >> button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

IGMP Snooping VLAN Table Columns

Delete

Check to delete the entry. The designated entry will be deleted during the next save.

VLAN ID

The VLAN ID of the entry.

IGMP Snooping Enabled

Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.

Querier Election

Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address

Define the IPv4 address as source address used in IP header for IGMP Querier election.

When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address.

Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Compatibility

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.

The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

PRI

Priority of Interface.

It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

RV

Robustness Variable.

The Robustness Variable allows tuning for the expected packet loss on a network.

The allowed range is 1 to 255, default robustness variable value is 2.

QI

Query Interval.

The Query Interval is the interval between General Queries sent by the Querier.

The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

QRI

Query Response Interval.

The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.

The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP)

Last Member Query Interval.

The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count.

The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is

10 in tenths of seconds (1 second).

URI

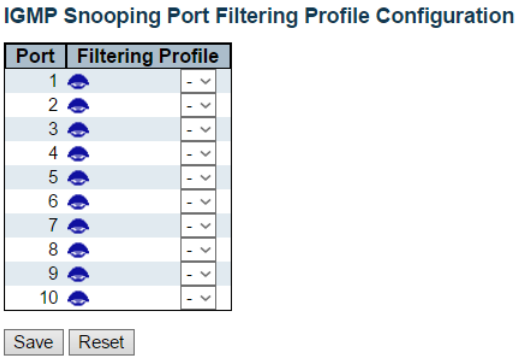
Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group.

The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

- **Refresh**: Refreshes the displayed table starting from the "VLAN" input fields.
- **<<:** Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.
- **Add New IGMP VLAN:** Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.
- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

3.1.11.1.3. IPMC - IGMP Snooping - Port Group Filtering



Port

The logical port for the settings.

Filtering Profile

Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:

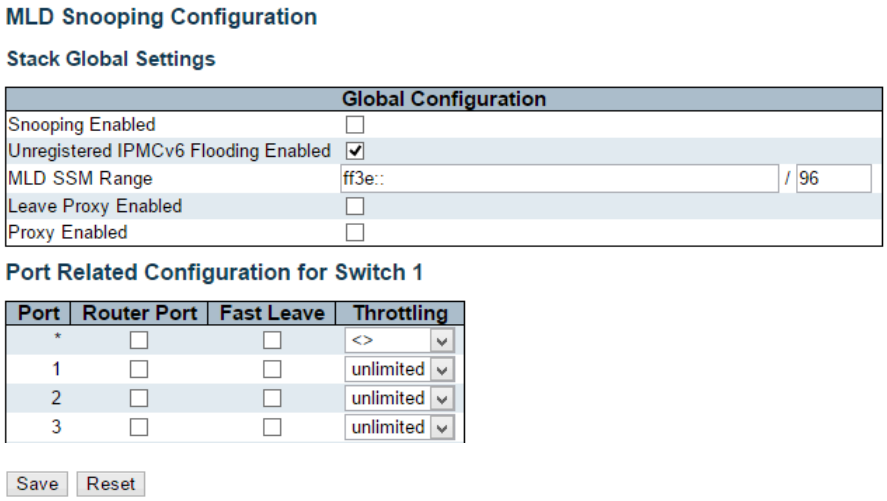
- **Navigate**: List the rules associated with the designated profile.

Buttons

- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

3.1.11.2. IPMC - MLD Snooping

3.1.11.2.1. IPMC - MLD Snooping - Basic Configuration



This page provides MLD Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the currently selected stack unit, as reflected by the page header.

Snooping Enabled

Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding Enabled

Enable unregistered IPMCv6 traffic flooding.

The flooding control takes effect only when MLD Snooping is enabled.

When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

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

Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

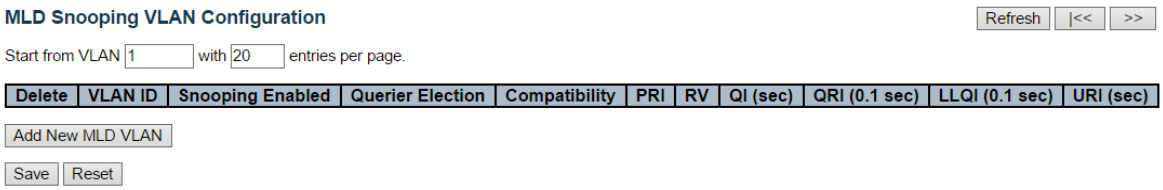
Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.11.2.2. IPMC - MLD Snooping - VLAN Configuration



Navigating the MLD Snooping VLAN Table

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match.

The >> button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

MLD Snooping VLAN Table Columns

Delete

Check to delete the entry. The designated entry will be deleted during the next save.

VLAN ID

The VLAN ID of the entry.

MLD Snooping Enabled

Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.

Querier Election

Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.

Compatibility

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network.

The allowed selection is MLD-Auto, Forced MLDv1, Forced MLDv2, default compatibility value is MLD-Auto.

PRI

Priority of Interface.

It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

RV

Robustness Variable.

The Robustness Variable allows tuning for the expected packet loss on a link.

The allowed range is 1 to 255, default robustness variable value is 2.

QI

Query Interval.

The Query Interval is the interval between General Queries sent by the Querier.

The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

QRI

Query Response Interval.

The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.

The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

LLQI

Last Listener Query Interval.

The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages.

The allowed range is 0 to 31744 in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).

URI

Unsolicited Report Interval.

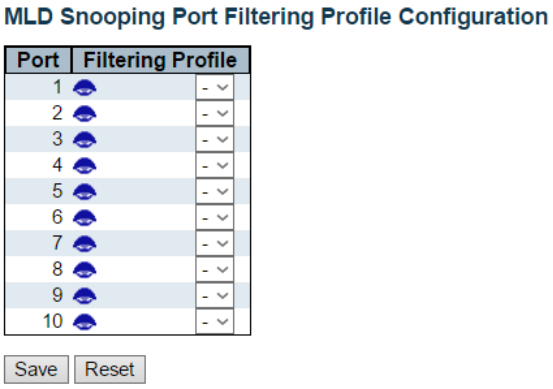
The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address.

The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

- **Refresh**: Refreshes the displayed table starting from the "VLAN" input fields.
- **<<:** Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.
- **Add New MLD VLAN:** Click to add new MLD VLAN. Specify the VID and configure the new entry. Click "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.
- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

3.1.11.2.3. IPMC - MLD Snooping - Port Group Filtering



Port

The logical port for the settings.

Filtering Profile

Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:

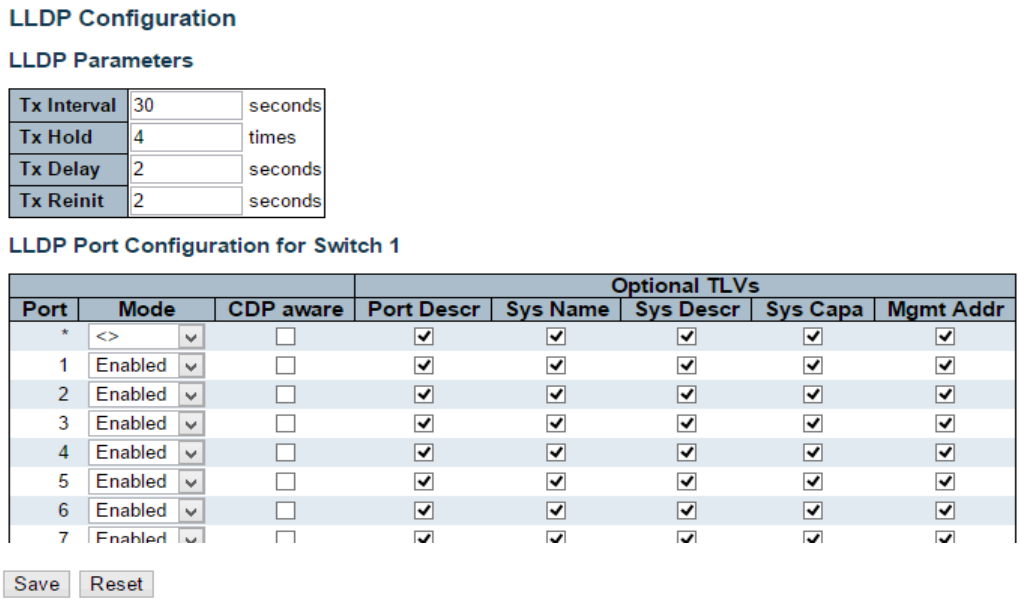
- **Navigate**: List the rules associated with the designated profile.

Buttons

- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

3.1.12. Configuration - LLDP

3.1.12.1. LLDP - LLDP



This page allows the user to inspect and configure the current LLDP port settings.

LLDP Parameters

Tx Interval

The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.

Tx Hold

Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.

Tx Delay

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.

Tx Reinit

When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, Signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

The LLDP port settings relate to the currently selected stack unit, as reflected by the page header.

Port

The switch port number of the logical LLDP port.

Mode

Select LLDP mode.

Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.

Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information.

Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors.

Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

CDP Aware

Select CDP awareness.

The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.

CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.

Note: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.

Port Descr

Optional TLV: When checked the "port description" is included in LLDP information transmitted.

Sys Name

Optional TLV: When checked the "system name" is included in LLDP information transmitted.

Sys Descr

Optional TLV: When checked the "system description" is included in LLDP information transmitted.

Sys Capa

Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

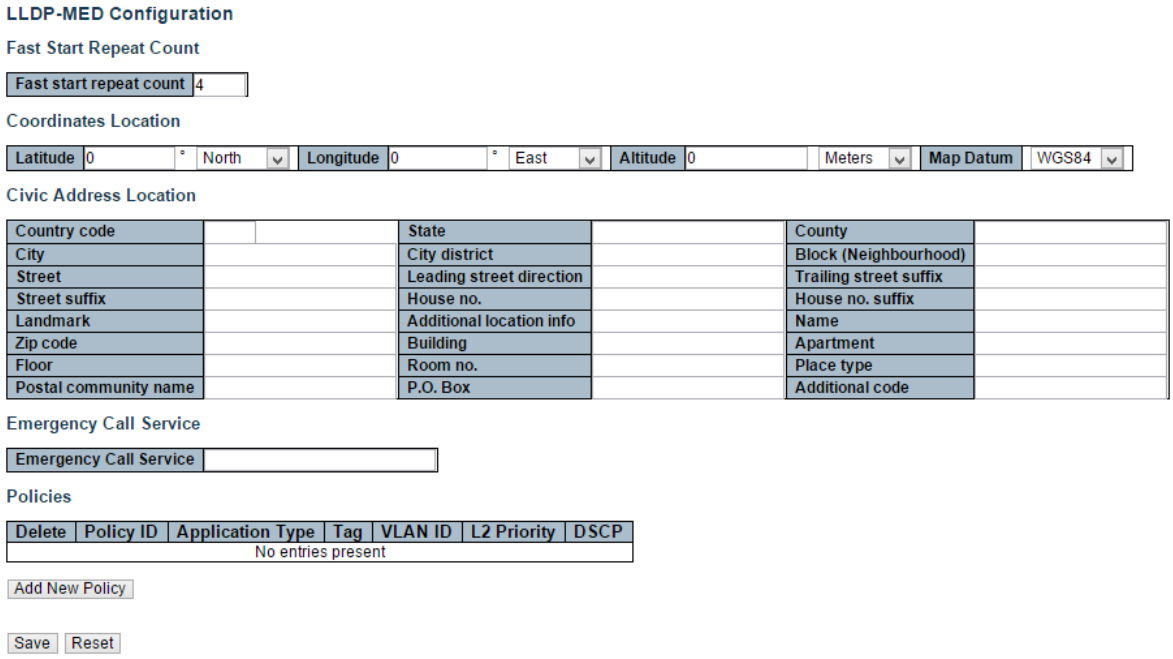
Mgmt Addr

Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.12.2. LLDP - LLDP-MED



This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

Fast start repeat count

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. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the

possibility of the neighbors receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an 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 Network Connectivity Devices, or 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 (Neighborhood)
Neighborhood, block.

Street
Street - Example: Poppelvej.

Leading street direction
Leading street direction - Example: N.

Trailing street suffix
Trailing street suffix - Example: SW.

Street suffix
Street suffix - Example: Ave, Platz.

House no.
House number - Example: 21.

House no. suffix
House number suffix - Example: A, 1/2.

Landmark
Landmark or vanity address - Example: Columbia University.

Additional location info
Additional location info - Example: South Wing.

Name

Name (residence and office occupant) - Example: Flemming Jahn.

Zip code

Postal/zip code - Example: 2791.

Building

Building (structure) - Example: Low Library.

Apartment

Unit (Apartment, suite) - Example: Apt 42.

Floor

Floor - Example: 4.

Room no.

Room number - Example: 450F.

Place type

Place type - Example: Office.

Postal community name

Postal community name - Example: Leonia.

P.O. Box

Post office box (P.O. BOX) - Example: 12345.

Additional code

Additional code - Example: 1320300003.

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Emergency Call Service

Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Delete

Check to delete the policy. It will be deleted during the next save.

Policy ID

ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.

Application Type

Intended use of the application types:

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

2. Voice Signaling (conditional) - for use in network topologies that require a different policy for the voice Signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.
3. Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signaling (conditional) - for use in network topologies that require a different policy for the guest voice Signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.
5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.
6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signaling (conditional) - for use in network topologies that require a separate policy for the video Signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

Tag

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

Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format

also includes priority tagged frames as defined by IEEE 802.1Q-2003.

VLAN ID

VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.

L2 Priority

L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

DSCP

DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Adding a new policy

Click "**Add New Policy**" to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save".

The number of policies supported is 32

Port Policies Configuration

Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

Port

The port number to which the configuration applies.

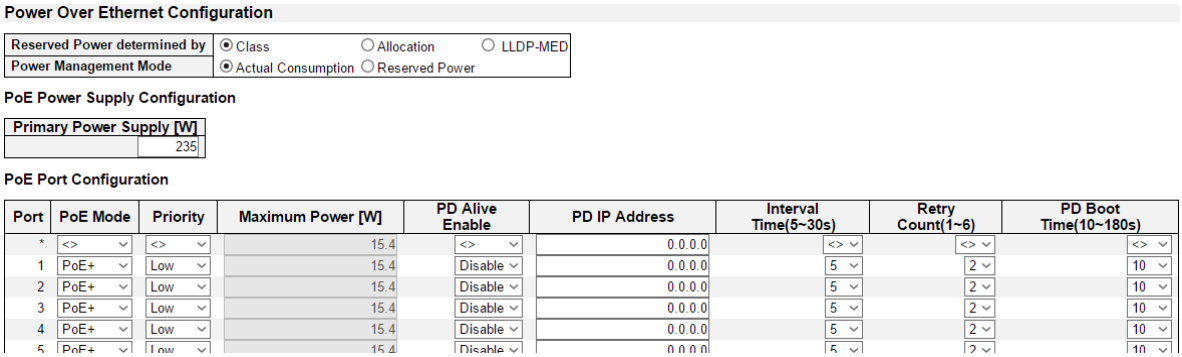
Policy Id

The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.13. Configuration - PoE



Power Over Ethernet Configuration

Reserved Power determined by	◉ Class ○ Allocation ○ LLDP-MED
Power Management Mode	◉ Actual Consumption ○ Reserved Power

PoE Power Supply Configuration

Primary Power Supply [W]
235

PoE Port Configuration

Port	PoE Mode	Priority	Maximum Power [W]	PD Alive Enable	PD IP Address	Interval Time(5~30s)	Retry Count(1~6)	PD Boot Time(10~180s)
*	<>	<>	15.4	<>	0.0.0.0	<>	<>	<>
1	PoE+	Low	15.4	Disable	0.0.0.0	5	2	10
2	PoE+	Low	15.4	Disable	0.0.0.0	5	2	10
3	PoE+	Low	15.4	Disable	0.0.0.0	5	2	10
4	PoE+	Low	15.4	Disable	0.0.0.0	5	2	10
5	PoE+	Low	15.4	Disable	0.0.0.0	5	2	10

This page allows the user to inspect and configure the current PoE port settings.

Power over Ethernet Configuration

Reserved Power determined by

There are three modes for configuring how the ports/PDs may reserve power.

1. Allocated mode: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.
2. Class mode: In this mode each port automatically determines how much power toreserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect.
3. LLDP-MED mode: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode. In this mode the Maximum Power fields have no effect

For all modes: If a port uses more power than the reserved power for the port, the port is shut down.

Power Management Mode

There are 2 modes for configuring when to shut down the ports:

1. Actual Consumption: In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.
2. Reserved Power: In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.

Power Supply Configuration

Primary and Backup Power Source

Some switches support having two PoE power supplies. One is used as primary power source, and one as backup power source. If the switch doesn't support backup power supply only the primary power supply settings will be shown. In case that the primary power source fails the backup power source will take over. For being able to determine the amount of power the PD may use, it must be defined what amount of power the primary and backup power sources can deliver.

Valid values are in the range 0 to 2000 Watts.

Port Configuration

Port

This is the logical port number for this row.

Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.

PoE Mode

The PoE Mode represents the PoE operating mode for the port.

- **Disabled:** PoE disabled for the port.
- **PoE:** Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W)
- **PoE+**: Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W)

Priority

The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.

The priority is used in the case where the remote devices requires more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

Maximum Power

The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.

The maximum allowed value is 30 W.

PD Alive Enable

This scroll-down menu allows you to enable/disable PD Alive function/Self healing.

PD Alive IP Address

Here you can input the network device's IP address connected to a specific port. The system will try to ping (using the IP address input here) and get a reply from the network device 5 times in a 3 minute interval. If the system isn't getting any replies from the network device, that PoE port will be turned off and turned back on (power cycle).

Interval Time (5~30S)

Here you can set the ping interval time. When set, the PoE switch will ping the PoE device connected to that port once with the interval time you set here.

Retry Count

Here you can set the ping retry count.

PD Boot Time (10~180S)

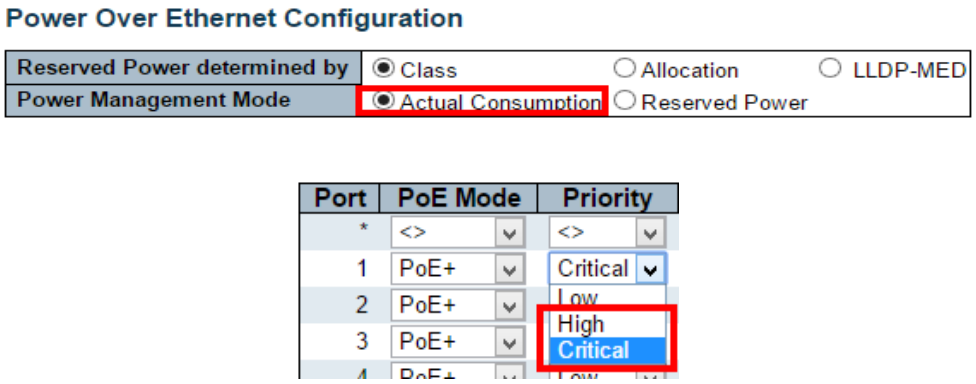
Here you can set the PD boot time. If the PoE switch does not get any reply from the PoE device connected to that port within the time you set here, That port will go through a power cycle.

Buttons

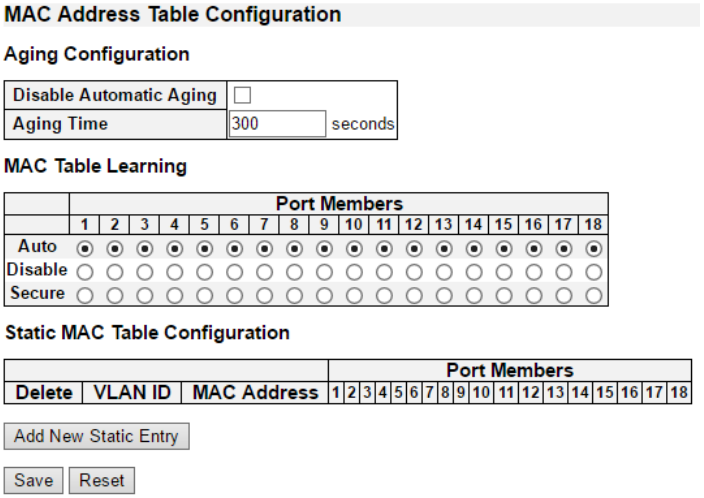
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

Note: If a PD is connected to the PoE switch and the PoE budget is not enough for that PD, the PoE LED will be blinking and provides no power to the newly connected PD.

It is recommended to set the Power Management Mode to **Actual Consumption**, and set the ports that connect to crucial devices to **High** or **Critical** as shown in the figures down below.



3.1.14. Configuration - MAC Table



The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds. The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking the "**Disable automatic aging**" checkbox. .

MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can do learning based upon the following settings:

Auto

Learning is done automatically as soon as a frame with unknown SMAC is received.

Disable

No learning is done.

Secure

Only static MAC entries are learned, all other frames are 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

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.

Delete

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

VLAN ID

The VLAN ID of the entry.

MAC Address

The MAC address of the entry.

Port Members

Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

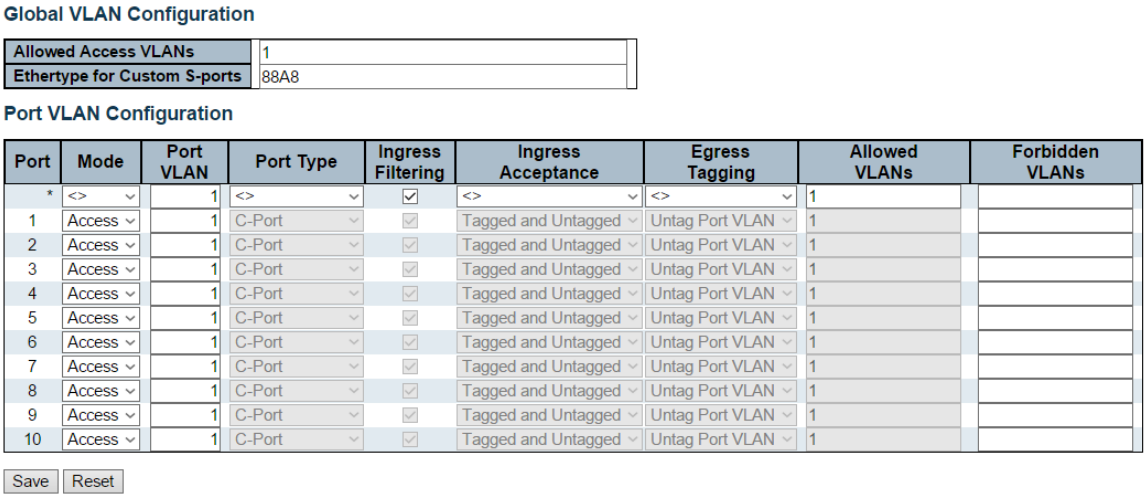
Adding a New Static Entry

Click "**Add New Static Entry**" to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.15. Configuration - VLANs



This page allows for controlling VLAN configuration on the switch.

The page is divided into a global section and a per-port configuration section.

Global VLAN Configuration

Allowed Access VLANs

This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

Ethertype for Custom S-ports

This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration

Port

This is the logical port number of this row.

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

Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1.

On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.

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

Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

Unaware:
On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

C-Port:
On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.

S-Port:
On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

S-Custom-Port:
On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.

Ingress Filtering

Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.

If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.

If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

Ingress Acceptance

Hybrid ports allow for changing the type of frames that are accepted on ingress.

Tagged and Untagged

Both tagged and untagged frames are accepted.

Tagged Only

Only tagged frames are accepted on ingress. Untagged frames are discarded.

Untagged Only

Only untagged frames are accepted on ingress. Tagged frames are discarded.

Egress Tagging

Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

Untag Port VLAN

Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.

Tag All

All frames, whether classified to the Port VLAN or not, are transmitted with a tag.

Untag All

All frames, whether classified to the Port VLAN or not, are transmitted without a tag.

This option is only available for ports in Hybrid mode.

Allowed VLANs

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.

The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095.

The field may be left empty, which means that the port will not become member of any VLANs.

Forbidden VLANs

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. The syntax is identical to the syntax used in the Enabled VLANs field.

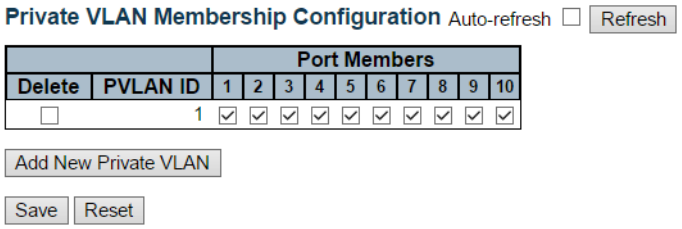
By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Buttons

- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

3.1.16. Configuration - Private VLAN

3.1.16.1. Private VLAN - Membership



The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This 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.

Delete

To delete a private VLAN entry, check this box. The entry will be deleted during the next save.

Private VLAN ID

Indicates the ID of this particular private VLAN.

Port Members

A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New Private VLAN

Click Add New Private VLAN to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.

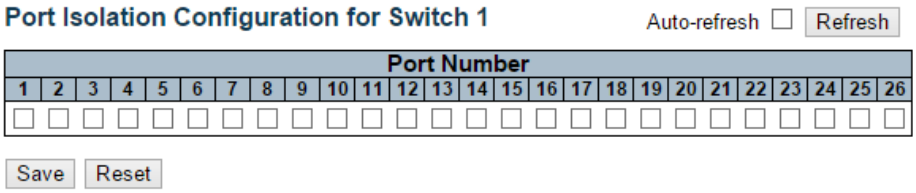
The Private VLAN is enabled when you click "Save".

The Delete button can be used to undo the addition of new Private VLANs.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh**: Click to refresh the page immediately.
- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

3.1.16.2. Private VLAN - Port Isolation



Overview

This page is used for enabling or disabling port isolation on ports in a Private VLAN.

A port member of a VLAN can be isolated to other isolated ports on the same VLAN.

The port settings relate to the currently selected stack unit, as reflected by the page header.

This feature works across the stack.

Configuration

Port Members

A check box is provided for each port of a private VLAN.

When checked, port isolation is enabled on that port.

When unchecked, port isolation is disabled on that port.

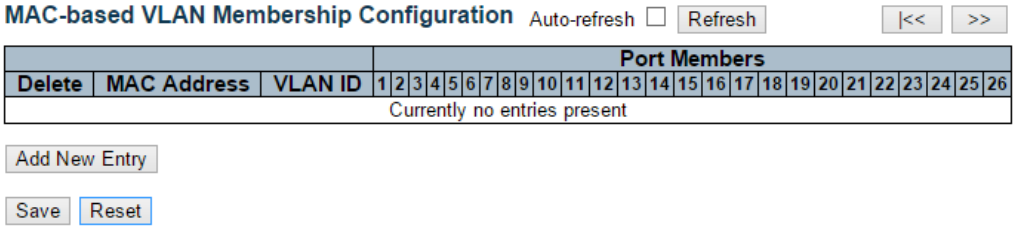
By default, port isolation is disabled on all ports.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.17. Configuration - VCL

3.1.17.1. VCL - MAC-based VLAN



The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Delete

To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

MAC Address

Indicates the MAC address.

VLAN ID

Indicates the VLAN ID.

Port Members

A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New MAC-based VLAN

Click "**Adding New Entry**" to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095.

The MAC-based VLAN entry is enabled on the selected stack switch unit when you click on "Save". A MAC-based VLAN without any port members on any stack unit will be deleted when you click "Save".

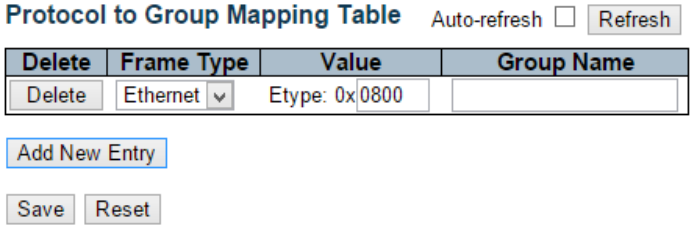
The "**Delete**" button can be used to undo the addition of new MAC-based VLANs. The maximum possible MAC-based VLAN entries are limited to 256.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **|<<:** Updates the table starting from the first entry in the MAC-based VLAN Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.1.17.2. VCL - Port-based VLAN

3.1.17.2.1. VCL - Port-based VLAN - Protocol to Group



This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the selected stack switch unit.

Delete

To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.

Frame Type

Frame Type can have one of the following values:

1. Ethernet
2. LLC
3. SNAP

Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.

Value

Valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu.

Below is the criteria for three different Frame Types:

1. For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff
2. For LLC: Valid value in this case is comprised of two different sub-values.
   a. **DSAP:** 1-byte long string (0x00-0xff)
   b. **SSAP:** 1-byte long string (0x00-0xff)
3. For SNAP: Valid value in this case also is comprised of two different sub-values.
   a. **OUI:** OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.
   b. **PID:** 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 an

OUI for 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 OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

Group Name

A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-z) and integers(0-9).

Note: special character and underscore(_) are not allowed.

Adding a New Group to VLAN mapping entry

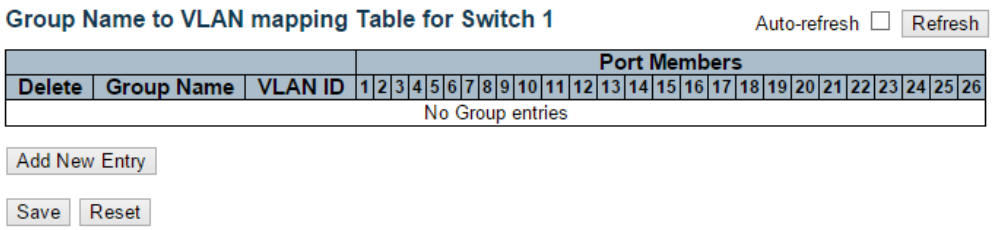
Click "**Add New Entry**" to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed.

The "**Delete**" button can be used to undo the addition of new entry. The maximum possible Protocol to Group mappings are limited to 128.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.

3.1.17.2.2. VCL - Port-based VLAN - Group to VLAN



This page allows you to map an already configured Group Name to a VLAN for the selected stack switch unit.

Delete

To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save

Group Name

A valid Group Name is a string at the most 16 characters which consists of a combination of alphabets (a-z or A-z) and integers(0-9), no special character is allowed. Whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.

VLAN ID

Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.

Port Members

A row of check boxes for each port is displayed for each Group Name toVLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New Group to VLAN mapping entry

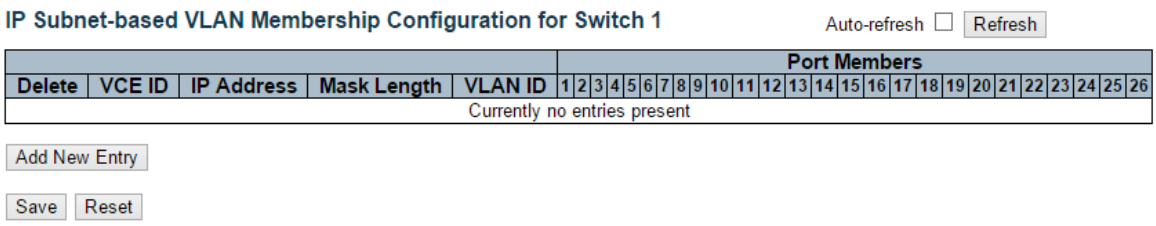
Click "**Add New Entry**" to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095.

The "**Delete**" button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 64.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.

3.1.17.3. VCL - IP Subnet-based VLAN



The IP subnet-based VLAN entries can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Delete

To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

VCE ID

Indicates the index of the entry. It is user configurable. It's value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.

IP Address

Indicates the IP address.

Mask Length

Indicates the network mask length.

VLAN ID

Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

Port Members

A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New IP subnet-based VLAN

Click "**Add New Entry**" to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 through 4095.

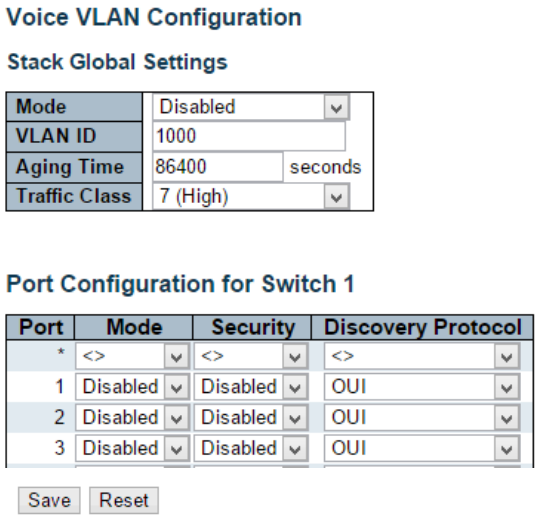
The IP subnet-based VLAN entry is enabled on the selected stack switch unit when you click on "Save". The "**Delete**" button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table.

3.1.18. Configuration - Voice VLAN

3.1.18.1. Voice VLAN - Configuration



The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Mode

Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

- **Enabled:** Enable Voice VLAN mode operation.
- **Disabled:** Disable Voice VLAN mode operation.

VLAN ID

Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.

Aging Time

Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

Traffic Class

Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

Port Mode

Indicates the Voice VLAN port mode.

Possible port modes are:

- **Disabled:** Disjoin from Voice VLAN.
- **Auto:** Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.
- **Forced:** Force join to Voice VLAN.

Port Security

Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

- **Enabled:** Enable Voice VLAN security mode operation.
- **Disabled:** Disable Voice VLAN security mode operation.

Port Discovery Protocol

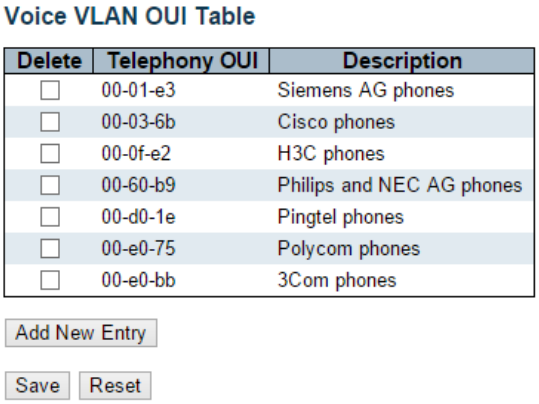
Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:

- **OUI:** Detect telephony device by OUI address.
- **LLDP:** Detect telephony device by LLDP.
- **Both:** Both OUI and LLDP.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.18.2. Voice VLAN - OUI



Configure VOICE VLAN OUI table on this page. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of OUI process.

Delete

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

Telephony OUI

A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

Description

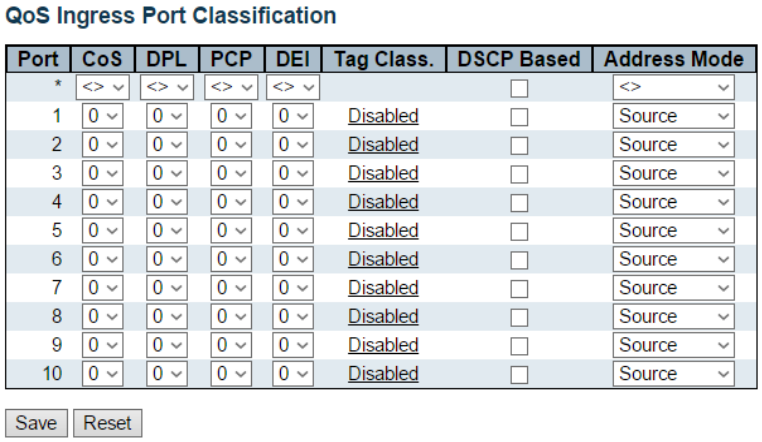
The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

Buttons

- **Add New Entry:** Click to add a new access management entry.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.19. Configuration - QoS

3.1.19.1. QoS - Port Classification



QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<>	<>	<>	<>			<>
1	0	0	0	0	Disabled		Source
2	0	0	0	0	Disabled		Source
3	0	0	0	0	Disabled		Source
4	0	0	0	0	Disabled		Source
5	0	0	0	0	Disabled		Source
6	0	0	0	0	Disabled		Source
7	0	0	0	0	Disabled		Source
8	0	0	0	0	Disabled		Source
9	0	0	0	0	Disabled		Source
10	0	0	0	0	Disabled		Source

Save Reset

This page allows you to configure the basic QoS Ingress Classification settings for all switch ports.

Port

The port number for which the configuration below applies.

CoS

Controls the default class of service.

All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.

The classified CoS can be overruled by a QCL entry.

Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

DPL

Controls the default drop precedence level.

All frames are classified to a drop precedence level.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

The classified DPL can be overruled by a QCL entry.

PCP

Controls the default PCP value.

All frames are classified to a PCP value.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

DEI

Controls the default DEI value.

All frames are classified to a DEI value.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

Tag Class.

Shows the classification mode for tagged frames on this port.

- **Disabled**: Use default CoS and DPL for tagged frames.
- **Enabled**: Use mapped versions of PCP and DEI for tagged frames.

Click on the mode in order to configure the mode and/or mapping.

Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

DSCP Based

Click to Enable DSCP Based QoS Ingress Port Classification.

Address Mode

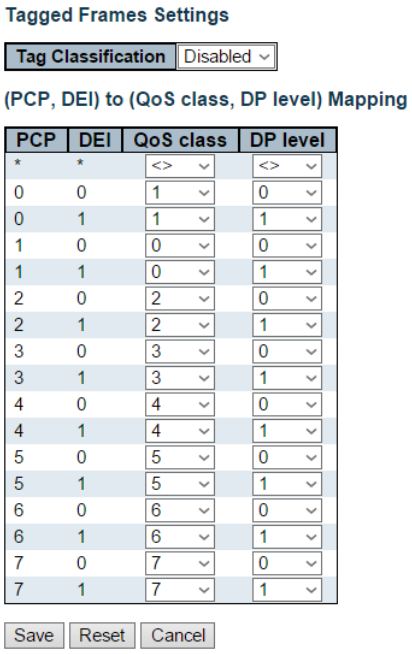
The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are:

- **Source**: Enable SMAC/SIP matching.
- **Destination**: Enable DMAC/DIP matching.

Buttons

- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

QoS Ingress Port Tag Classification for Specific Port



The classification mode for tagged frames are configured on this page.

Tag Classification

Controls the classification mode for tagged frames on this port.

- **Disabled**: Use default QoS class and Drop Precedence Level for tagged frames.
- **Enabled**: Use mapped versions of PCP and DEI for tagged frames.

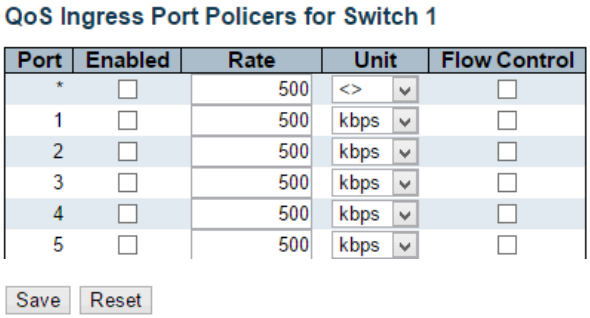
(PCP, DEI) to (QoS class, DP level) Mapping

Controls the mapping of the classified (PCP, DEI) to (QoS class, DP level) values when Tag Classification is set to Enabled.

Buttons

- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.
- **Cancel**: Click to undo any changes made locally and return to the previous page.

3.1.19.2. QoS - Port Policing



This page allows you to configure the Policer settings for all switch ports.

The settings relate to the currently selected stack unit, as reflected by the page header.

Port

The port number for which the configuration below applies.

Enabled

Controls whether the policer is enabled on this switch port.

Rate

Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-13200 when the "Unit" is "Mbps" or "kfps".

Unit

Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".

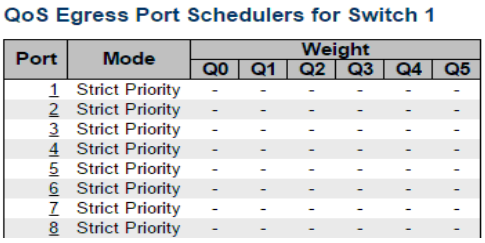
Flow Control

If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.19.3. QoS - Port Scheduler



QoS Egress Port Schedulers for Switch 1

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

The ports belong to the currently selected stack unit, as reflected by the page header.

Port

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

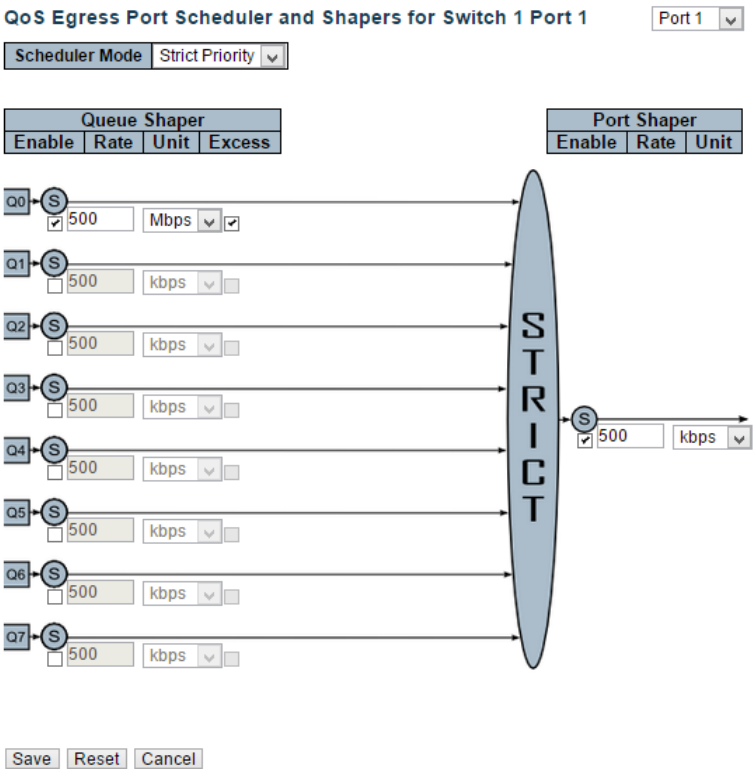
Click on the port number in order to configure the schedulers.

Mode

Shows the scheduling mode for this port.

Qn

Shows the weight for this queue and port.



This page allows you to configure the Scheduler and Shapers for a specific port.

The settings relate to the currently selected stack unit, as reflected by the page header.

Scheduler Mode

Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable

Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate

Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Queue Shaper Unit

Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess

Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight

Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent

Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable

Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate

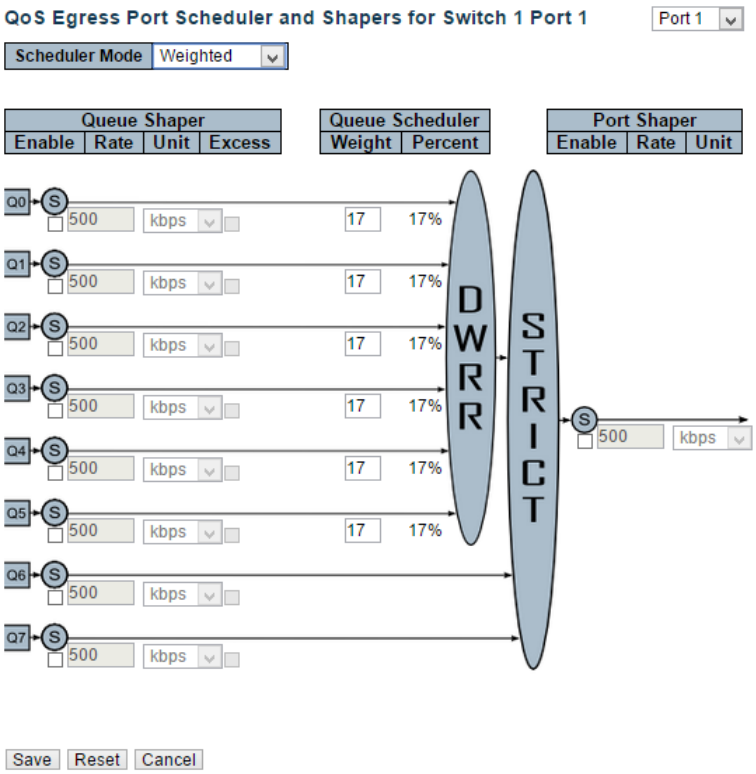
Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Port Shaper Unit

Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Click to undo any changes made locally and return to the previous page.



This page allows you to configure the Scheduler and Shapers for a specific port.

The settings relate to the currently selected stack unit, as reflected by the page header.

Scheduler Mode

Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable

Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate

Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Queue Shaper Unit

Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess

Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight

Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent

Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable

Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate

Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Port Shaper Unit

Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Click to undo any changes made locally and return to the previous page.

3.1.19.4. QoS - Port Shaping

QoS Egress Port Shapers for Switch 1

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 page provides an overview of QoS Egress Port Shapers for all switch ports.

The ports belong to the currently selected stack unit, as reflected by the page header.

Port

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

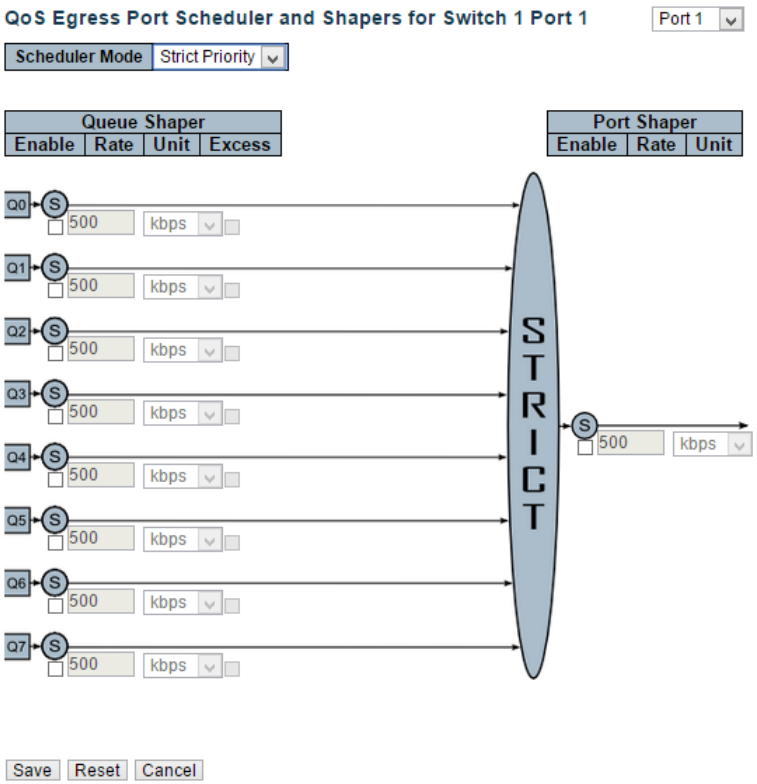
Click on the port number in order to configure the shapers.

Qn

Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".

Port

Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".



This page allows you to configure the Scheduler and Shapers for a specific port.

The settings relate to the currently selected stack unit, as reflected by the page header.

Scheduler Mode

Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable

Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate

Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Queue Shaper Unit

Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess

Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight

Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent

Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable

Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate

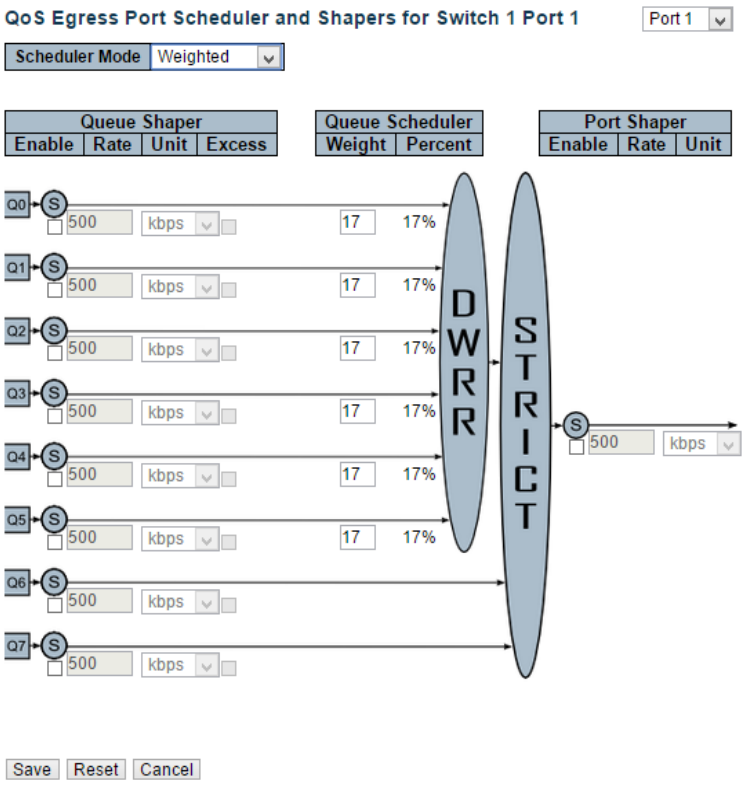
Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Port Shaper Unit

Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Click to undo any changes made locally and return to the previous page.



This page allows you to configure the Scheduler and Shapers for a specific port.

The settings relate to the currently selected stack unit, as reflected by the page header.

Scheduler Mode

Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.

Queue Shaper Enable

Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate

Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Queue Shaper Unit

Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess

Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight

Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent

Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable

Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate

Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

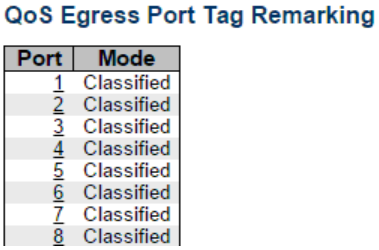
Port Shaper Unit

Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Click to undo any changes made locally and return to the previous page.

3.1.19.5. QoS - Port Tag Remarking



QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.

The ports belong to the currently selected stack unit, as reflected by the page header.

Port

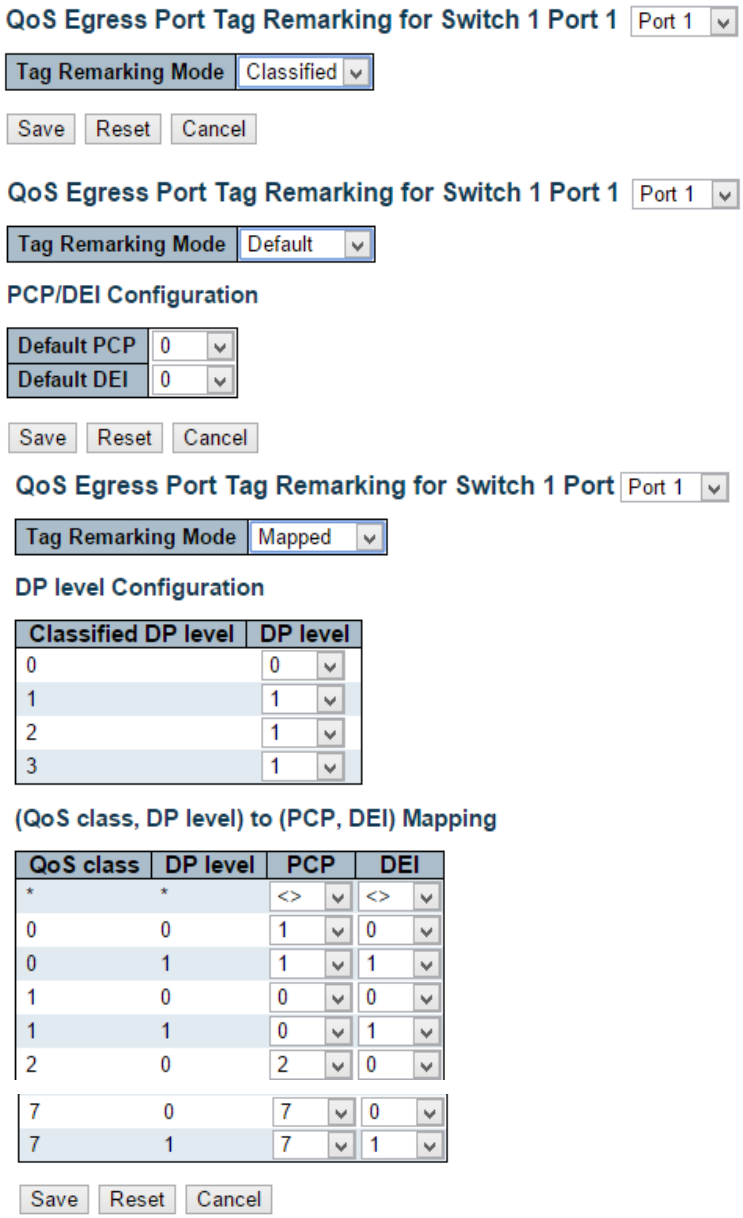
The logical port for the settings contained in the same row.

Click on the port number in order to configure tag remarking.

Mode

Shows the tag remarking mode for this port.

- **Classified:** Use classified PCP/DEI values.
- **Default:** Use default PCP/DEI values.
- **Mapped:** Use mapped versions of QoS class and DP level.



The QoS Egress Port Tag Remarking for a specific port are configured on this page.

Mode

Controls the tag remarking mode for this port.

- **Classified:** Use classified PCP/DEI values.
- **Default:** Use default PCP/DEI values.
- **Mapped:** Use mapped versions of QoS class and DP level.

PCP/DEI Configuration

Controls the default PCP and DEI values used when the mode is set to Default.

DP level Configuration

Controls the Drop Precedence level translation table when the mode is set to Mapped.

The purpose of this table is to reduce the 2 bit classified DP level to a 1 bit DP level used in the (QoS class, DP level) to (PCP, DEI) mapping process.

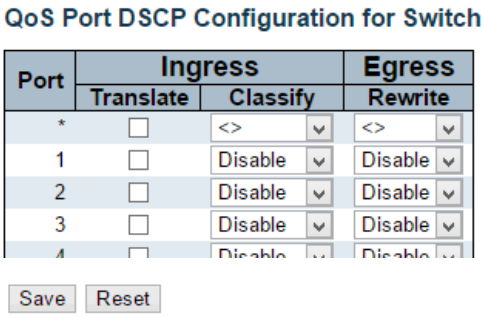
(QoS class, DP level) to (PCP, DEI) Mapping

Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Click to undo any changes made locally and return to the previous page.

3.1.19.6. QoS - Port DSCP



This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

The settings relate to the currently selected stack unit, as reflected by the page header.

Port

The Port column shows the list of ports for which you can configure dscp ingress and egress settings.

Ingress

In Ingress settings you can change ingress translation and classification settings for individual ports.

There are two configuration parameters available in Ingress:

1. Translate
2. Classify

1. Translate

To Enable the Ingress Translation click the checkbox.

2. Classify

Classification for a port have 4 different values.

- **Disable:** No Ingress DSCP Classification.
- **DSCP=0:** Classify if incoming (or translated if enabled) DSCP is 0.
- **Selected:** Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
- **All:** Classify all DSCP.

Egress

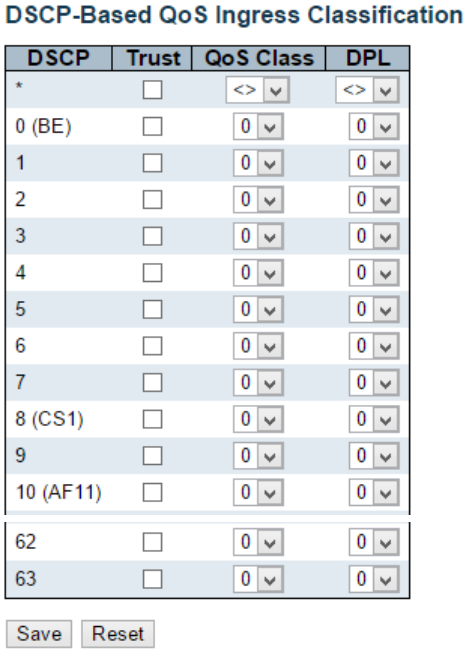
Port Egress Rewriting can be one of -

- **Disable:** No Egress rewrite.
- **Enable:** Rewrite enabled without remapping.
- **Remap:** DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.19.7. QoS - DSCP-Based QoS



This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

DSCP

Maximum number of supported DSCP values are 64.

Trust

Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.

QoS Class

QoS class value can be any of (0-7)

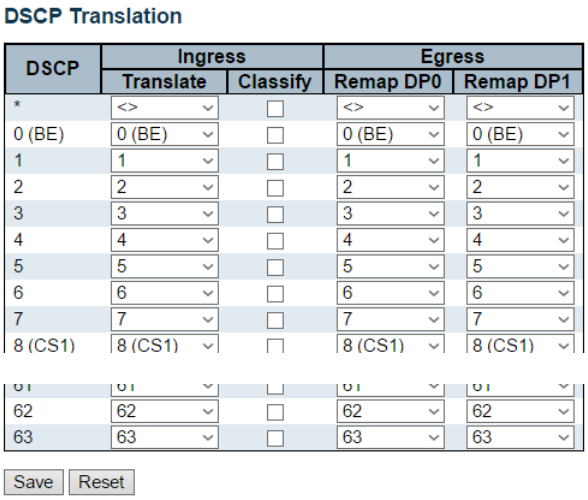
DPL

Drop Precedence Level (0-3)

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.19.8. QoS - DSCP Translation



This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

DSCP

Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

Ingress

Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

There are two configuration parameters for DSCP Translation -

1. Translate
2. Classify

1. Translate

DSCP at Ingress side can be translated to any of (0-63) DSCP values.

2. Classify

Click to enable Classification at Ingress side.

Egress

There are the following configurable parameters for Egress side -

1. Remap DP0 Controls the remapping for frames with DP level 0.
2. Remap DP1 Controls the remapping for frames with DP level 1.

1. Remap DP0

Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

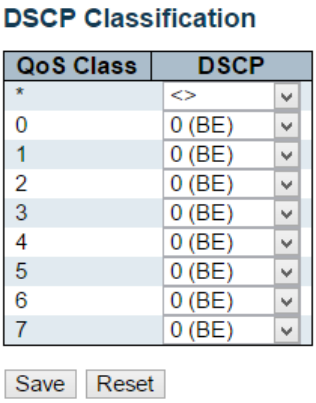
2. Remap DP1

Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Buttons

- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

3.1.19.9. QoS - DSCP Classification



This page allows you to configure the mapping of QoS class to DSCP value.

The settings relate to the currently selected stack unit, as reflected by the page header.

QoS Class

Actual QoS class.

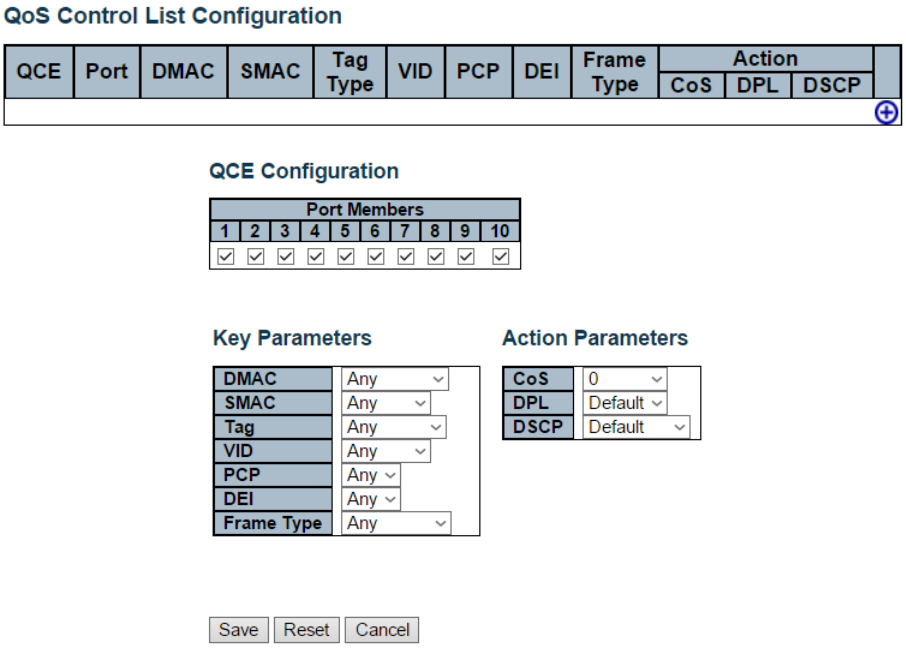
DSCP

Select the classified DSCP value (0-63).

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.19.10. QoS - QoS Control List



QoS Control List Configuration

This page shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.

Click on the lowest plus sign to add a new QCE to the list.

QCE

Indicates the QCE id.

Port

Indicates the list of ports configured with the QCE.

DMAC

Indicates the destination MAC address. Possible values are:

- **Any**: Match any DMAC.
- **Unicast**: Match unicast DMAC.
- **Multicast**: Match multicast DMAC.
- **Broadcast**: Match broadcast DMAC.

The default value is 'Any'.

SMAC

Match specific source MAC address or 'Any'.

If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

Tag Type

Indicates tag type. Possible values are:

- **Any**: Match tagged and untagged frames. This is the default setting.
- **Untagged**: Match untagged frames.
- **Tagged**: Match tagged frames.

VID

Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

PCP

Priority Code Point: Valid values of PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI

Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

Frame Type

Indicates the type of frame. Possible values are:

- **Any**: Match any frame type.
- **Ethernet**: Match EtherType frames.
- **LLC**: Match (LLC) frames.
- **SNAP**: Match (SNAP) frames.
- **IPv4**: Match IPv4 frames.
- **IPv6**: Match IPv6 frames.

Action

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

Possible actions are:

- **CoS**: Classify Class of Service.
- **DPL**: Classify Drop Precedence Level.
- **DSCP**: Classify DSCP value.

Modification Buttons

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

Add: Inserts a new QCE before the current row.

Edit: Edits the QCE.

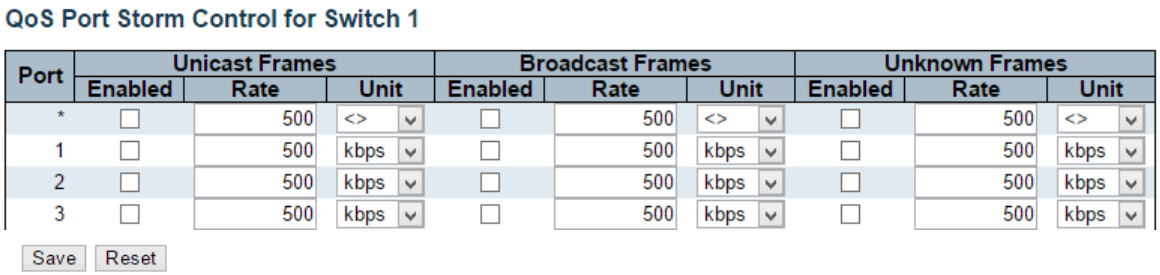
Up: Moves the QCE up the list.

Down: Moves the QCE down the list.

Delete: Deletes the QCE.

Add: The lowest plus sign adds a new entry at the bottom of the QCE listings.

3.1.19.11. QoS - Storm Control



This page allows you to configure the storm control settings for all switch ports.

There is a storm rate control for unicast frames, broadcast frames and unknown (flooded) frames.

The settings relate to the currently selected stack unit, as reflected by the page header.

Port

The port number for which the configuration below applies.

Enabled

Controls whether the storm control is enabled on this switch port.

Rate

Controls the rate for the storm control. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-13200 when the "Unit" is "Mbps" or "kfps".

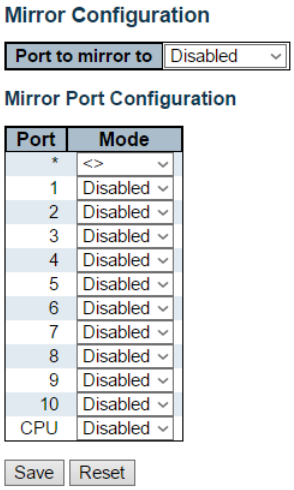
Unit

Controls the unit of measure for the storm control rate as kbps, Mbps, fps or kfps . The default value is "kbps".

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.20. Configuration - Mirroring



Configure port Mirroring on this page.

To debug network problems, selected traffic can be copied, or mirrored, on a mirror port where a frame analyzer can be attached to analyze the frame flow.

The traffic to be copied on the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

Port to mirror to

Port to mirror also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.

Mirror Port Configuration

The following table is used for Rx and Tx enabling.

Port

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

Mode

Select mirror mode.

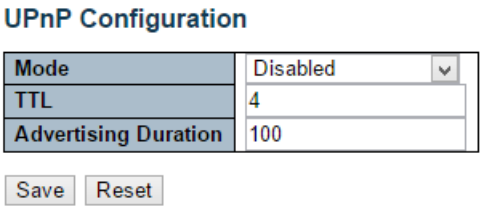
- **Rx only:** Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.
- **Tx only:** Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.
- **Disabled:** Neither frames transmitted nor frames received are mirrored.
- **Enabled:** Frames received and frames transmitted are mirrored on the mirror port.

Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror mirror port Tx frames. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

Buttons

- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

3.1.21. Configuration - UPnP



Configure UPnP on this page.

Mode

Indicates the UPnP operation mode. Possible modes are:

- **Enabled:** Enable UPnP mode operation.
- **Disabled:** Disable UPnP mode operation.

When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

TTL

The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.

Advertising Duration

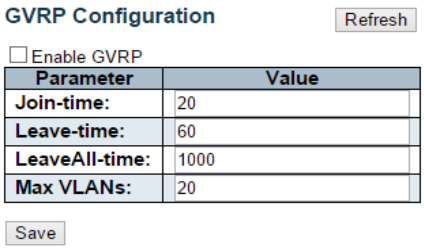
The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.22. Configuration - GVRP

3.1.22.1. GVRP - Global Config



This page allows you to configure the basic GVRP Configuration settings for all switch ports.

Enable GVRP globally

The GVRP feature is enabled by setting the check mark in the checkbox named Enable GVRP.

GVRP protocol timers

Join-time is a value in the range 1-20 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 20.

Leave-time is a value in the range 60-300 in the units of centi seconds, i.e. in units of one hundredth of a second.The default is 60.

LeaveAll-time is a value in the range 1000-5000 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 1000.

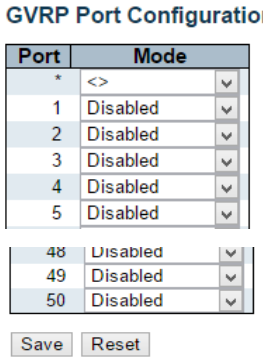
Max number of VLANs

When GVRP is enabled a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off.

Buttons

- **Save:** Click to save changes.

3.1.22.2. GVRP - Port Config

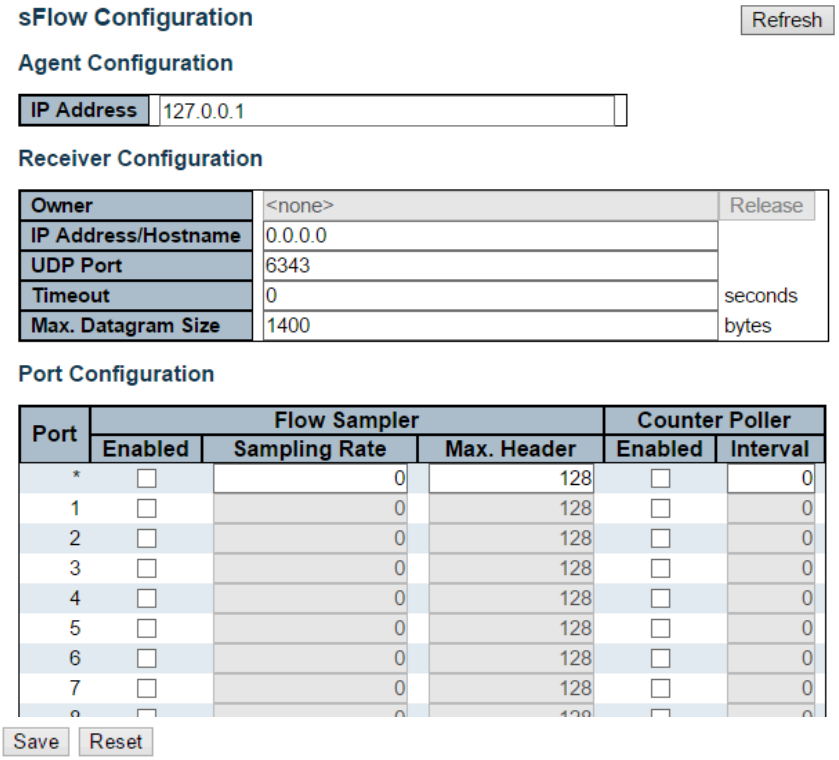


This page allows you to enable a port for GVRP.

Button

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.23. Configuration - sFlow



This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot or master change will disable sFlow sampling.

Agent Configuration

IP Address

The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time.

Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

Owner

Basically, sFlow can be configured in two ways: 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 "**Release**" 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

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.

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/disables flow sampling on this 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.

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

Enables/disables counter polling on this port.

Counter Poller Interval

With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

Buttons

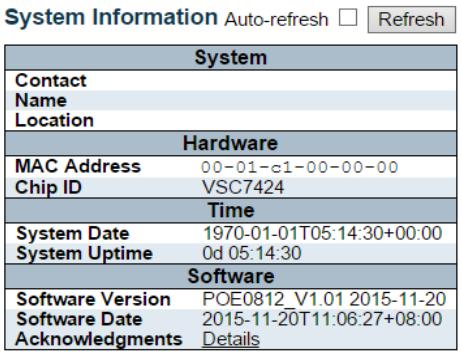
- **Release:** See description under Owner.
- **Refresh:** Click to refresh the page. Note that unsaved changes will be lost.
- **Save:** Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.2. Web Management - Monitor

You can monitor and view system status here. Also, all the settings you've made in the Configuration section of the management web page can be viewed here as well.

3.2.1. Monitor - System

3.2.1.1. System - Information



The switch system information is provided here.

Contact

The system contact configured in Configuration | System | Information | System Contact.

Name

The system name configured in Configuration | System | Information | System Name.

Location

The system location configured in Configuration | System | Information | System Location.

MAC Address

The MAC Address of this switch.

System Date

The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.

System Uptime

The period of time the device has been operational.

Switch ID

The switch ID.

Chip ID

The Chip ID of this switch.

Software Version

The software version of this switch.

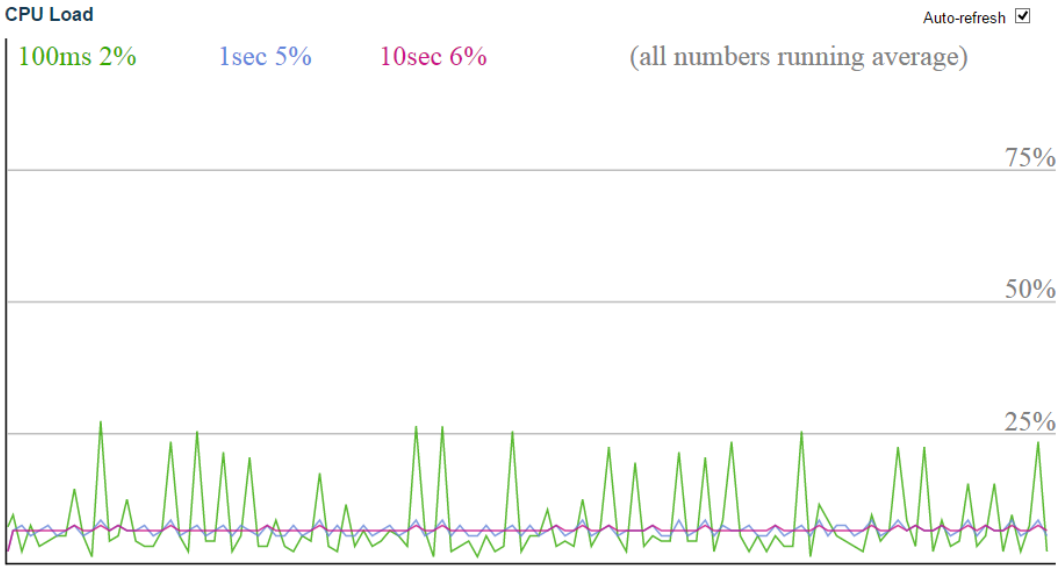
Software Date

The date when the switch software was produced.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page.

3.2.1.2. System - CPU Load



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

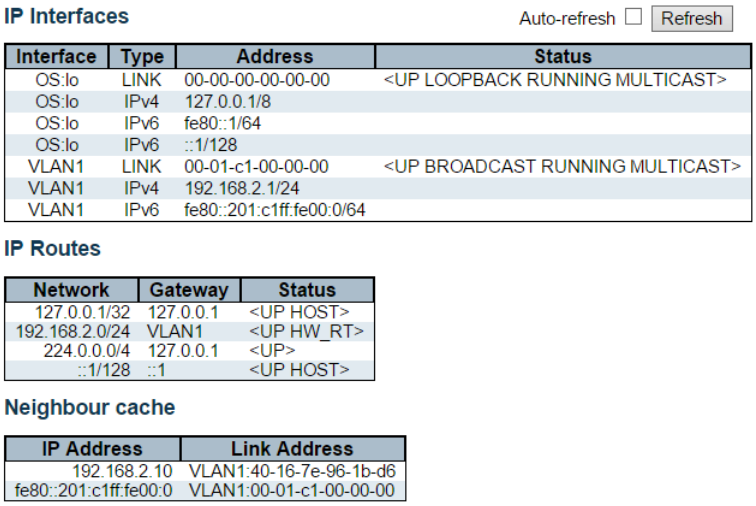
The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

3.2.1.3. System - IP Status



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::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-01-c1-00-00-00	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.2.1/24	
VLAN1	IPv6	fe80::201:c1ff:fe00:0/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
192.168.2.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.2.10	VLAN1:40-16-7e-96-1b-d6
fe80::201:c1ff:fe00:0	VLAN1:00-01-c1-00-00-00

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.

IP Interfaces

Interface

The name of the interface.

Type

The address type of the entry. This may be LINK or IPv4.

Address

The current address of the interface (of the given type).

Status

The status flags of the interface (and/or address).

IP Routes

Network

The destination IP network or host address of this route.

Gateway

The gateway address of this route.

Status

The status flags of the route.

Neighbour cache

IP Address

The IP address of the entry.

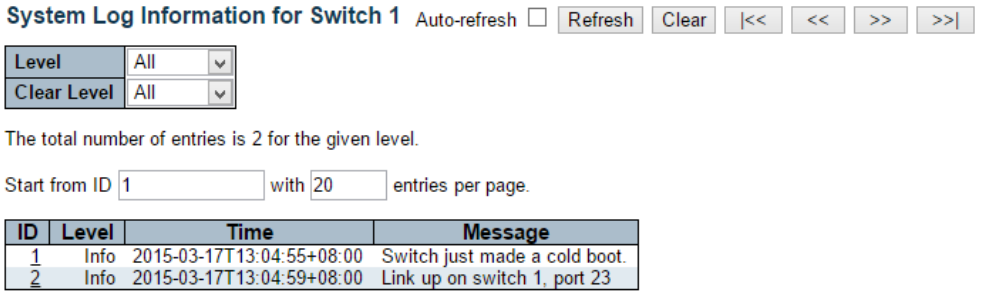
Link Address

The Link (MAC) address for which a binding to the IP address given exist..

Buttons

- **Refresh**: Click to refresh the page immediately.
- **Auto-refresh**: Check this box to refresh the page automatically.

3.2.1.4. System - Log



The switch system log information is provided here.

ID

The ID (>= 1) of the system log entry.

Level

The level of the system log entry. The following level types are supported:

- **Info:** Information level of the system log.
- **Warning:** Warning level of the system log.
- **Error:** Error level of the system log.
- **All:** All levels.

Time

The time of the system log entry.

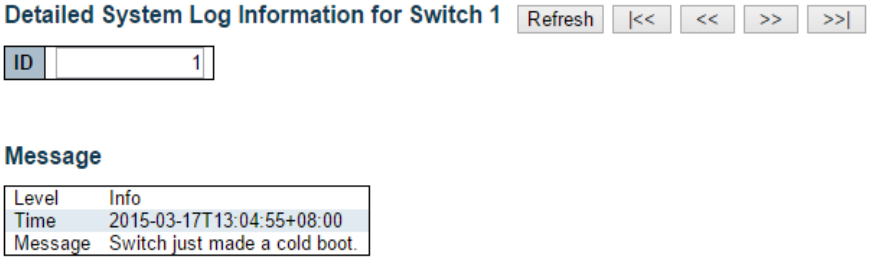
Message

The message of the system log entry.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Updates the system log entries, starting from the current entry ID.
- **Clear:** Flushes the selected log entries.
- **|<<:** Updates the system log entries, starting from the first available entry ID.
- **<<**: Updates the system log entries, ending at the last entry currently displayed.
- **>>:** Updates the system log entries, starting from the last entry currently displayed.
- **>>|:** Updates the system log entries, ending at the last available entry ID.

3.2.1.5. System - Detailed Log



The switch system detailed log information is provided here.

ID

The ID (>= 1) of the system log entry.

Message

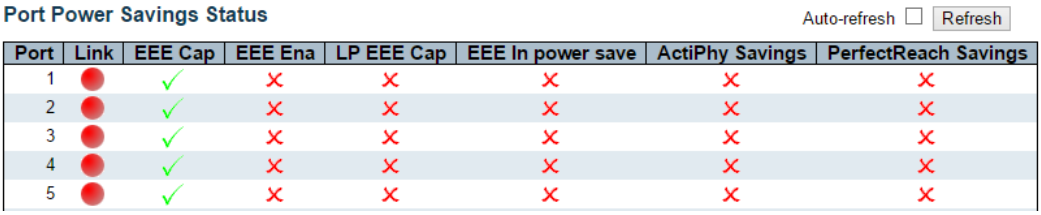
The detailed message of the system log entry.

Buttons

- **Refresh:** Updates the system log entry to the current entry ID.
- **|<<:** Updates the system log entry to the first available entry ID.
- **<<:** Updates the system log entry to the previous available entry ID.
- **>>:** Updates the system log entry to the next available entry ID.
- **>>|:** Updates the system log entry to the last available entry ID.

3.2.3. Monitor - Green Ethernet

3.2.3.1. Green Ethernet - Port Power Savings Status



This page provides the current status for EEE.

Local Port

This is the logical port number for this row.

Link

Shows if the link is up for the port (green = link up, red = link down).

EEE cap

Shows if the port is EEE capable.

EEE Ena

Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).

LP EEE cap

Shows if the link partner is EEE capable.

EEE In power save

Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec.

Actiphy Savings

Shows if the system is currently saving power due to ActiPhy.

PerfectReach Savings

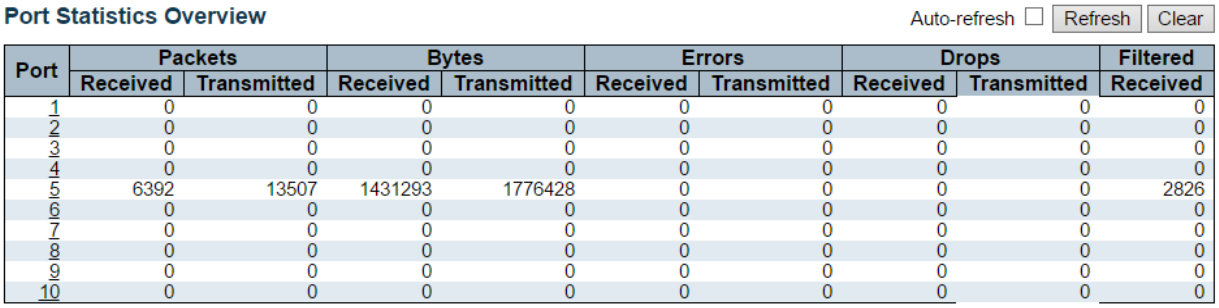
Shows if the system is currently saving power due to PerfectReach.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page.

3.2.4. Monitor - Ports

3.2.4.1. Ports - Traffic Overview



Port Statistics Overview

Auto-refresh ☐ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	6392	13507	1431293	1776428	0	0	0	0	2826
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0

This page provides an overview of general traffic statistics for all switch ports.

The ports belong to the currently selected stack unit, as reflected by the page header.

Port

The logical port for the settings 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.

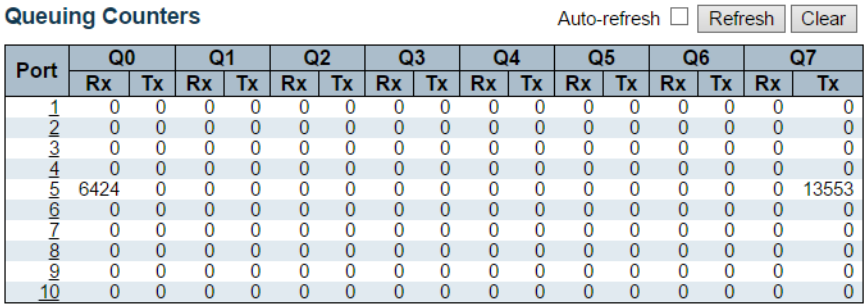
Filtered

The number of received frames filtered by the forwarding process.

Buttons

- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clears the counters for all ports.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

3.2.4.2. Ports - QoS Statistics



Queuing Counters

Auto-refresh ☐ Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	6424	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13553
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

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

The ports belong to the currently selected stack unit, as reflected by the page header.

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.

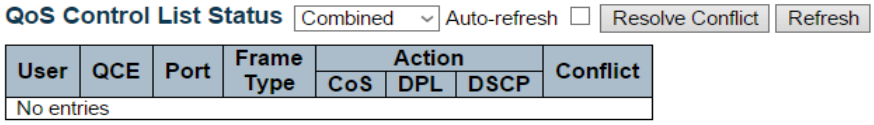
Rx/Tx

The number of received and transmitted packets per queue.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clears the counters for all ports.

3.2.4.3. Ports - QCL Status



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

User

Indicates the QCL user.

QCE

Indicates the QCE id.

Port

Indicates the list of ports configured with the QCE.

Frame Type

Indicates the type of frame. Possible values are:

- **Any**: Match any frame type.
- **Ethernet**: Match EtherType frames.
- **LLC**: Match (LLC) frames.
- **SNAP**: Match (SNAP) frames.
- **IPv4**: Match IPv4 frames.
- **IPv6**: Match IPv6 frames.

Action

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

Possible actions are:

- **CoS**: Classify Class of Service.
- **DPL**: Classify Drop Precedence Level.
- **DSCP**: Classify DSCP value.

Conflict

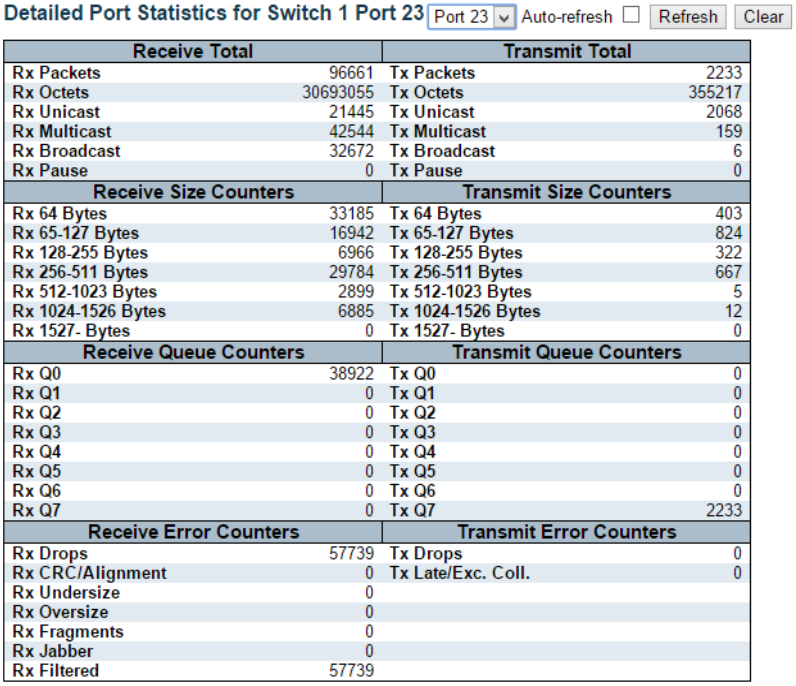
Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

Buttons

- 

: Select the QCL status from this drop down list.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Resolve Conflict:** Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.
- **Refresh** : Click to refresh the page.

3.2.4.4. Ports - Detailed Statistics



Detailed Port Statistics for Switch 1 Port 23 Port 23 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	96661	Tx Packets	2233
Rx Octets	30693055	Tx Octets	355217
Rx Unicast	21445	Tx Unicast	2068
Rx Multicast	42544	Tx Multicast	159
Rx Broadcast	32672	Tx Broadcast	6
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	33185	Tx 64 Bytes	403
Rx 65-127 Bytes	16942	Tx 65-127 Bytes	824
Rx 128-255 Bytes	6966	Tx 128-255 Bytes	322
Rx 256-511 Bytes	29784	Tx 256-511 Bytes	667
Rx 512-1023 Bytes	2899	Tx 512-1023 Bytes	5
Rx 1024-1526 Bytes	6885	Tx 1024-1526 Bytes	12
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	38922	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	2233
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	57739	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	57739		

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The selected port belongs to the currently selected stack unit, as reflected by the page header.

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.

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 operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

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.

Note 1: Short frames are frames that are smaller than 64 bytes.

Note 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.

Buttons

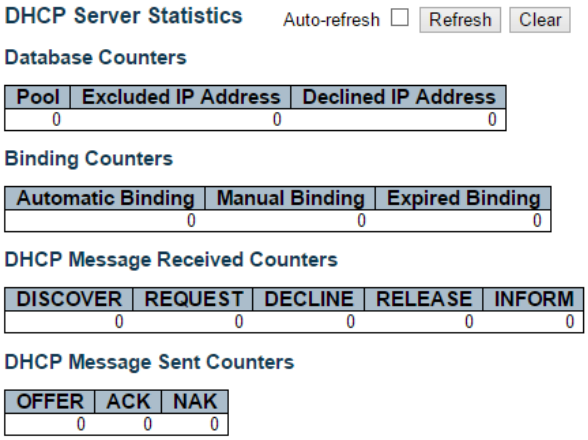
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clears the counters for the selected port.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Note: The port select box determines which port is affected by clicking the buttons.

3.2.5. Monitor - DHCP

3.2.5.1. DHCP - Server

3.2.5.1.1. DHCP - Server - Statistics



This page displays the database counters and the number of DHCP messages sent and received by DHCP server.

Database Counters

Display counters of various databases.

Pool

Number of pools.

Excluded IP Address

Number of excluded IP address ranges.

Declined IP Address

Number of seclined IP addresses.

Binding Counters

Display counters of various databases.

Automatic Binding

Number of bindings with network-type pools.

Manual Binding

Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.

Expired Binding

Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP Message Received Counters

Display counters of DHCP messages received by DHCP server.

DISCOVER

Number of DHCP DISCOVER messages received.

REQUEST

Number of DHCP REQUEST messages received.

DECLINE

Number of DHCP DECLINE messages received.

RELEASE

Number of DHCP RELEASE messages received.

INFORM

Number of DHCP INFORM messages received.

DHCP Message Sent Counters

Display counters of DHCP messages sent by DHCP server.

OFFER

Number of DHCP OFFER messages sent.

ACK

Number of DHCP ACK messages sent.

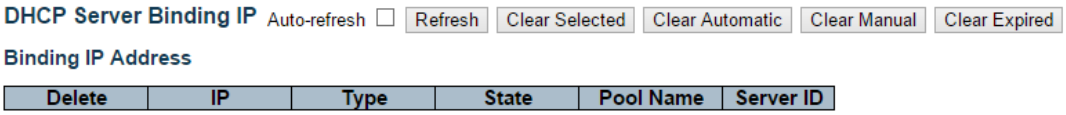
NAK

Number of DHCP NAK messages sent.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Click to Clears DHCP Message Received Counters and DHCP Message Sent Counters.

3.2.5.1.2. DHCP - Server - Binding



This page displays bindings generated for DHCP clients.

Binding IP Address

Display all bindings.

IP

IP address allocated to DHCP client.

Type

Type of binding. Possible types are Automatic, Manual, Expired.

State

State of binding. Possible states are Committed, Allocated, Expired.

Pool Name

The pool that generates the binding.

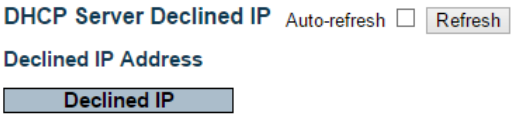
Server ID

Server IP address to service the binding.

Buttons

- **Refresh:** Click to refresh the page immediately.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Clear Selected:** Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.
- **Clear Automatic:** Click to clear all Automatic bindings and Change them to Expired bindings.
- **Clear Manual:** Click to clear all Manual bindings and Change them to Expired bindings.
- **Clear Expired:** Click to clear all Expired bindings and free them.

3.2.5.1.3. DHCP - Server - Declined IP



This page displays declined IP addresses.

Declined IP Addresses

Display IP addresses declined by DHCP clients.

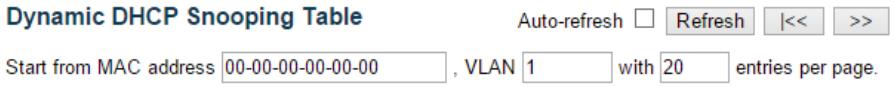
Declined IP

List of IP addresses declined.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.

3.2.5.2. DHCP - Snooping Table



This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

Navigating the DHCP snooping Table

Each page shows up to 99 entries from the Dynamic DHCP snooping table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic DHCP snooping Table.

The "MAC address" and "VLAN" input fields allows the user to select the starting point in the Dynamic DHCP snooping Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic DHCP snooping Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

DHCP snooping Table Columns

MAC Address

User MAC address of the entry.

VLAN ID

VLAN-ID in which the DHCP traffic is permitted.

Source Port

Switch Port Number for which the entries are displayed.

IP Address

User IP address of the entry.

IP Subnet Mask

User IP subnet mask of the entry.

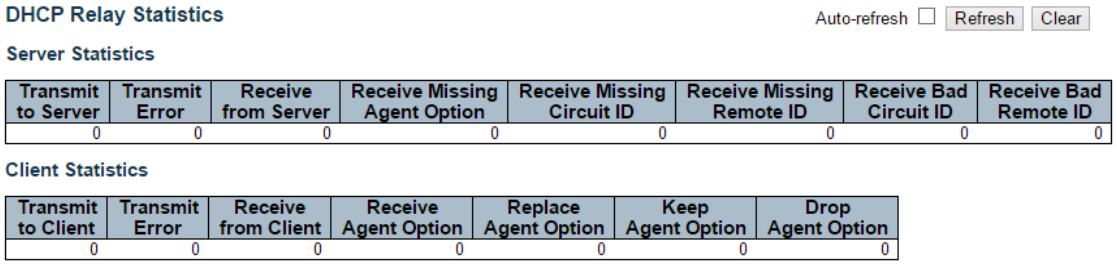
DHCP Server Address

DHCP Server address of the entry.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **Clear:** Flushes all dynamic entries.
- **|<<:** Updates the table starting from the first entry in the Dynamic DHCP snooping Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.5.3. DHCP - Relay Statistics


DHCP Relay Statistics

Auto-refresh ☐ Refresh Clear

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

This page provides statistics for DHCP relay.

Server 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 Server

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.

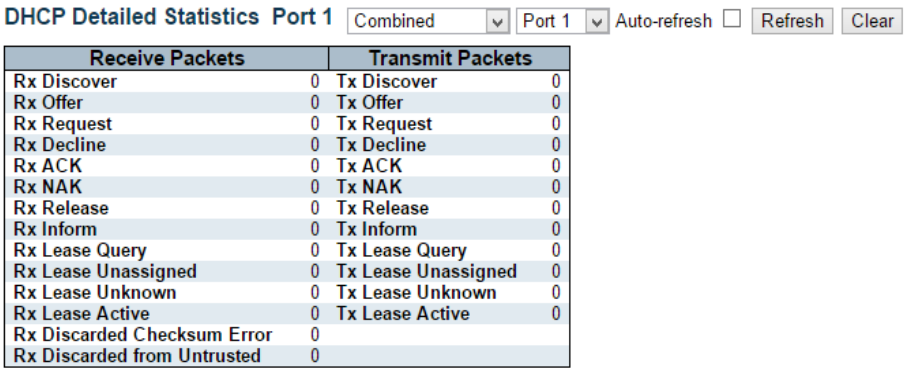
Drop Agent Option

The number of packets that were dropped which were received with relay agent information.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clear all statistics.

3.2.5.4. DHCP - Detailed Statistics



This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

Receive and Transmit Packets

Rx and Tx Discover

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

Rx and Tx Offer

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

Rx and Tx Request

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

Rx and Tx Decline

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

Rx and Tx ACK

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

Rx and Tx NAK

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

Rx and Tx Release

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

Rx and Tx Inform

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

Rx and Tx Lease Query

The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned

The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown

The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active

The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error

The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted

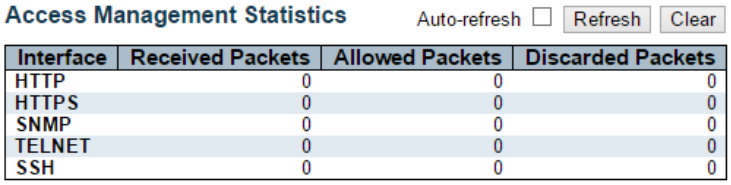
The number of discarded packet that are coming from untrusted port.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clears the counters for the selected port.

3.2.6. Monitor - Security

3.2.6.1. Security - Access Management Statistics



This page provides statistics for access management.

Interface

The interface type through which the remote host can access the switch.

Received Packets

Number of received packets from the interface when access management mode is enabled.

Allowed Packets

Number of allowed packets from the interface when access management mode is enabled.

Discarded Packets

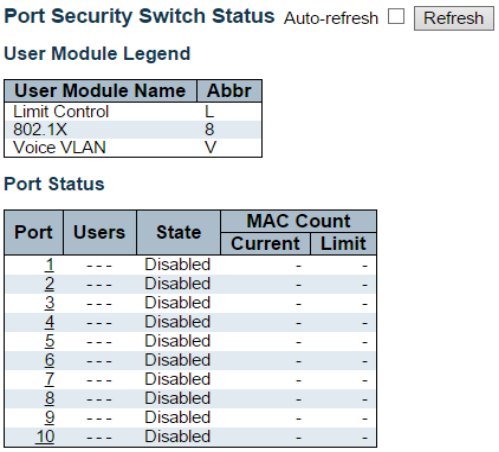
Number of discarded packets from the interface when access management mode is enabled.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clear all statistics.

3.2.6.2. Security - Network

3.2.6.2.1. Security - Network - Port Security - Switch



Port Security Switch Status Auto-refresh ☐ Refresh

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	---	Disabled	-	-
5	---	Disabled	-	-
6	---	Disabled	-	-
7	---	Disabled	-	-
8	---	Disabled	-	-
9	---	Disabled	-	-
10	---	Disabled	-	-

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules- the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

User Module Legend

The legend shows all user modules that may request Port Security services.

User Module Name

The full name of a module that may request Port Security services.

Abbr

A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

Port Status

The table has one row for each port on the selected switch in the stack and a number of columns.

Port

The port number for which the status applies. Click the port number to see the status for this particular port.

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 (see Abbr) has enabled port security.

State

Shows the current state of the port. It can take one of four values:

- **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 Web-page.

MAC Count (Current, Limit)

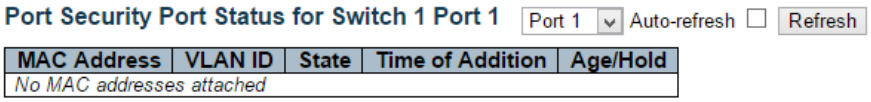
The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

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 (-).

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.

3.2.6.2.2. Security - Network - Port Security - Port



This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

MAC Address & VLAN ID

The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

State

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

Time of Addition

Shows the date and time when this MAC address was first seen on the port.

Age/Hold

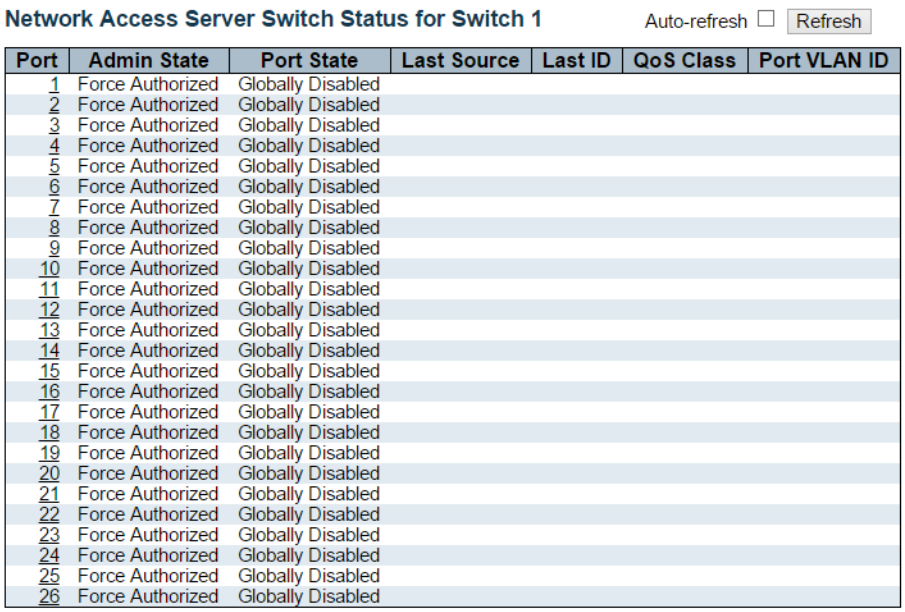
If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this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

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.

3.2.6.2.3. Security - Network - NAS - Switch



Network Access Server Switch Status for Switch 1 Auto-refresh Refresh

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled				
2	Force Authorized	Globally Disabled				
3	Force Authorized	Globally Disabled				
4	Force Authorized	Globally Disabled				
5	Force Authorized	Globally Disabled				
6	Force Authorized	Globally Disabled				
7	Force Authorized	Globally Disabled				
8	Force Authorized	Globally Disabled				
9	Force Authorized	Globally Disabled				
10	Force Authorized	Globally Disabled				
11	Force Authorized	Globally Disabled				
12	Force Authorized	Globally Disabled				
13	Force Authorized	Globally Disabled				
14	Force Authorized	Globally Disabled				
15	Force Authorized	Globally Disabled				
16	Force Authorized	Globally Disabled				
17	Force Authorized	Globally Disabled				
18	Force Authorized	Globally Disabled				
19	Force Authorized	Globally Disabled				
20	Force Authorized	Globally Disabled				
21	Force Authorized	Globally Disabled				
22	Force Authorized	Globally Disabled				
23	Force Authorized	Globally Disabled				
24	Force Authorized	Globally Disabled				
25	Force Authorized	Globally Disabled				
26	Force Authorized	Globally Disabled				

This page provides an overview of the current NAS port states for the selected switch.

Port

The switch port number. Click to navigate to detailed NAS statistics for this port.

Admin State

The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State

The current state of the port. Refer to NAS Port State for a description of the individual states.

Last Source

The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID

The user name (supplicant identity) carried in themost recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class

QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID

The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

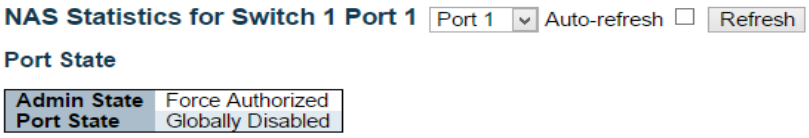
If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.

3.2.6.2.5. Security - Network - NAS - Port



This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics only.

Use the port select box to select which port details to be displayed. The selected port belongs to the currently selected stack unit as reflected by the table header.

Port State

Admin State

The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port State

The current state of the port. Refer to NAS Port State for a description of the individual states.

QoS Class

The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID

The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Port Counters

EAPOL Counters

These supplicant frame counters are available for the following administrative states:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

EAPOL Counters			
Direction	**Name**	**IEEE Name**	**Description**
Rx	**Total**	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	**Response ID**	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	**Responses**	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	**Start**	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	**Logoff**	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	**Invalid Type**	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	**Invalid Length**	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	**Total**	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	**Request ID**	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	**Requests**	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

Backend Server Counters

These backend (RADIUS) frame counters are available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Backend Server Counters			
Direction	**Name**	**IEEE Name**	**Description**
Rx	**Access Challenges**	dot1xAuthBackendAccessChallenges	**802.1X-based**: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. **MAC-based**: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
Rx	**Other Requests**	dot1xAuthBackendOtherRequestsToSupplicant	**802.1X-based**: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. **MAC-based**: Not applicable.
Rx	**Auth. Successes**	dot1xAuthBackendAuthSuccesses	**802.1X- and MAC-based**: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
Rx	**Auth. Failures**	dot1xAuthBackendAuthFails	**802.1X- and MAC-based**: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
Tx	**Responses**	dot1xAuthBackendResponses	**802.1X-based:** Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. **MAC-based:** Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

Last Supplicant/Client Info

Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Last Supplicant/Client Info		
Name	**IEEE Name**	**Description**
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	**802.1X-based**: The protocol version number carried in the most recently received EAPOL frame. **MAC-based**: Not applicable.
Identity	-	**802.1X-based**: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. **MAC-based**: Not applicable.

Selected Counters

Selected Counters

The Selected Counters table is visible when the port is in one of the following administrative states:

- Multi 802.1X
- MAC-based Auth.

The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

Attached MAC Addresses

Identity

Shows the identity of the supplicant, as received in the Response Identity EAPOL frame.

Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached.

This column is not available for MAC-based Auth.

MAC Address

For Multi 802.1X, this column holds the MAC address of the attached supplicant.

For MAC-based Auth., this column holds the MAC address of the attached client.

Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.

VLAN ID

This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

State

The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

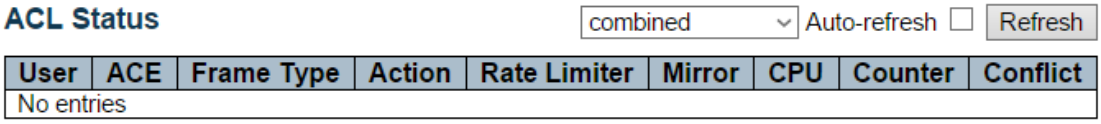
Last Authentication

Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** This button is available in the following modes:
  - Force Authorized
  - Force Unauthorized
  - Port-based 802.1X
  - Single 802.1X
- **Clear:** Click to clear the counters for the selected port.
- **Clear All:** This button is available in the following modes:
  - Multi 802.1X
  - MAC-based Auth.X
- **Clear This:** Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however. This button is available in the following modes:
  - Multi 802.1X
  - MAC-based Auth.X

3.2.6.2.6. Security - Network - 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 512 on each switch.

User

Indicates the ACL user.

ACE

Indicates the ACE ID on local switch.

Frame Type

Indicates 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

Indicates the forwarding action of the ACE.

- **Permit:** Frames matching the ACE may be forwarded and learned.
- **Deny:** Frames matching the ACE are dropped.

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.

CPU

Forward packet that matched the specific ACE to CPU.

Counter

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

Conflict

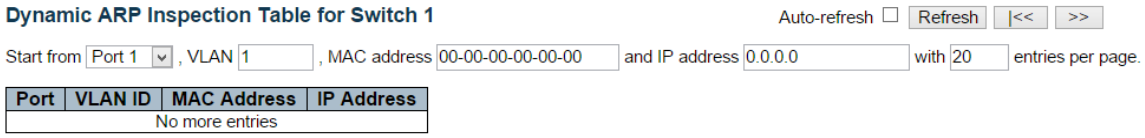
Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

The select box determines which ACL user is affected by clicking the buttons.

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page.

3.2.6.2.7. Security - Network - ARP Inspection



Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The “<<” button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “>>|” button to start over.

ARP Inspection Table Columns

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the ARP traffic is permitted.

MAC Address

User MAC address of the entry.

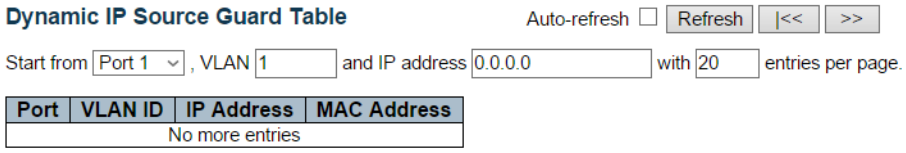
IP Address

User IP address of the entry.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **Clear:** Flushes all dynamic entries.
- **|<<:** Updates the table starting from the first entry in the Dynamic ARP Inspection Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.6.2.8. Security - Network - IP Source Guard



Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

Navigating the IP Source Guard Table

Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table.

The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the IP traffic is permitted.

IP Address

User IP address of the entry.

MAC Address

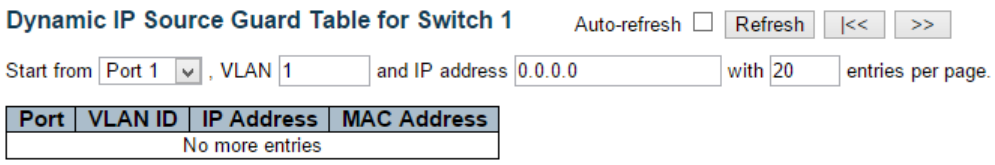
Source MAC address.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh**: Refreshes the displayed table starting from the input fields.
- **Clear**: Flushes all dynamic entries.
- << : Updates the table starting from the first entry in the Dynamic IP Source Guard Table.
- >> : Updates the table, starting with the entry after the last entry currently displayed.

3.2.6.2.10. Security - Network - IP Source Guard



Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

Navigating the IP Source Guard Table

Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table.

The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

IP Source Guard Table Columns

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the IP traffic is permitted.

IP Address

User IP address of the entry.

MAC Address

Source MAC address.

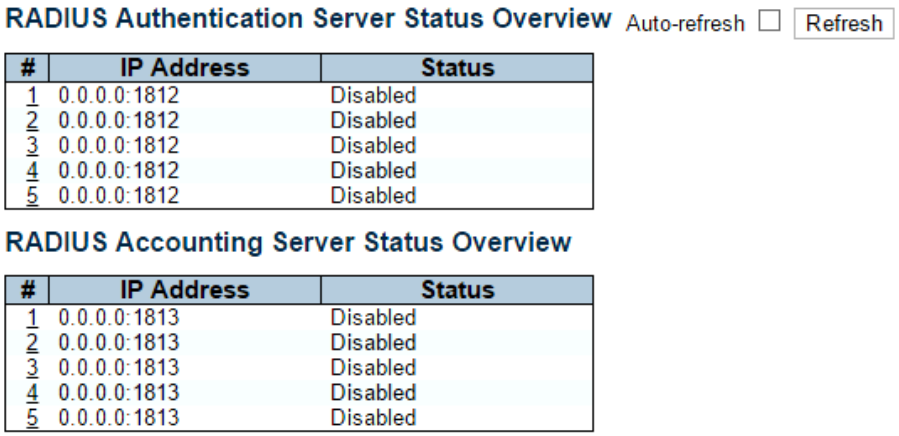
Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.

- **Clear:** Flushes all dynamic entries.
- **|<<:** Updates the table starting from the first entry in the Dynamic IP Source Guard Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.6.3. Security - AAA

3.2.6.3.1. Security - AAA - RADIUS Overview



RADIUS Authentication Server Status Overview Auto-refresh Refresh

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

RADIUS Authentication Servers

#

The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address

The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

Status

The current status of the server. This field takes one of the following values:

- **Disabled:** The server is disabled.
- **Not Ready:** The server is enabled, but IP communication is not yet up and running.
- **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
- **Dead (X seconds left):** Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Servers

#

The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address

The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

Status

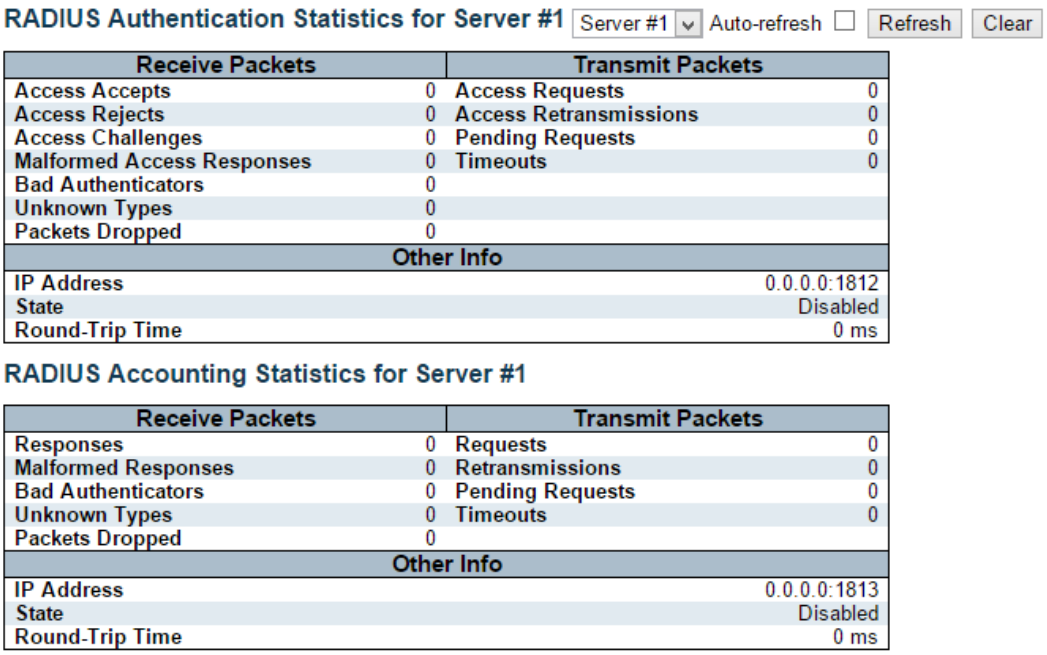
The current status of the server. This field takes one of the following values:

- **Disabled:** The server is disabled.
- **Not Ready:** The server is enabled, but IP communication is not yet up and running.
- **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept 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.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.

3.2.6.3.2. Security - AAA - RADIUS Details



RADIUS Authentication Statistics for Server #1 Server #1 Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:1812
State			Disabled
Round-Trip Time			0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:1813
State			Disabled
Round-Trip Time			0 ms

This page provides detailed statistics for a particular RADIUS server.

RADIUS Authentication Statistics

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	**Access Accepts**	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	**Access Rejects**	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	**Access Challenges**	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	**Malformed Access Responses**	radiusAuthClientExtMalformedAccessResponses	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.
Rx	**Bad Authenticators**	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	**Unknown Types**	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	**Packets Dropped**	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	**Access Requests**	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	**Access Retransmissions**	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	**Pending Requests**	radiusAuthClientExtPendingRequests	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.
Tx	**Timeouts**	radiusAuthClientExtTimeouts	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.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
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	radiusAuthClientExtRoundTripTime	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

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB.

Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	radiusAccClientExtMalformedResponses	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.
Rx	Bad Authenticators	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	Pending Requests	radiusAccClientExtPendingRequests	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.
Tx	Timeouts	radiusAccClientExtTimeouts	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.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4670 Name	Description
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	radiusAccClientExtRoundTripTime	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.

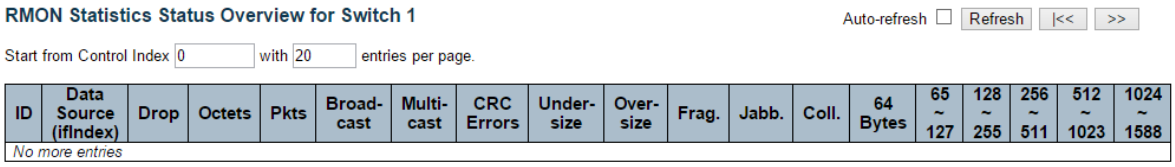
Buttons

The server select box determines which server is affected by clicking the buttons.

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

3.2.6.4. Security - Switch - RMON

3.2.6.4.1. Security - Switch - RMON - Statistics



This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" allows the user to select the starting point in the Statistics table. Clicking the Refresh button will update the displayed table starting from that or the next closest Statistics table match.

The >> button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

ID

Indicates the index of Statistics entry.

Data Source(ifIndex)

The port ID which wants to be monitored.

Drop

The total number of events in which packets were dropped by the probe due to lack of resources.

Octets

The total number of octets of data (including those in bad packets) received on the network.

Pkts

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broad-cast

The total number of good packets received that were directed to the broadcast address.

Multi-cast

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, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under-size

The total number of packets received that were less than 64 octets.

Over-size

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

The total number of packets (including bad packets) received that were 64 octets in length.

65~127

The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

128~255

The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

256~511

The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

512~1023

The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

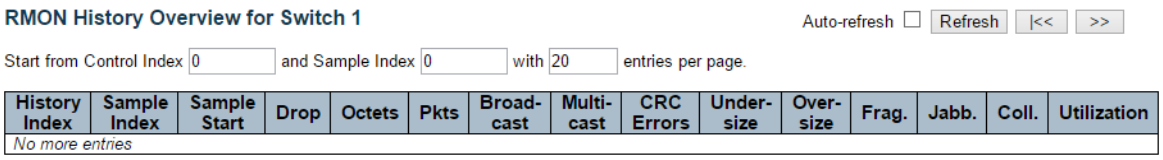
1024~1588

The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **|<<:** Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.6.4.2. Security - Switch - RMON - History



This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

The "Start from History Index and Sample Index" allows the user to select the starting point in the History table. Clicking the Refresh button will update the displayed table starting from that or the next closest History table match.

The “>>” will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

History Index

Indicates the index of History control entry.

Sample Index

Indicates the index of the data entry associated with the control entry.

Sample Start

The value of sysUpTime at the start of the interval over which this sample was measured.

Drop

The total number of events in which packets were dropped by the probe due to lack of resources.

Octets

The total number of octets of data (including those in bad packets) received on the network.

Pkts

The total number of packets (including bad packets, broadcast packets, and multicast 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.

CRCErrors

The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

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.

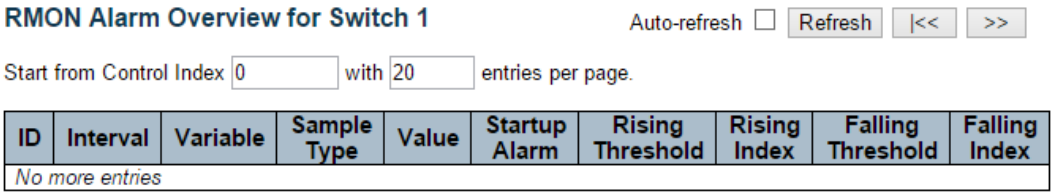
Utilization

The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **|<<:** Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.6.4.3. Security - Switch - RMON - Alarm



This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the Refresh button will update the displayed table starting from that or the next closest Alarm table match.

The “>>” will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

ID

Indicates the index of Alarm control entry.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable

Indicates the particular variable 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 sent when this entry is first set to valid.

Rising Threshold

Rising threshold value.

Rising Index

Rising event index.

Falling Threshold

Falling threshold value.

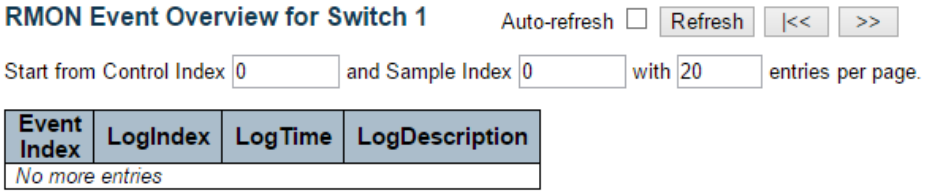
Falling Index

Falling event index.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **|<<:** Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.6.4.4. Security - Switch - RMON - Events



This page provides an overview of RMON Event table entries.Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table table.

The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the Refresh button will update the displayed table starting from that or the next closest Event table match.

The “>>” will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "Nomore entries" is shown in the displayed table. Use the “|<<” button to start over.

Event Index

Indicates the index of the event entry.

Log Index

Indicates the index of the log entry.

LogTIme

Indicates Event log time

LogDescription

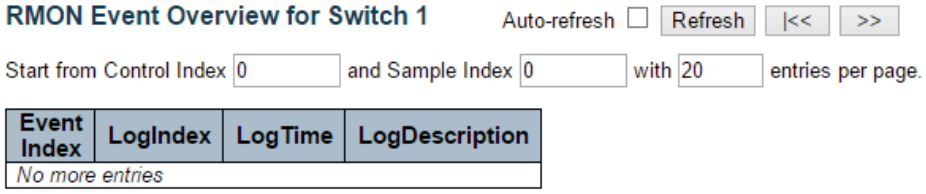
Indicates the Event description.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **|<<:** Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.7. Monitor - LACP

3.2.7.1. LACP - System Status



This page provides a status overview for all LACP instances.

Aggr ID

The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'

Partner System ID

The system ID (MAC address) of the aggregation partner.

Partner Key

The Key that the partner has assigned to this aggregation ID.

Last changed

The time since this aggregation changed.

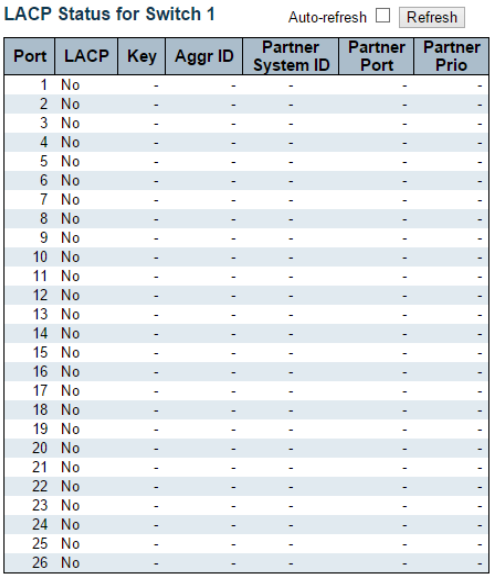
Local Ports

Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port".

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page.

3.2.7.2. LACP - Port Status


LACP Status for Switch 1 Auto-refresh Refresh

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-
11	No	-	-	-	-	-
12	No	-	-	-	-	-
13	No	-	-	-	-	-
14	No	-	-	-	-	-
15	No	-	-	-	-	-
16	No	-	-	-	-	-
17	No	-	-	-	-	-
18	No	-	-	-	-	-
19	No	-	-	-	-	-
20	No	-	-	-	-	-
21	No	-	-	-	-	-
22	No	-	-	-	-	-
23	No	-	-	-	-	-
24	No	-	-	-	-	-
25	No	-	-	-	-	-
26	No	-	-	-	-	-

This page provides a status overview for LACP status for all ports.

Port

The switch port number.

LACP

'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.

Key

The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID

The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.

Partner System ID

The partner's System ID (MAC address).

Partner Port

The partner's port number connected to this port.

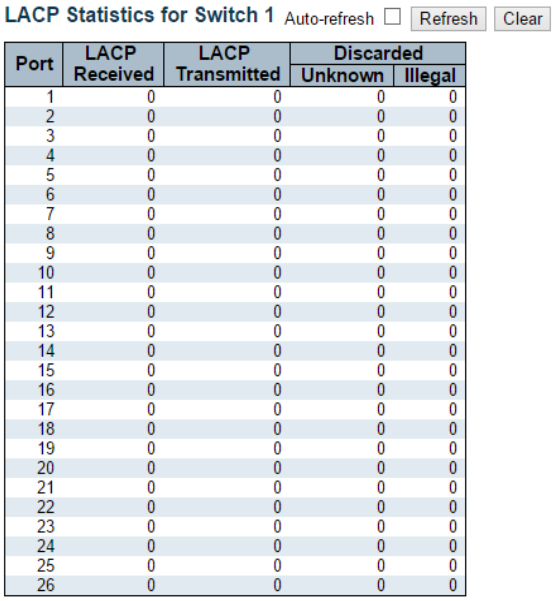
Partner Prio

The partner's port priority.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page.

3.2.7.3. LACP - Port Statistics



Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0

This page provides an overview for LACP statistics for all ports.

Port

The switch port number.

LACP Received

Shows how many LACP frames have been received at each port.

LACP Transmitted

Shows how many LACP frames have been sent from each port.

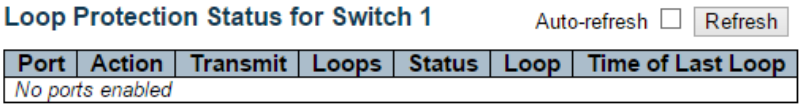
Discarded

Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clears the counters for all ports.

3.2.8. Monitor - Loop Protection



This page displays the loop protection port status the ports of the currently selected switch.

Port

The switch port number of the logical port.

Action

The currently configured port action.

Transmit

The currently configured port transmit mode.

Loops

The number of loops detected on this port.

Status

The current loop protection status of the port.

Loop

Whether a loop is currently detected on the port.

Time of Last Loop

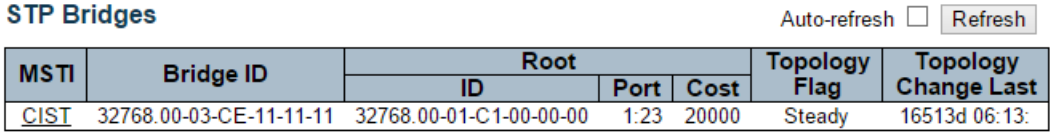
The time of the last loop event detected.

Buttons

- **Refresh:** Click to refresh the page immediately.
- **Auto-refresh:** Check this box to enable an automatic refresh of the page at regular intervals.

3.2.9. Monitor - Spanning Tree

3.2.9.1. Spanning Tree - Bridge Status



This page provides a status overview of all STP bridge instances.

The displayed table contains a row for each STP bridge instance, where the column displays the following information:

MSTI

The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID

The Bridge ID of this Bridge instance.

Root ID

The Bridge ID of the currently elected root bridge.

Root Port

The switch port currently assigned the root port role.

Root Cost

Root Path Cost. For the Root Bridge it 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 Flag of this Bridge instance.

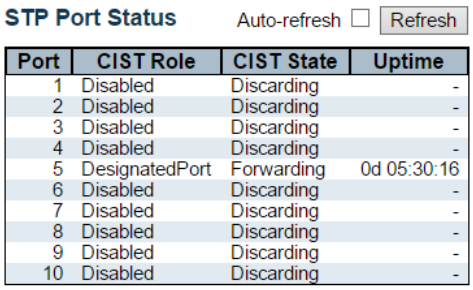
Topology Change Last

The time since last Topology Change occurred.

Buttons

- **Refresh:** Click to refresh the page immediately.
- **Auto-refresh:** Check this box to enable an automatic refresh of the page at regular intervals.

3.2.9.2. Spanning Tree - Port Status



This page displays the STP CIST port status for physical ports of the switch.

Port

The switch port number of the logical STP port.

CIST Role

The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort Disabled.

CIST State

The current STP port state of the CIST port. The port state can be one of the following values: Discarding Learning Forwarding.

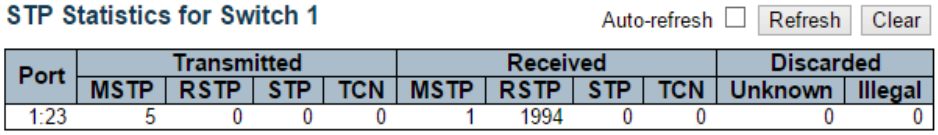
Uptime

The time since the bridge port was last initialized.

Buttons

- **Refresh**: Click to refresh the page immediately.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

3.2.9.3. Spanning Tree - Port Statistics



Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1:23	5	0	0	0	1	1994	0	0	0	0

This page displays the STP port statistics counters of bridge ports in the currently selected switch.

Port

The switch port number of the logical STP port.

MSTP

The number of MSTP BPDU's received/transmitted on the port.

RSTP

The number of RSTP BPDU's received/transmitted on the port.

STP

The number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN

The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

Discarded Unknown

The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Discarded Illegal

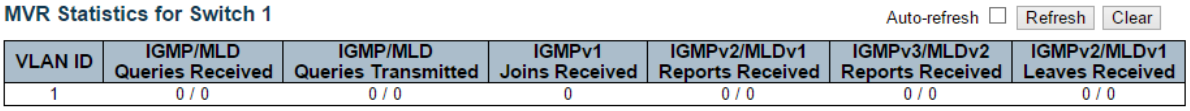
The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons

- **Refresh:** Click to refresh the page immediately.
- **Clear:** Click to reset the counters.
- **Auto-refresh:** Check this box to enable an automatic refresh of the page at regular intervals.

3.2.10. Monitor - MVR

3.2.10.1. MVR - Statistics



This page provides MVR Statistics information.

The statistics is related to the currently selecting stack unit, as reflected by the page header.

VLAN ID

The Multicast VLAN ID.

IGMP/MLD Queries Received

The number of Received Queries for IGMP and MLD, respectively.

IGMP/MLD Queries Transmitted

The number of Transmitted Queries for IGMP and MLD, respectively.

IGMPv1 Joins Received

The number of Received IGMPv1 Join's.

IGMPv2/MLDv1 Report's Received

The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

IGMPv3/MLDv2 Report's Received

The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.

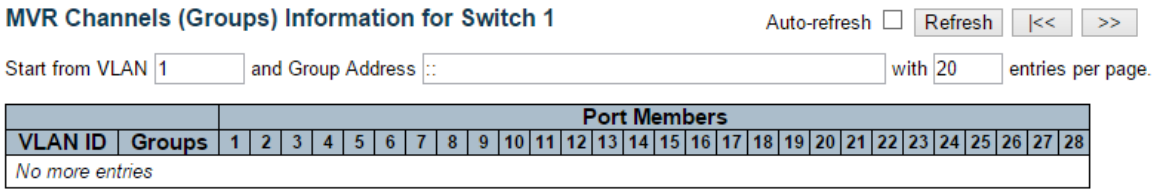
IGMPv2/MLDv1 Leave's Received

The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Buttons

- **Auto-refresh:** Check this box to enable an automatic refresh of the page at regular intervals.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clears all Statistics counters.

3.2.10.2. MVR - MVR Channel Groups



Entries in the MVR Channels (Groups) Information Table are shown on this page. The MVR Channels (Groups) Information Table is sorted first by VLAN ID, and then by group.

Navigating the MVR Channels (Groups) Information Table

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The “>>” will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

MVR Channels (Groups) Information Table Columns

VLAN ID

VLAN ID of the group.

Groups

Group ID of the group displayed.

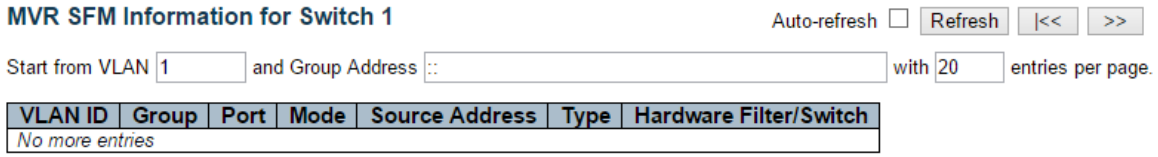
Port Members

Ports under this group.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.10.3. MVR - MVR SFM Information



Entries in the MVR SFM Information Table are shown on this page. The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Navigating the MVR SFM Information Table

Each page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MVR SFM Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The “>>” will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

MVR SFM Information Table Columns

VLAN ID
VLAN ID of the group.

Group
Group address of the group displayed.

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
IP Address of the source. Currently, system limits the total number of IP source addresses for

filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.

Type

Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

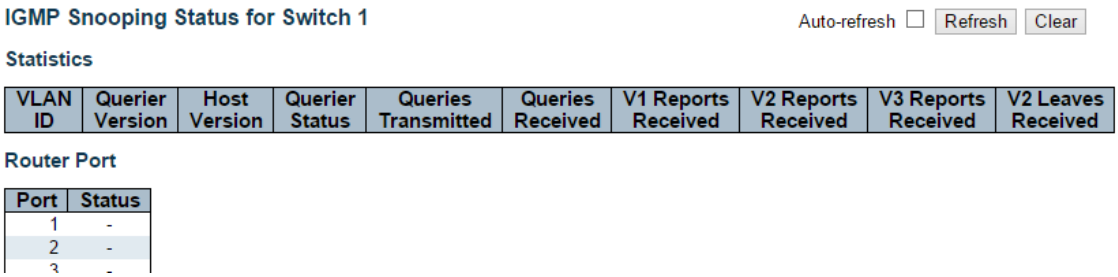
Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table starting from the first entry in the MVR SFM Information Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed

3.2.11. Monitor - IPMC

3.2.11.1. IPMC - IGMP Snooping

3.2.11.1.1. IPMC - IGMP Snooping - Status



This page provides IGMP Snooping status.

The status related to the currently selected stack unit, as reflected by the page header.

VLAN ID

The VLAN ID of the entry.

Querier Version

Working Querier Version currently.

Host Version

Working Host Version currently.

Querier Status

Shows the Querier status is "ACTIVE" or "IDLE".

"DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

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

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port

Switch port number.

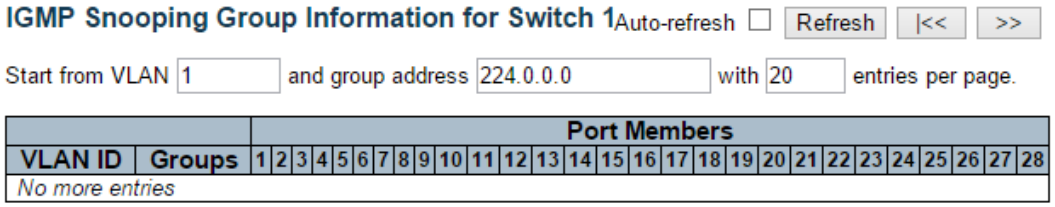
Status

Indicate whether specific port is a router port or not.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clears all Statistics counters.

3.2.11.1.2. IPMC - IGMP Snooping - Groups Information



Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.

Navigating the IGMP Group Table

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the Refresh button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, thetwo input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

IGMP Group Table Columns

VLAN ID
VLAN ID of the group.

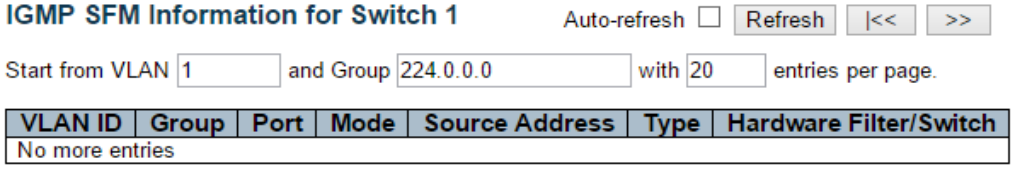
Groups
Group address of the group displayed.

Port Members
Ports under this group.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table, starting with the first entry in the IGMP Group Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.11.1.3. IPMC - IGMP Snooping - IPv4 SFM Information



Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Navigating the IGMP SFM Information Table

Each page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The “>>” will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

IGMP SFM Information Table Columns

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

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

IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type

Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

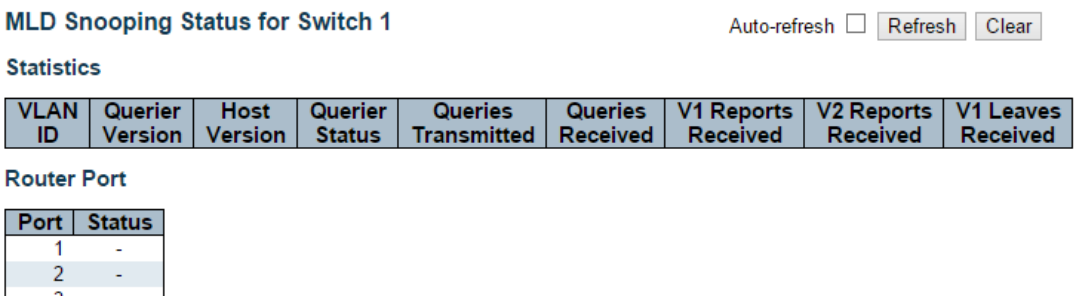
Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table starting from the first entry in the IGMP SFM Information Table
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.11.2. IPMC - MLD Snooping

3.2.11.2.1. IPMC - MLD Snooping - Status



This page provides MLD Snooping status.

The status related to the currently selected stack unit, as reflected by the page header.

VLAN ID

The VLAN ID of the entry.

Querier Version

Working Querier Version currently.

Host Version

Working Host Version currently.

Querier Status

Shows the Querier status is "ACTIVE" or "IDLE".

"DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V1 Leaves Received

The number of Received V1 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port

Switch port number.

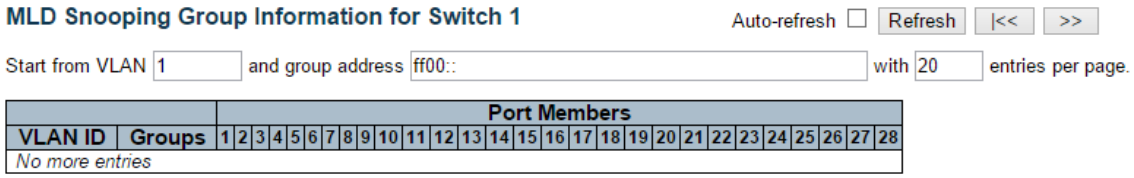
Status

Indicate whether specific port is a router port or not.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clears all Statistics counters.

3.2.11.2.2. IPMC - MLD Snooping - Groups Information



Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.

Navigating the MLD Group Table

Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MLD Group Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The “>>” will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

MLD Group Table Columns

VLAN ID

VLAN ID of the group.

Groups

Group address of the group displayed.

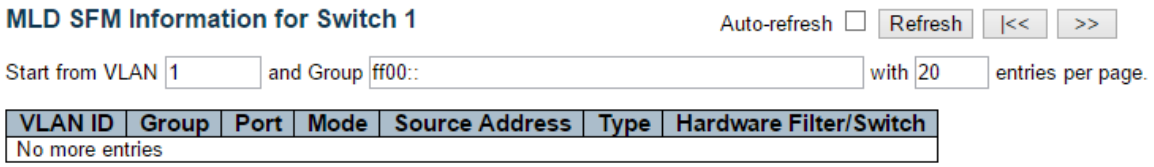
Port Members

Ports under this group.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table, starting with the first entry in the MLD Group Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.11.2.3. IPMC - MLD Snooping - IPv6 SFM Information



Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Navigating the MLD SFM Information Table

Each page shows up to 99 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MLD SFM Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The “<<” will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

MLD SFM Information Table Columns

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

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

IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type

Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table starting from the first entry in the MLD SFM Information Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.12. Monitor - LLDP

3.2.12.1. LLDP - Neighbours

LLDP Remote Device Summary Auto-refresh ☐ Refresh

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
Port 23	00-01-C1-00-00-00	4	Port #4		Bridge(+)	192.168.2.253 (IPv4)
Port 23	00-03-CE-46-7C-0B	4	Port #4		Bridge(+)	192.168.20.254 (IPv4)
Port 23	D4-6A-91-36-10-34	7	Port #7		Bridge(+)	192.168.2.230 (IPv4)
Port 23	00-03-CE-24-51-88	8	Port #8		Bridge(+)	192.168.2.4 (IPv4)

This page provides a status overview for all LLDP neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. The columns hold the following information:

Local Port

The port on which the LLDP frame was received.

Chassis ID

The Chassis ID is the identification of the neighbour's LLDP frames.

Port ID

The Port ID is the identification of the neighbour port.

Port Description

Port Description is the port description advertised by the neighbour unit.

System Name

System Name is the name advertised by the neighbour unit.

System Capabilities

System Capabilities describes the neighbour unit's capabilities. The possible capabilities are:

1. Other
2. Repeater
3. Bridge
4. WLAN Access Point
5. Router
6. Telephone
7. DOCSIS cable device
8. Station only
9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

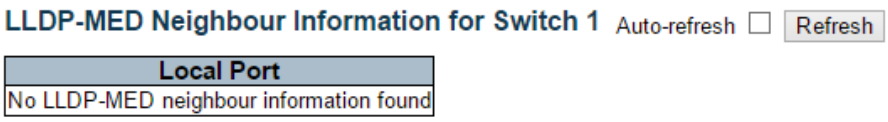
Management Address

Management Address is the neighbour unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbour's IP address.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page.

3.2.12.2. LLDP - LLDP-MED Neighbours



This page provides a status overview of all LLDP-MED neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. This function applies to VoIP devices which support LLDP-MED. The columns hold the following information:

Port

The port on which the LLDP frame was received.

Device Type

LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device Definition

LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (included for historical reasons)
4. IEEE 802.11 Wireless Access Point
5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

LLDP-MED Capabilities

LLDP-MED Capabilities describes the neighbour unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE

5. Extended Power via MDI - PD
6. Inventory
7. Reserved

Application Type

Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice Signaling - for use in network topologies that require a different policy for the voice Signaling than for the voice media.
3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice Signaling than for the guest voice media.
5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.
6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signaling - for use in network topologies that require a separate policy for the video Signaling than for the video media.

Policy

Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown

- **Unknown:** The network policy for the specified application type is currently unknown.
- **Defined:** The network policy is defined.

TAG

TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

- **Untagged:** The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.
- **Tagged:** The device is using the IEEE 802.1Q tagged frame format.

VLAN ID

VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

Priority

Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).

DSCP

DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

Auto-negotiation

Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.

Auto-negotiation status

Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

Auto-negotiation Capabilities

Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page.

3.2.12.3. LLDP - PoE

LLDP Neighbour Power Over Ethernet Information for Switch 1 Auto-refresh ☐ Refresh

Local Port	Power Type	Power Source	Power Priority	Maximum Power
23	PSE Device	Primary Power Supply	Low	0 [W]
23	PSE Device	Primary Power Supply	Low	0 [W]
23	PSE Device	Primary Power Supply	Low	0 [W]
23	PSE Device	Primary Power Supply	Low	0 [W]

This page provides a status overview for all LLDP PoE neighbours. The displayed table contains a row for each port on which an LLDP PoE neighbour is detected. The columns hold the following information:

Local Port

The port for this switch on which the LLDP frame was received.

Power Type

The Power Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD).

If the Power Type is unknown it is represented as "Reserved".

Power Source

The Power Source represents the power source being utilized by a PSE or PD device.

If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown"

If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE.

If it is unknown what power supply the PD device is using it is indicated as "Unknown"

Power Priority

Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's port that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low.

If the power priority is unknown it is indicated as "Unknown"

Maximum Power

The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.

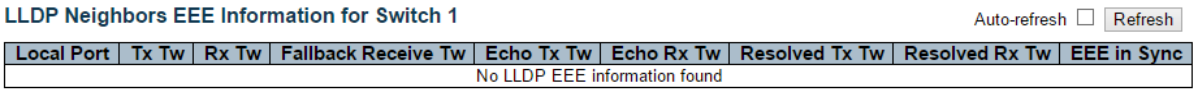
The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it

is represented as "reserved"

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page.

3.2.12.4. LLDP - EEE



By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx "wakeup time ", as a way to agree upon the minimum wakeup time they need.

This page provides an overview of EEE information exchanged by LLDP.

LLDP Neighbors EEE Information

The displayed table contains a row for each port. The columns hold the following information:

Local Port

The port on which LLDP frames are received or transmitted.

Tx Tw

The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.

Rx Tw

The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.

Fallback Receive Tw

The link partner's fallback receive Tw.

A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

Echo Tx Tw

The link partner's Echo Tx Tw value.

The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

Echo Rx Tw

The link partner's Echo Rx Tw value.

Resolved Tx Tw

The resolved Tx Tw for this link. Note : NOT the link partner

The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw

The resolved Rx Tw for this link. Note : NOT the link partner

The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

EEE in Sync

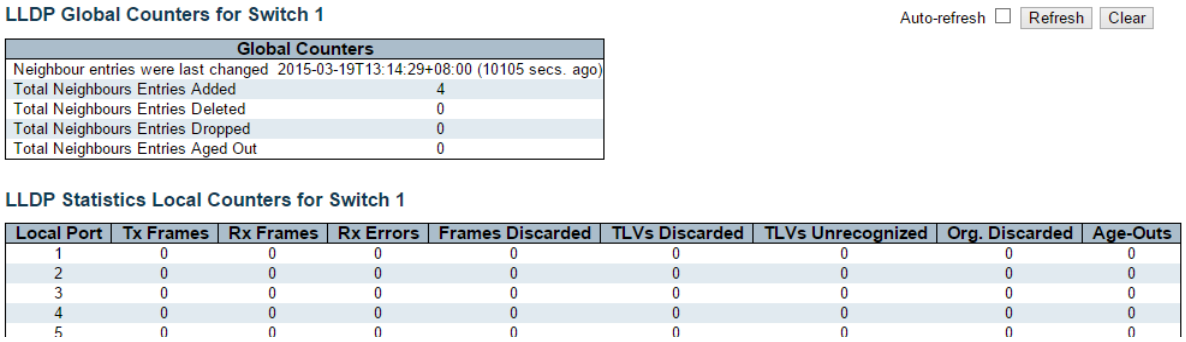
Shows whether the switch and the link partner have agreed on wake times.

- Red - Switch and link partner have not agreed on wakeup times.
- Green - Switch and link partner have agreed on wakeup times.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page.

3.2.12.5. LLDP - Port Statistics



This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole stack, while local counters refer to per port counters for the currently selected switch.

Global Counters

Neighbour entries were last changed

Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbours Entries Added

Shows the number of new entries added since switch reboot.

Total Neighbours Entries Deleted

Shows the number of new entries deleted since switch reboot.

Total Neighbours Entries Dropped

Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbours Entries Aged Out

Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

Local Port

The port on which LLDP frames are received or transmitted.

Tx Frames

The number of LLDP frames transmitted on the port.

Rx Frames

The number of LLDP frames received on the port.

Rx Errors

The number of received LLDP frames containing some kind of error.

Frames Discarded

If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

TLVs Discarded

Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). 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 organizationally received TLVs.

Age-Outs

Each LLDP frame contains information about how long time 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.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page.
- **Clear:** Clears the local counters. All counters (including global counters) are cleared upon reboot.

3.2.13. Monitor - PoE

Power Over Ethernet Status for Switch 1

Auto-refresh ☐ Refresh

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
9	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
10	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
11	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
12	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
13	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
14	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
15	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
16	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
17	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
18	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
19	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
20	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
21	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
22	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
23	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
24	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

This page allows the user to inspect the current status for all PoE ports.

Local Port

This is the logical port number for this row.

PD Class

Each PD is classified according to a class that defines the maximum power the PD will use.

The PD Class shows the PDs class.

Five Classes are defined:

- Class 0: Max. power 15.4 W
- Class 1: Max. power 4.0 W
- Class 2: Max. power 7.0 W
- Class 3: Max. power 15.4 W
- Class 4: Max. power 30.0 W

Power Requested

The Power Requested shows the requested amount of power the PD wants to be reserved.

Power Allocated

The Power Allocated shows the amount of power the switch has allocated for the PD.

Power Used

The Power Used shows how much power the PD currently is using.

Current Used

The Power Used shows how much current the PD currently is using.

Priority

The Priority shows the port's priority configured by the user.

Port Status

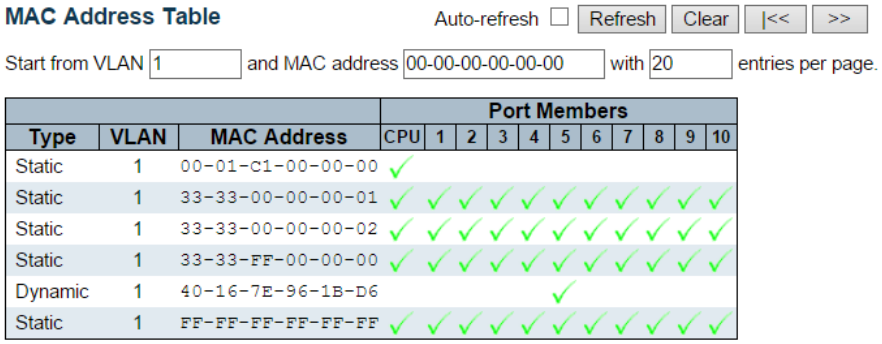
The Port Status shows the port's status. The status can be one of the following values:

- PoE not available - No PoE chip found - PoE not supported for the port.
- PoE turned OFF - PoE disabled : PoE is disabled by user.
- PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.
- No PD detected - No PD detected for the port.
- PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down.
- PoE turned OFF - PD is off.
- Invalid PD - PD detected, but is not working correctly.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page.

3.2.14. Monitor - MAC Table



Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

MAC Table Columns

Type
Indicates whether the entry is a static or a dynamic entry.

MAC address
The MAC address of the entry.

VLAN
The VLAN ID of the entry.

Port Members

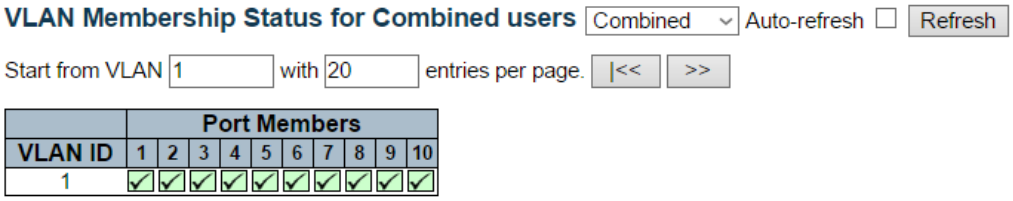
The ports that are members of the entry.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.
- **Clear:** Flushes all dynamic entries.
- **|<<:** Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.15. Monitor - VLANs

3.2.15.1. VLANs - VLAN Membership



This page provides an overview of membership status of VLAN users.

VLAN User

Various internal software modules may use VLAN services to configure VLAN memberships on the fly.

The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

VLAN ID

VLAN ID for which the Port members are displayed.

Port Members

A row of check boxes for each port is displayed for each VLAN ID.

- If a port is included in a VLAN, the following image will be displayed:
- If a port is in the forbidden port list, the following image will be displayed:
- If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed . The port will not be a member of the VLAN in this case.

Navigating the VLAN Membership Status page

Each page shows up to 99 entries from the VLAN table (default being 20), selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input field allows the user to select the starting point in the VLAN Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next VLAN Table match.

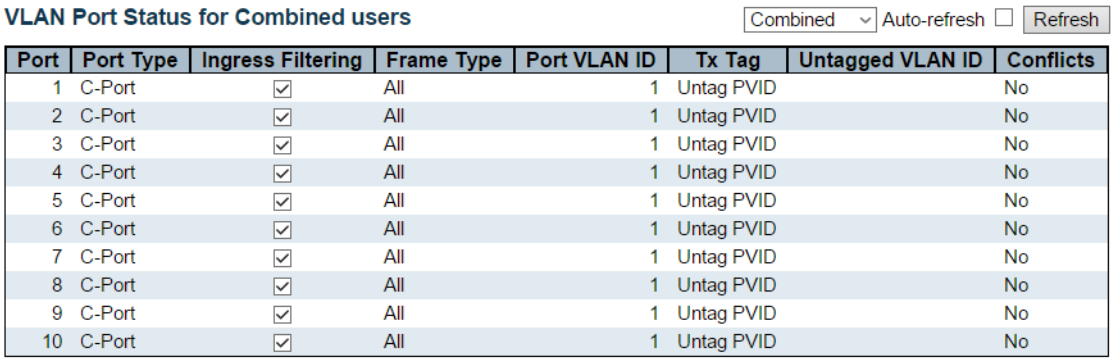
The “>>” button will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached, the text "No data exists for the selected user" is shown in the table. Use the “|<<” button to start over.

Buttons

- 

: Select VLAN Users from this drop down list.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.

3.2.15.2. VLANs - VLAN Ports



VLAN Port Status for Combined users

Combined Auto-refresh Refresh

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

This page provides VLAN Port Status.

VLAN User

Various internal software modules may use VLAN services to configure VLAN port configuration on the fly.

The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.

Port

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

Port Type

Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port.

The field is empty if not overridden by the selected user.

Ingress Filtering

Shows whether a given user wants ingress filtering enabled or not.

The field is empty if not overridden by the selected user.

Frame Type

Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port.

The field is empty if not overridden by the selected user.

Port VLAN ID

Shows the Port VLAN ID (PVID) that a given user wants the port to have.

The field is empty if not overridden by the selected user.

Tx Tag

Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port.

The field is empty if not overridden by the selected user.

Untagged VLAN ID

If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress.

The field is empty if not overridden by the selected user.

Conflicts

Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress.

Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority.

If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module.

The "Combined" user reflects what is actually configured in hardware.

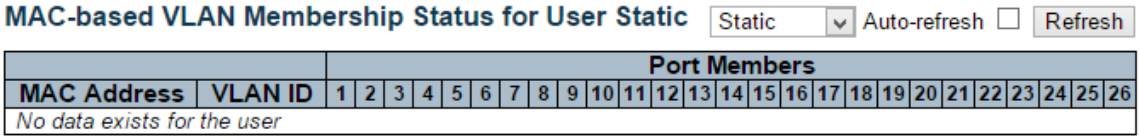
Buttons

- 

: Select VLAN **Users** from this drop down list.
- **Auto-refresh**: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh** : Click to refresh the page immediately.

3.2.16. Monitor - VCL

3.2.16.1. VCL - MAC-based VLAN



This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently we support following VLAN User types:

- CLI/Web/SNMP: These are referred to as static.
- NAS: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

MAC Address

Indicates the MAC address.

VLAN ID

Indicates the VLAN ID.

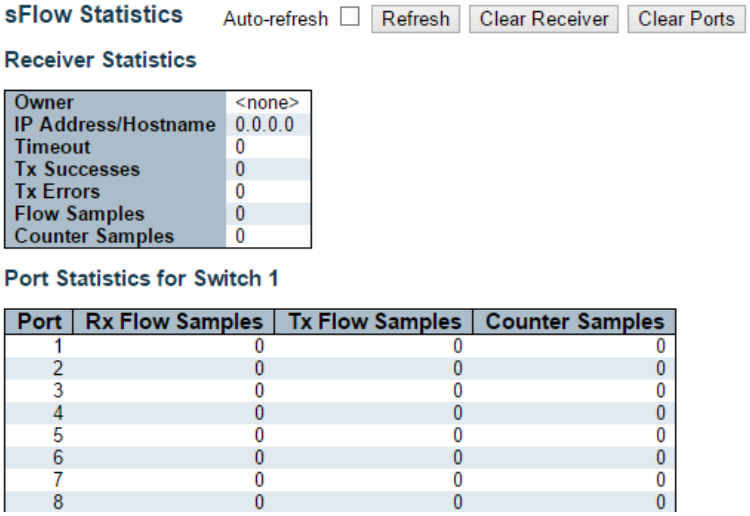
Port Members

Port members of the MAC-based VLAN entry.

Buttons

- **Refresh:** Refreshes the displayed table.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds (only present if stacking is enabled).

3.2.17. Monitor - sFlow



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

The IP address or hostname of the sFlow receiver.

Timeout

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.

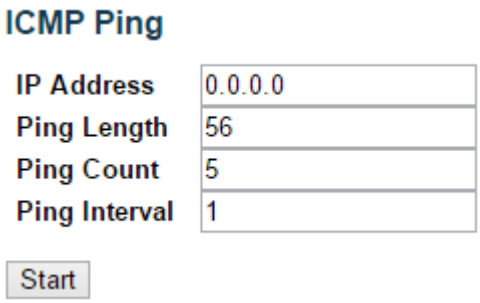
Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds (only present if stacking is enabled).
- **Refresh:** Click to refresh the page.
- **Clear Receiver:** Clears the sFlow receiver counters.
- **Clear Port:** Clears the per-port counters.

3.3. Web Management - Diagnostics

This section of the management web page provides you tools for diagnosing your network.

3.3.1. Diagnostics - Ping



This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you press the "Start" button, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space(the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING server 10.10.132.20, 56 bytes of data.
64 bytes from 10.10.132.20: icmp_seq=0, time=0ms
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms
64 bytes from 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

IP Address
The destination IP Address.

Ping Length
The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

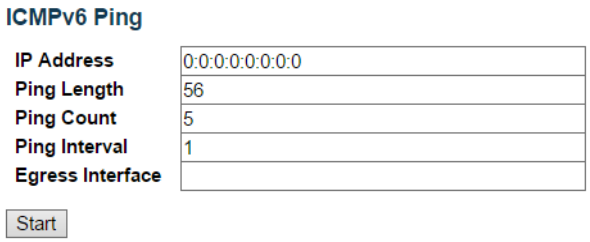
Ping Count
The count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval
The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Buttons

- **Start:** Click to start transmitting ICMP packets.
- **New Ping:** Click to re-start diagnostics with PING.

3.3.2. Diagnostics - Ping6



This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you press the "Start" button, ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING6 server ::10.10.132.20, 56 bytes of data.
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

IP Address
The destination IP Address.

Ping Length
The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count
The count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval
The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Egress Interface (Only for IPv6)

The VLAN ID (VID) 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.

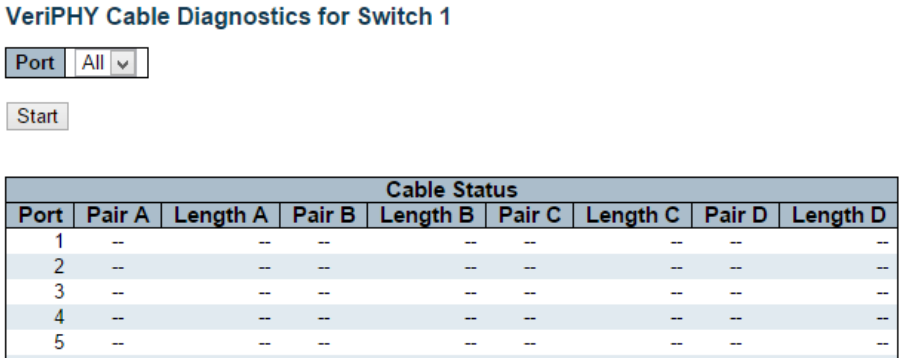
Do not specify egress interface for loopback address.

Do specify egress interface for link-local or multicast address.

Buttons

- **Start:** Click to start transmitting ICMP packets.
- **New Ping:** Click to re-start diagnostics with PING.

3.3.3. Diagnostics - VeriPHY



This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

Press the "Start" button to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

The ports belong to the currently selected stack unit, as reflected by the page header.

Port

The port where you are requesting VeriPHY Cable Diagnostics.

Cable Status

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

3.4. Web Management - Maintenance

Here you can make system maintenance such rebooting the PoE switch, reset all settings (except Switch's IP address) back to default value, updating switch firmware, or upload/download all system settings.

3.4.1. Maintenance - Restart Device



You can restart the stack on this page. After restart, the stack will boot normally.

Buttons

- **Yes:** Click to restart device.
- **No:** Click to return to the Port State page without restarting.

3.4.2. Maintenance - Factory Defaults



You can reset the configuration of the stack on this page. Only the IP configuration is retained.

The new configuration is available immediately, which means that no restart is necessary.

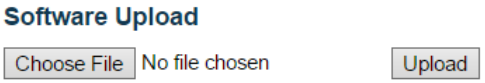
Buttons

- **Yes:** Click to reset the configuration to Factory Defaults.
- **No:** Click to return to the Port State page without resetting the configuration.

Note: Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default

3.4.3. Maintenance - Software

3.4.3.1. Software - Upload



You can update the switch's firmware here.

Buttons

- **Choose File:** Click this button to choose the firmware file.
- **Update:** Click this button to start upload the firmware.

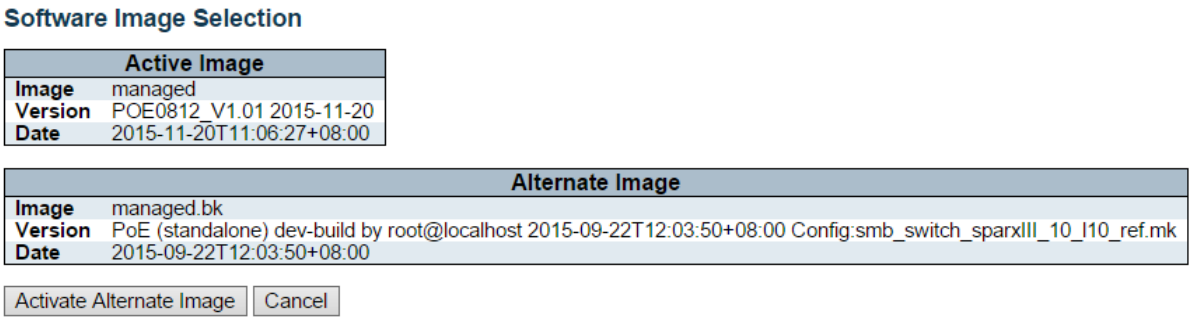


The system will inform you when the new firmware is uploaded to the switch. After updating the firmware, the switch will reboot.



Warning: The management web page will stop functioning during the firmware updating process. Do not restart or power off the device at this time or the switch may malfunction.

3.4.3.2. Software - Image Select



This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

Note:
In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.

If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.

The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Image Information

Image
The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named image.bk.

Version
The version of the firmware image.

Date
The date where the firmware was produced.

Buttons

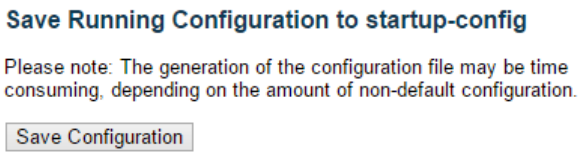
- **Activate** Alternate Image: Click to use the alternate image. This button may be disabled depending on system state.
- **Cancel**: Cancel activating the backup image. Navigates away from this page.

3.4.4. Maintenance - Configuration

You can manage the system configuration files here in this section.The switch stores its system settings in a number of text files in CLI format. There are three system files:

- **Running-config:** A virtual file that represents the currently active configuration on the switch. This file is volatile and will be lost if the switch reboots if it is not saved as the startup-config.
- **Startup-config:** The startup configuration for the switch, which will be read when the switch is booting.
- **Default-config:** A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

3.4.4.1. Configuration - Save Startup-config

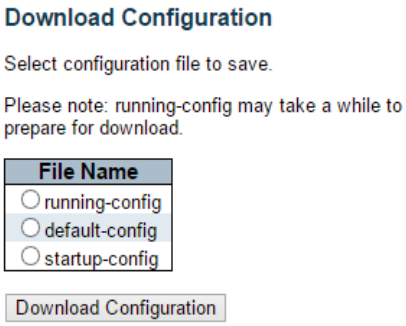


Buttons

- **Save Configuration:** Click to save the current running-config as the startup-config file.

Note: After making any settings to the switch, you must save the current running-config to the startup-config. All your settings will be lost if you didn't save the current running-config to the startup-config and reboot the switch.

3.4.4.2. Configuration - Download



File Name

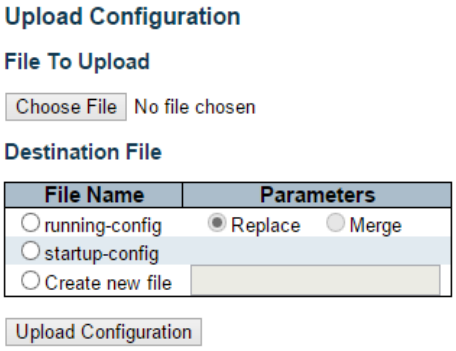
Here you can choose the configuration file you would like to save to your PC, including:

- **Running-config**
- **Startup-config**
- **Default-config**

Buttons

- **Download Configuration:** Click this button to save the configuration you chose.

3.4.4.3. Configuration - Upload



You can upload a configuration file here and replace it with all other configuration files saved on the switch (except default-config, which is read-only).

File to Upload

To select the configuration file you would like to upload to the switch from your PC, please press the **Choose File** button and choose the configuration file.

Destination File

Here you can choose which configuration file will be replaced by the uploaded file. If the destination file is running-config, the file will be applied to the current switch configuration in two ways:

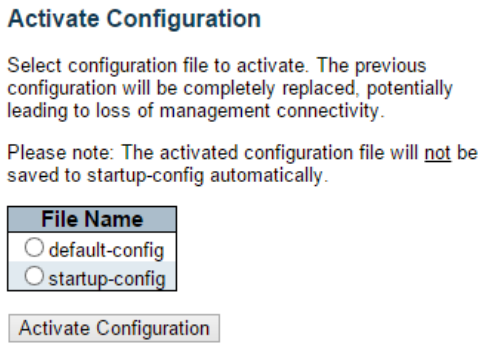
- **Replace mode:** The current configuration is fully replaced with the configuration in the uploaded file.
- **Merge mode:** The uploaded file is merged into running-config.

Also, you can save a configuration file to the switch with user-defined file name here. Please note that you can only have 2 such files, and if the file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files until an existing file is overwritten or deleted.

Buttons

- **Upload Configuration:** Click this button to upload the configuration you chose.

3.4.4.4. Configuration - Activate

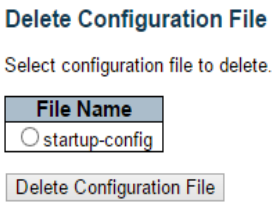


Here you can choose the configuration file that will be activated immediately. Please note that although the configuration file you choose here will be activated and run as the current configuration setting, it will not be saved as the startup-config automatically.

Buttons

- **Activate Configuration:** Click this button to activate the configuration you chose.

3.4.4.5. Configuration - Delete



Here you can delete the configuration files saved on the switch.

File Name

Choose the configuration file that you would like to delete here.

Buttons

- **Delete Configuration File:** Click this button to delete the configuration you chose.

Appendix A: Product Safety



This appendix describes safety issues regarding to this product. To use this product safely, it is highly recommended to read this appendix before installing and using this product.

Failure to follow these precautions and warnings might cause product malfunction, electrical shock, or even fire. If this product is working abnormally (e.g. generating smoke), please stop using this product and contact your distributor or retailer immediately.

DO NOT install this product under conditions listed below:

- DO NOT install this product in an environment with conditions exceeding its specified operating environment.
- DO NOT install this product in an environment that is subjected to direct sunlight or near any heating equipment.
- DO NOT install this product in an environment with extreme temperature changes. Extreme temperature changes, even within the product's operating temperature range, may cause malfunctions.
- DO NOT install this product in a location near any sources of water or liquid.
- DO NOT stack this product with other network devices directly on top of one another. Stacking network devices directly without applying a mounting rack will cause this product to overheat.
- DO NOT install this product on an unstable surface. Doing so might cause this product to fall, resulting malfunction.

Product Maintenance Guide:

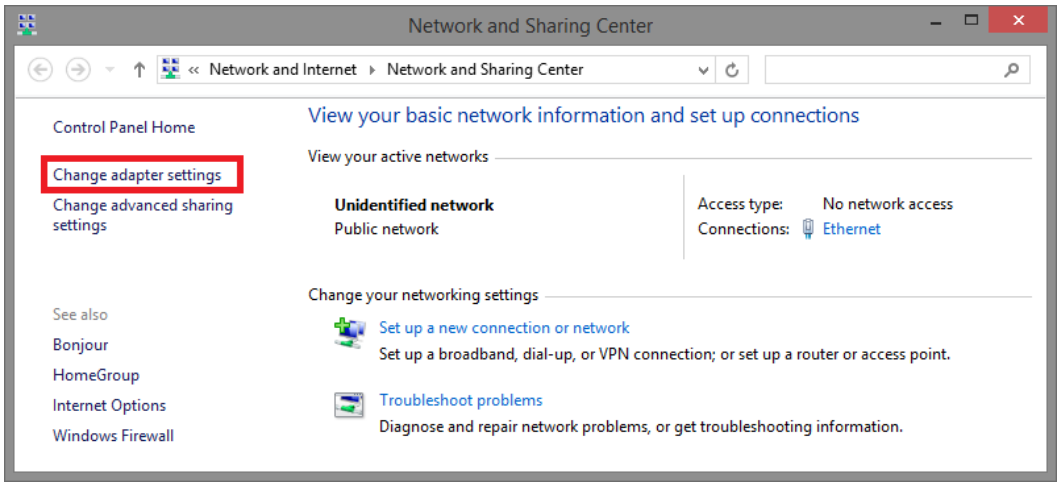
- DO NOT disassemble this product. Doing so might cause malfunction and void your product's warranty.
- It is recommended to keep your product clear of dust. To remove dust from your product, please use a dry brush and brush it off gently.
- When not using this product, please store it in an environment with low humidity, cool temperature, and free of dust. Failure to do so might cause malfunction.
- Before powering up this product, please make sure that the electric power source meets this product's requirement. DO NOT use other power adapters if this product comes with its own power adapter in the package.

Appendix B: IP Configuration for Your PC

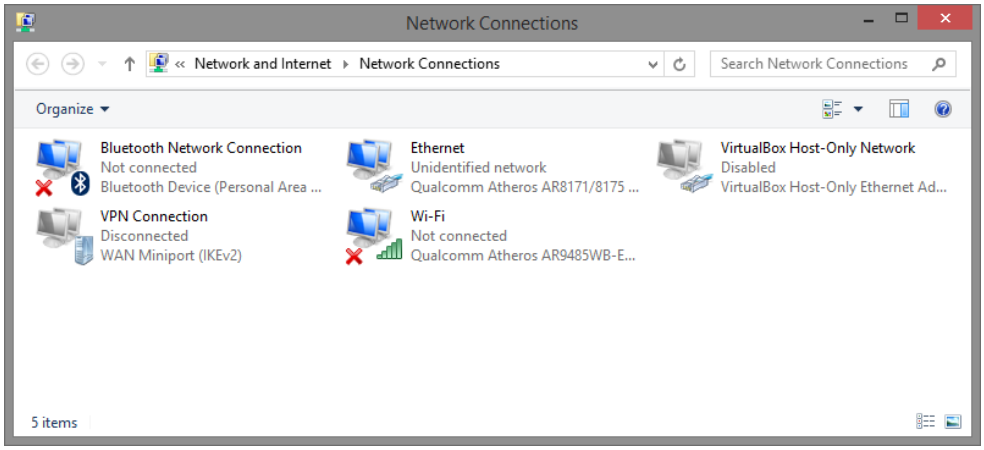
This appendix describes how to set the IP address of your PC so you can connect to product configuration webpage. The configuration webpage allows you to set system variables or monitor system status.

The following section will guide you to set the IP address properly in a Microsoft Windows 8 environment. Setting IP address in other Microsoft operating system (such as Windows Vista or Windows 7) is quite the same and can be related.

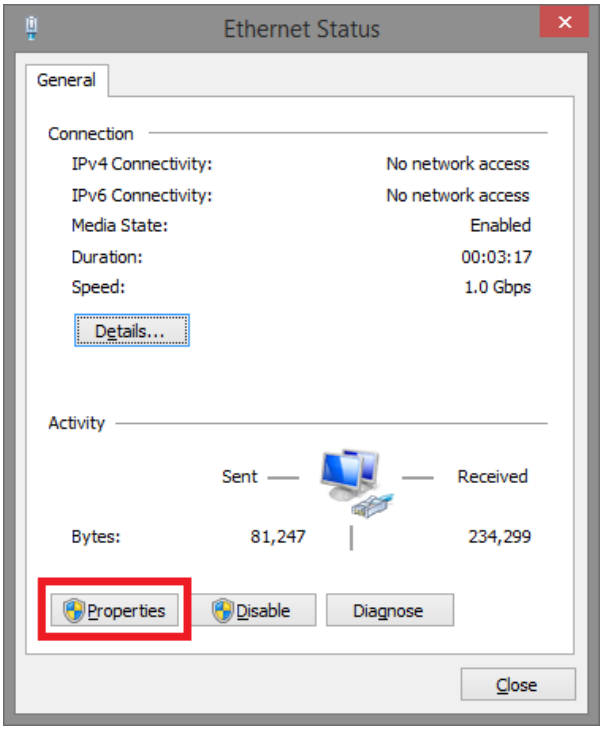
1. Open **Network and Sharing Center** in **Control Panel**, and click on **Change adapter settings** as shown in the figure down below.



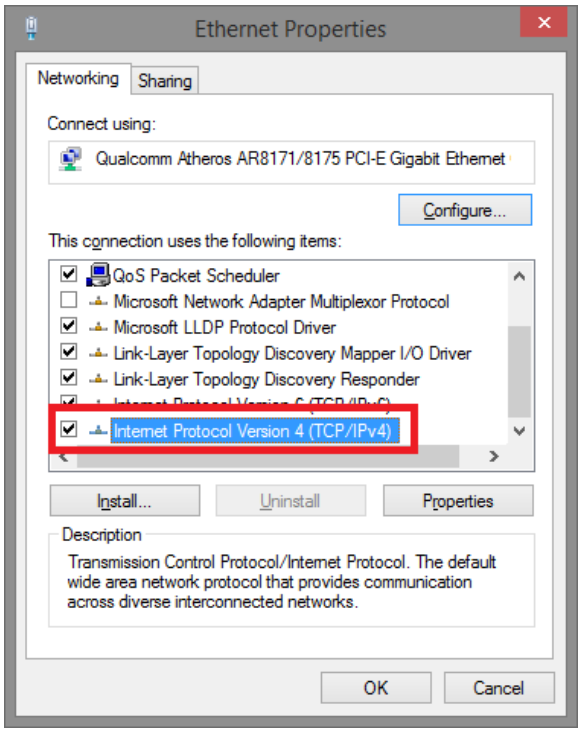
2. A **Network Connections** window will pop up, **showing** all the network connections available on your PC. Please double-click on the network connection you are using to connect to the switch.



3. An **Ethernet Status** window will pop up. Please click on the **Properties** button as shown in the figure down below.



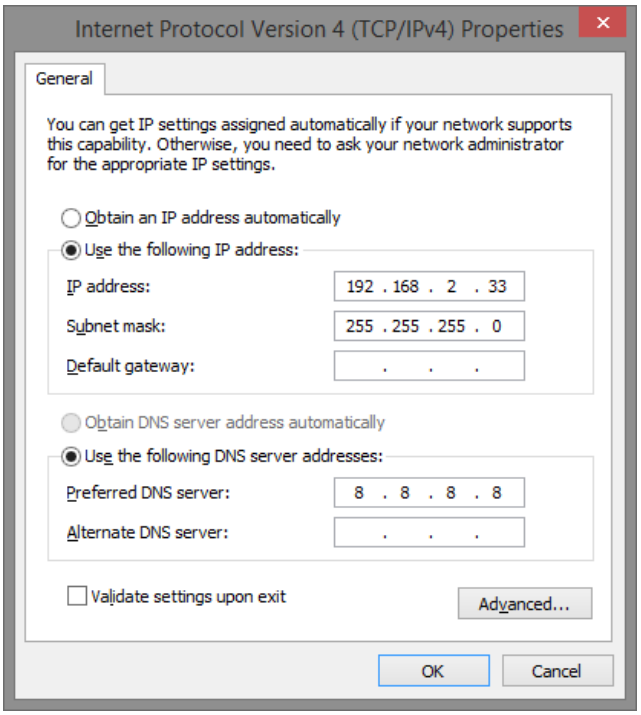
4. An **Ethernet Properties** window will pop up. Please double click on the **Internet Protocol Version 4 (TCP/IPv4)**.



5. An **Internet Protocol Version 4 (TCP/IPv4) Properties** window will pop up. Please set your PC's IP address and subnet mask as shown in the figure down below.

   By defaul t, your product's IP address should be **192.168.2.1**.You can set any IP address as long as it's not the same with your product's IP address and is in the same network segment with your product's IP address.

   Press **OK** to apply the TCP/IPv4 settings you just m ade. Now you can connect to your product using a web browser (i.e. Internet Explorer, Chrome, or Firefox).



Appendix C: Glossary

This appendix contains the terms and glossaries that are used in this user manual.

A

ACE

ACE is an acronym for **A**ccess **C**ontrol **E**ntry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for **A**ccess **C**ontrol **L**ist. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.

ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

ARP

ARP is an acronym for **A**ddress **R**esolution **P**rotocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CDP

CDP is an acronym for **C**isco **D**iscovery **P**rotocol.

D

DEI

DEI is an acronym for **D**rop **E**ligible **I**ndicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for **D**ata **E**ncryption **S**tandard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for **D**ynamic **H**ost **C**onfiguration **P**rotocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID

(option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for **D**omain **N**ame **S**ystem. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.

An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

Drop Precedence Level

Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 or higher corresponds to 'Discard Eligible' (Yellow) frames.

DSCP

DSCP is an acronym for **D**ifferentiated **S**ervices **C**ode **P**oint. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

H

HTTP

HTTP is an acronym for **H**ypertext **T**ransfer **P**rotocol. It is a protocol that used to transfer or convey information on the World Wide Web (www).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for **H**ypertext **T**ransfer **P**rotocol over **S**ecure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for **I**nternet **C**ontrol **M**essage **P**rotocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for **I**nternet **G**roup **M**anagement **P**rotocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for **I**nternet **M**essage **A**ccess **P**rotocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, andSMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for **I**nternet **P**rotocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for **IP** **M**ulti**C**ast.

IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol, allows bundling several physical ports together to form a single logical port.

LLC

The IEEE 802.2 **L**ogical **L**ink **C**ontrol (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The **L**ink **L**ayer **D**iscovery **P**rotocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LLQI

LLQI (Last Listener Query Interval) is the maximum response time used to calculate the Maximum Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC

LOC is an acronym for **L**oss **O**f **C**onnectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for **M**ulticast **L**istener **D**iscovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MSTP

In 2002, the IEEE introduced an evolution ofRSTP: the **M**ultiple **S**panning **T**ree **P**rotocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

N

NTP

NTP is an acronym for **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

Optional TLVs.

A LLDP frame contains multiple TLVs

For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP

PCP is an acronym for **P**riority **C**ode **P**oint. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for **P**owered **D**evice. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

Ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

Ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

PoE is an acronym for **P**ower **O**ver **E**thernet.

Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

Private VLAN

In a private VLAN, PVLANs provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

PTP

PTP is an acronym for **P**recision **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for **Q**oS **C**ontrol **E**ntry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for **Q**oS **C**ontrol **L**ist. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for **Q**uality **o**f **S**ervice. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

R

RARP

RARP is an acronym for **R**everse **A**ddress **R**esolution **P**rotocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

sFlow

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for **S**imple **M**ail **T**ransfer **P**rotocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The **S**ub **N**etwork **A**ccess **P**rotocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for **S**imple **N**etwork **M**anagement **P**rotocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for **S**imple **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SSH

SSH is an acronym for **S**ecure **SH**ell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality.

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for **T**erminal **A**cess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for **T**ransmission **C**ontrol **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a

message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for **TEL**etype **NET**work. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for **T**rivial **F**ile **T**ransfer **P**rotocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS

ToS is an acronym for **T**ype **o**f **S**ervice. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for **T**ype **L**ength **V**alue. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

U

UDP

UDP is an acronym for **U**ser **D**atagram **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the

entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for **U**niversal **P**lug and **P**lay. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are

forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

Revision History

Version	Firmware Ver.	Date	Remark
Ver 1.0	2016-04-21	2016/08/09	1. First version.
Ver 2.2	v1.0.1	2019/09/05	Add Virtual Stacking