NS3502-8P-2T-2S-V2 User Manual

P/N 1073640-EN • REV D • ISS 13JUL22

Copyright

© 2022 Carrier. All rights reserved. Specifications subject to change without prior notice.

This document may not be copied in whole or in part or otherwise reproduced without prior written consent from Carrier, except where specifically permitted under US and international copyright law.

Trademarks and patents

IFS names and logos are a product brand of Aritech, a part of Carrier.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer

PLACED ON THE MARKET BY:
Carrier Fire & Security Americas Corporation Inc.
13995 Pasteur Blvd, Palm Beach Gardens, FL 33418, USA

AUTHORIZED EU REPRENSENTATIVE:
Carrier Fire & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Netherlands

Version

Class A: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC compliance

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This Device must accept any interference received, including interference that may cause undesired operation.

FCC compliance

Notice! 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.

Canada

This Class A digital apparatus complies with CAN ICES-003 (A)/NMB-3 (A).

Cet appareil numérique de la classe A est conforme à la norme CAN ICES-003 (A)/NMB-3 (A).

ACMA compliance

Notice! 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.

Certification

EU directives

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.

Product warnings and disclaimers

THESE PRODUCTS ARE INTENDED FOR SALE TO AND INSTALLATION BY QUALIFIED PROFESSIONALS. CARRIER FIRE & SECURITY CANNOT PROVIDE ANY ASSURANCE THAT ANY PERSON OR ENTITY BUYING ITS PRODUCTS, INCLUDING ANY “AUTHORIZED DEALER” OR “AUTHORIZED RESELLER”, IS PROPERLY TRAINED OR EXPERIENCED TO CORRECTLY INSTALL FIRE AND SECURITY RELATED PRODUCTS.

For more information on warranty disclaimers and product safety information, please check https://firesecurityproducts.com/policy/product-warning/ or scan the following code:

Contact information

EMEA: https://firesecurityproducts.com

Australian/New Zealand: https://firesecurityproducts.com.au/

Product documentation

Please consult the following web link to retrieve the electronic version of the product documentation. The manuals are available in several languages.

Content

Important information 3

Chapter 1 **Introduction 6**
Package contents 6
Product description 6
Product features 11
Product specifications 14

Chapter 2 **Installation 19**
Hardware description 19
Cabling 23

Chapter 3 **Switch management 29**
Requirements 29
Management access overview 29
Administration console 30
Web management 31
SNMP-based network management 32

Chapter 4 **Web configuration 33**
Main web page 35
System 36
DHCP server 61
UDLD 72
Simple Network Management Protocol (SNMP) 74
Port management 85
Link aggregation 93
VLAN 100
Spanning Tree Protocol (STP) 127
Multicast 145
Quality of Service (QoS) 171
Access Control Lists (ACL) 194
Authentication 200
Security 236
MAC address table 253
LLDP 257
Network diagnostics 271
Loop protection 275
RMON 277
Power over Ethernet (PoE) 286
Port identification 300

Chapter 5 **Command line interface 301**
Accessing the CLI 301

Telnet login 301

Chapter 6 **Command line mode 302**
System Command 303
IP Command 309
Port Management Command 315
MAC Address Table Command 318
VLAN Configuration Command 322
Private VLAN Configuration Command 329
Security Command 331
Spanning Tree Protocol Command 377
Link Aggregation Command 386
Link Aggregation Control Protocol Command 388
LLDP Command 391
LLDP MED Command 395
Thermal Command 399
PoE Command 400
Ethernet Virtual Connections Command 401
Ethernet Protection Switching Command 406
Maintainence entity End Point Command 407
Quality of Service Command 414
Mirror Command 427
Configuration Command 428
Firmware Command 429
UPnP Command 429
MVR Command 431
Voice VLAN Command 434
Ethernet Ring Protection Switching Command 439
Loop Protect Command 443
IPMC Command 445
VLAN Control List Command 453
SMTP Command 457
Show Command 459

Chapter 7 **Switch operation 465**
Address table 465
Learning 465
Forwarding and filtering 465
Store-and-forward 465
Auto-negotiation 466

Chapter 8 **Troubleshooting 467**

Appendix A **Networking connection 468**

Glossary 470

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will Carrier be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of Carrier shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether Carrier has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, Carrier assumes no responsibility for errors or omissions.

Product Warnings

YOU UNDERSTAND THAT A PROPERLY INSTALLED AND MAINTAINED ALARM/SECURITY SYSTEM MAY ONLY REDUCE THE RISK OF EVENTS SUCH AS BURGLARY, ROBBERY, FIRE, OR SIMILAR EVENTS WITHOUT WARNING, BUT IT IS NOT INSURANCE OR A GUARANTEE THAT SUCH EVENTS WILL NOT OCCUR OR THAT THERE WILL BE NO DEATH, PERSONAL INJURY, AND/OR PROPERTY DAMAGE AS A RESULT.

THE ABILITY OF CARRIER PRODUCTS, SOFTWARE OR SERVICES TO WORK PROPERLY DEPENDS ON A NUMBER OF PRODUCTS AND SERVICES MADE AVAILABLE BY THIRD PARTIES OVER WHICH CARRIER HAS NO CONTROL AND FOR WHICH CARRIER SHALL NOT BE RESPONSIBLE INCLUDING, BUT NOT LIMITED TO, INTERNET, CELLULAR AND LANDLINE CONNECTIVITY; MOBILE DEVICE AND OPERATING SYSTEM COMPATIBILITY; MONITORING SERVICES; ELECTROMAGNETIC OR OTHER INTERFERENCE, AND PROPER INSTALLATION AND MAINTENANCE OF AUTHORIZED PRODUCTS (INCLUDING ALARM OR OTHER CONTROL PANEL AND SENSORS).

ANY PRODUCT, SOFTWARE, SERVICE OR OTHER OFFERING MANUFACTURED, SOLD OR LICENSED BY CARRIER, MAY BE HACKED, COMPROMISED AND/OR CIRCUMVENTED AND CARRIER MAKES NO REPRESENTATION, WARRANTY, COVENANT OR PROMISE THAT ITS PRODUCTS (INCLUDING SECURITY PRODUCTS), SOFTWARE, SERVICES OR OTHER OFFERINGS WILL NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED.

CARRIER DOES NOT ENCRYPT COMMUNICATIONS BETWEEN ITS ALARM OR OTHER CONTROL PANELS AND THEIR WIRELESS OUTPUTS/INPUTS INCLUDING

BUT NOT LIMITED TO, SENSORS OR DETECTORS UNLESS REQUIRED BY APPLICABLE LAW. AS A RESULT THESE COMMUNICATIONS MAY BE INTERCEPTED AND COULD BE USED TO CIRCUMVENT YOUR ALARM/SECURITY SYSTEM.

THE EQUIPMENT SHOULD ONLY BE OPERATED WITH AN APPROVED POWER ADAPTER WITH INSULATED LIVE PINS.

DO NOT CONNECT TO A RECEPTACLE CONTROLLED BY A SWITCH.

THIS UNIT INCLUDES AN ALARM VERIFICATION FEATURE THAT WILL RESULT IN A DELAY OF THE SYSTEM ALARM SIGNAL FROM THE INDICATED CIRCUITS. THE TOTAL DELAY (CONTROL UNIT PLUS SMOKE DETECTORS) SHALL NOT EXCEED 60 SECONDS. NO OTHER SMOKE DETECTOR SHALL BE CONNECTED TO THESE CIRCUITS UNLESS APPROVED BY THE LOCAL AUTHORITY HAVING JURISDICTION.

WARNING! The equipment should only be operated with an approved power adapter with insulated live pins.

Caution: Risk of explosion if battery is replaced by an incorrect type. Dispose of batteries according to the instructions. Contact your supplier for replacement batteries.

Warranty Disclaimers

CARRIER HEREBY DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING ANY IMPLIED WARRANTIES, THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

(USA only) SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM STATE TO STATE.

CARRIER DOES NOT MAKE ANY CLAIMS OR WARRANTIES TO YOU OF ANY KIND REGARDING ANY PRODUCT, SOFTWARE OR SERVICE'S POTENTIAL, ABILITY, OR EFFECTIVENESS TO DETECT, MINIMIZE, OR IN ANYWAY PREVENT DEATH, PERSONAL INJURY, PROPERTY DAMAGE, OR LOSS OF ANY KIND WHATSOEVER.

CARRIER DOES NOT REPRESENT TO YOU THAT ANY PRODUCT (INCLUDING SECURITY PRODUCTS), SOFTWARE, SERVICE OR OTHER OFFERING MAY NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED.

CARRIER DOES NOT WARRANT THAT ANY PRODUCT (INCLUDING SECURITY PRODUCTS), SOFTWARE OR SERVICE MANUFACTURED, SOLD OR LICENSED BY CARRIER WILL PREVENT, OR IN ALL CASES PROVIDE ADEQUATE WARNING OF OR PROTECTION FROM, BREAK-INS, BURGLARY, ROBBERY, FIRE, OR OTHERWISE.

CARRIER DOES NOT WARRANT TO YOU THAT ITS SOFTWARE OR PRODUCTS WILL WORK PROPERLY IN ALL ENVIRONMENTS AND APPLICATIONS AND DOES NOT WARRANT ANY PRODUCTS AGAINST HARMFUL ELECTROMAGNETIC INTERFERENCE INDUCTION OR RADIATION (EMI, RFI, ETC.) EMITTED FROM EXTERNAL SOURCES

CARRIER DOES NOT PROVIDE MONITORING SERVICES FOR YOUR ALARM/SECURITY SYSTEM (“MONITORING SERVICES”). IF YOU ELECT TO HAVE MONITORING SERVICES YOU MUST OBTAIN SUCH SERVICE FROM A THIRD PARTY AND CARRIER MAKES NO REPRESENTATION OR WARRANTY WITH RESPECT TO SUCH SERVICES INCLUDING WHETHER OR NOT THEY WILL BE COMPATIBLE WITH THE PRODUCTS, SOFTWARE OR SERVICES MANUFACTURED, SOLD OR LICENSED BY CARRIER.

Intended Use

Use this product only for the purpose it was designed for; refer to the data sheet and user documentation. For the latest product information, contact your local supplier or visit us online at firesecurityproducts.com.

The system should be checked by a qualified technician at least every 3 years and the backup battery replaced as required.

Advisory messages

Advisory messages alert you to conditions or practices that can cause unwanted results. The advisory messages used in this document are shown and described below.

WARNING: Warning messages advise you of hazards that could result in injury or loss of life. They tell you which actions to take or to avoid in order to prevent the injury or loss of life.

Caution: Caution messages advise you of possible equipment damage. They tell you which actions to take or to avoid in order to prevent the damage.

Note: Note messages advise you of the possible loss of time or effort. They describe how to avoid the loss. Notes are also used to point out important information that you should read.

Chapter 1
Introduction

The description of the IFS NS3502-8P-2T-2S-V2 model is as follows:

- L2+ 8-port 10/100/1000T 802.3at PoE
- + 2-port 10/100/1000T
- + 2-port 100/1000X SFP managed switch

Unless specified, the term “managed switch” mentioned in this user manual refers to the NS3502-8P-2T-2S-V2.

Package contents

Open the box of the managed switch and carefully unpack it. The box should contain the following items:

- The managed switch × 1
- Quick installation guide × 1
- RJ45 to RS232 cable × 1
- Rubber feet × 4
- Rack mounting brackets with attachment screws × 2
- Power cord × 1
- SFP dust-proof cap × 2

If any of these are missing or damaged, contact your dealer immediately. If possible, retain the carton including the original packing materials for repacking the product in case there is a need to return it to us for repair.

Product description

Cost-effective IPv6 managed Gigabit switch solution for enterprises

The Layer 2+ managed Gigabit switch features eight 10/100/1000T 802.3at PoE+ ports, two 10/100/1000T ports and two 100/1000X SFP ports. It supports static Layer 3

routing for enterprise-level networks, and features 30 W, 802.3at Power over Ethernet plus (PoE+), and two Gigabit SFP slots. With a total power budget of up to 240 W for different kinds of PoE applications, the managed switch provides quick, safe, and cost-effective PoE network solutions for security IP surveillance by small businesses and enterprises.

The L2/L4 switching engine offered by the managed switch performs effective data traffic control for enterprises and VoIP service providers, video streaming, and multicast applications. Providing user-friendly, advanced IPv6/IPv4 management interfaces, it is well suited for backbone and workgroup network applications that require affordability, high performance, and stable transmission quality.

Network cybersecurity network solution to minimize security risks

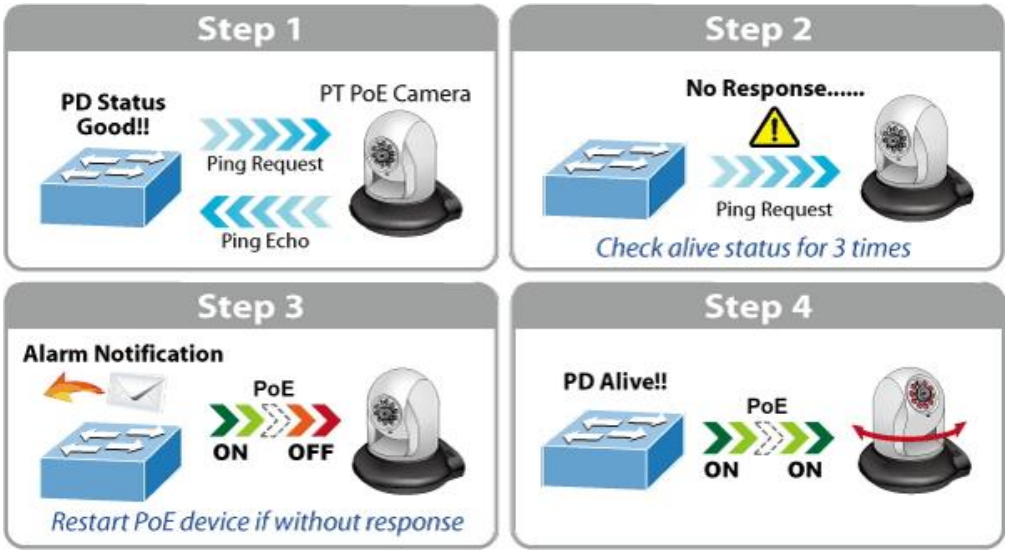
The managed switch has cybersecurity features to protect switch management and enhance the security of the mission-critical network without extra cost and effort. The managed switch also features expanded memory and upgrades both SSH and SSL protocols to provide strong protection against advanced threats. It includes a range of cybersecurity features such as DHCP Snooping, IP Source Guard, ARP Inspection Protection, 802.1x port-based and MAC-based network access control, RADIUS and TACACS+ user accounts management, SNMPv3 authentication, and so on to complement it as an all-around security solution. The network administrator can now construct highly-secure corporate networks with considerably less time and effort than before.

Convenient and smart ONVIF devices with detection feature

The managed switch's ONVIF Support is specifically designed to work with video IP surveillance programs, which can display connected ONVIF devices. In addition, clients can upload floor images to the managed switch, making the deployment of surveillance and other devices easy for planning and inspection purposes. Moreover, clients can obtain real-time surveillance information and online/offline status. PoE reboot control is also offered at the GUI level.

Intelligent powered device alive check

The managed switch can be configured to monitor connected powered device (PD) status in real time via a ping action. After the PD stops working and responding, the managed switch resumes the PoE port power and puts the PD back to work. The managed switch greatly enhances the network reliability through the PoE port resetting the PD’s power source and reducing the administrator management burden.

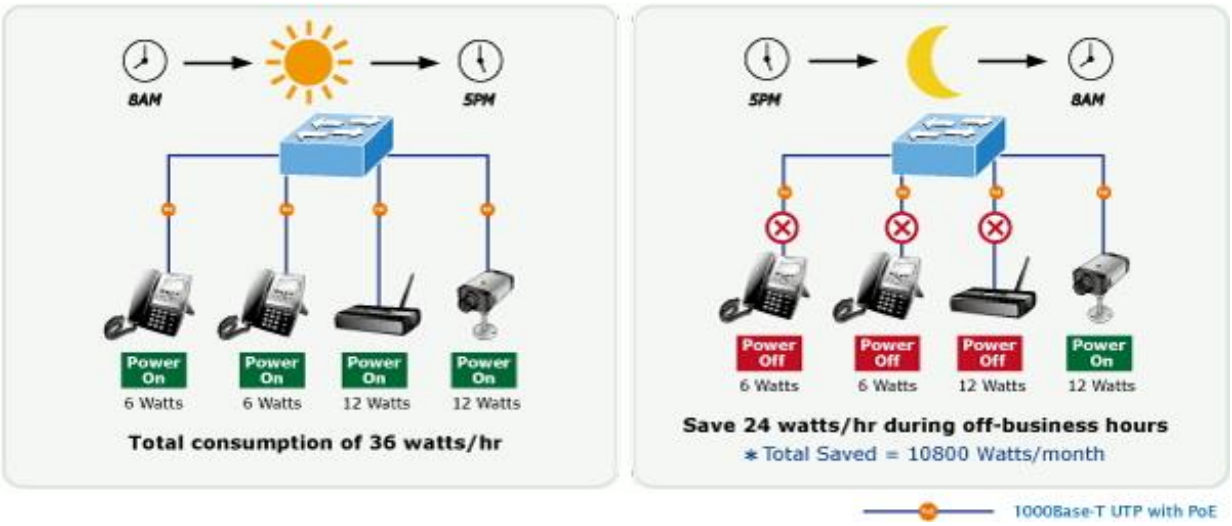


Scheduled power recycling

The managed switch permits each of the connected PoE IP cameras or PoE wireless access points to reboot at a specified time each week. This reduces the chance of IP camera or AP crashes resulting from buffer overflow.

PoE schedule for energy saving

Under the trend of energy saving worldwide and contributing to environmental protection, the managed switch can effectively control the power supply in addition to its capability of providing high Watt power. The “PoE schedule” function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals, and is a powerful function to help SMBs or enterprises save power and money. It also increases security by powering off PDs that should not be in use during non-business hours.

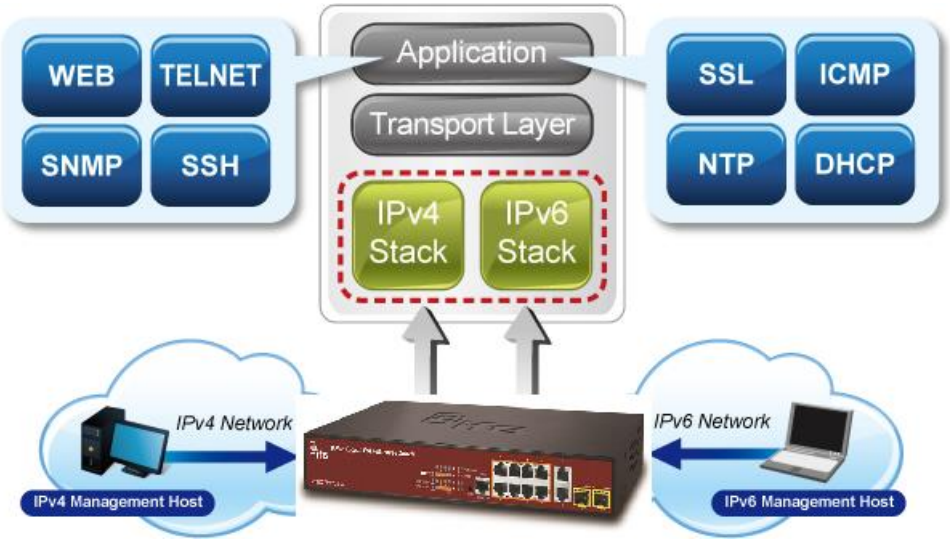


PoE usage monitoring

Via the power usage chart in the web management interface, the managed switch permits the administrator to monitor the status of the power usage of the connected PDs in real time, thus enhancing the management efficiency of the facilities.

Solution for IPv6 networking

To fulfill the demand of IPv6 (Internet Protocol version 6) network infrastructure, the managed switch supports both IPv4 and IPv6 management functions. It can work with current IPv4 network structure and also support the IPv6 network structure. With easy and friendly management interfaces and plenty of management functions included, the managed switch is the best choice for ISP to build the IPv6 FTTx edge service and for SMB to connect with IPv6 network.

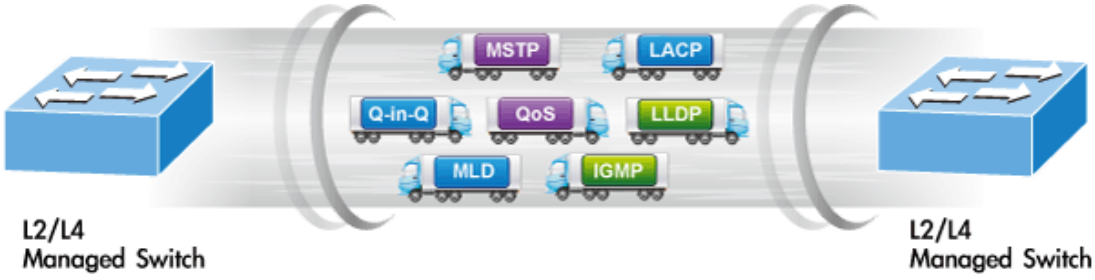


IPv4 and IPv6 VLAN routing for secure and flexible management

To help customers stay on top of their businesses, the managed switch not only provides ultra high transmission performance and excellent Layer 2 technologies, but also offers a IPv4/IPv6 VLAN routing feature that allows cross over of different VLANs and different IP addresses for the purpose of increased security, flexible management, and a simpler networking application.

Robust layer 2 features

The managed switch can be programmed for advanced switch management functions such as dynamic port link aggregation, Q-in-Q VLAN, private VLAN, Multiple Spanning Tree Protocol (MSTP), layer 2 to layer 4 QoS, bandwidth control, and IGMP / MLD snooping. The managed switch allows the operation of a high-speed trunk combining multiple ports. It enables up to six trunk groups with two ports per trunk group and supports connection fail-over.



Powerful security

The managed switch offers comprehensive layer 2 to layer 4 access control list (ACL) for enforcing security to the edge. It can be used to restrict to network access by denying packets based on source and destination IP address, TCP/UDP port number, or defined typical network applications. Its protection mechanism also comprises 802.1x port-based and MAC-based user and device authentication. With the private VLAN function, communication between edge ports can be prevented to ensure user privacy.

Enhanced security and traffic control

The managed switch provides DHCP Snooping, IP Source Guard, and Dynamic ARP Inspection functions to prevent IP snooping from attack and discard ARP packets with invalid MAC addresses. With enhanced security and strict traffic control, the managed switch plays a critical role in building highly-secure corporate networks.

Efficient and secure management

For efficient management, the managed switch is equipped with console, web, and SNMP management interfaces. With the built-in web-based management interface, the industrial switches offers an easy-to-use, platform-independent management and configuration facility. The managed switch supports standard Simple Network Management Protocol (SNMP) and can be managed by any management software based on the standard SNMP v1 or v2 protocol. For text-based management mode, the managed switch can be accessed via Telnet and the console port. Moreover, the managed switch offers secure management remotely by supporting SSH, SSL, and SNMP v3 connections where the packet content can be encrypted at each session.

Flexible and extendable solution

The managed switch features two mini-GBIC SFP slots that support dual speed 100BASE-FX and 1000BASE-SX/LX SFP (Small Form-factor Pluggable) fiber-optic modules, meaning the administrator now can flexibly choose the suitable SFP transceiver according to the transmission distance or the transmission speed required to extend the network efficiently. The distance can be extended from 550 m to 2 km (multi-mode fiber) up to above 10/20/30/40/50/70 km (single-mode fiber or WDM fiber). They are well suited for applications within enterprise data centers and distributions.

Intelligent SFP diagnosis mechanism

The managed switch supports a SFP-DDM (Digital Diagnostic Monitor) function that helps the network administrator easily monitor real-time parameters of the SFP and

SFP+ transceivers, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.

Product features

Physical port

- Ten 10/100/1000BASE-T gigabit Ethernet RJ45 ports with 8-port IEEE 802.3af / 802.3at PoE injector function.
- Two 100/1000BASE-X mini-GBIC/SFP slots.
- One RJ45 console interface for basic management and setup.

Power over Ethernet

- Complies with IEEE 802.3af / IEEE 802.3at Power over Ethernet / End-Span PSE.
- Complies with IEEE 802.3af Power over Ethernet / End-Span PSE.
- Up to eight ports of IEEE 802.3af/IEEE 802.3at devices powered.
- Supports PoE power up to 30 W for each PoE port.
- Auto detects powered device (PD).
- Circuit protection prevents power interference between ports.
- Remote power feeding up to 100 m.
- PoE management:
  - Total PoE power budget control
  - Per port PoE function enable/disable
  - PoE port power feeding priority
  - Per PoE port power limitation
  - PD classification detection
- Intelligent PoE features:
  - Temperature threshold control
  - PoE usage threshold control
  - PoE port status monitoring
  - PD alive check
  - Sequence port PoE

Layer 2 features

- Prevents packet loss with back pressure (half-duplex) and IEEE 802.3x PAUSE frame flow control (full-duplex).
- High performance of Store-and-Forward architecture and runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth.

Storm control support:

- Broadcast / Multicast / Unknown-Unicast

Supports VLAN

- IEEE 802.1Q tagged VLAN
- Up to 255 VLANs groups out of 4094 VLAN IDs
- Provider bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
- Private VLAN Edge (PVE)
- Protocol-based VLAN
- MAC-based VLAN
- Voice VLAN

Supports STP

- STP, IEEE 802.1D Spanning Tree Protocol
- RSTP, IEEE 802.1w Rapid Spanning Tree Protocol
- MSTP, IEEE 802.1s Multiple Spanning Tree Protocol, spanning tree by VLAN
- BPDU Guard

Supports link aggregation

- IEEE 802.3ad Link Aggregation Control Protocol (LACP)
- Cisco ether-channel (static trunk)
- Maximum five trunk groups, up to eight ports per trunk group
- Up to 8 Gbps bandwidth (duplex mode)

Provides port mirror (many-to-1)

Port mirroring to monitor the incoming or outgoing traffic on a particular port

Loop protection to avoid broadcast loops

Compatible with Cisco Uni-directional link detection (UDLD) which monitors a link between two switches and blocks the ports on both ends of the link if the link fails at any point between the two devices

Layer 3 IP routing features

- Supports a maximum of 32 static routes and route summarization.

Quality of Service

- Ingress shaper and egress rate limit per port bandwidth control
- Eight priority queues on all switch ports
- Traffic classification:

  - IEEE 802.1p CoS
  - TOS / DSCP / IP Precedence of IPv4/IPv6 packets
  - IP TCP/UDP port number
  - Typical network application
- Strict priority and Weighted Round Robin (WRR) CoS policies
- Supports QoS and In/Out bandwidth control on each port
- Traffic-policing policies on the switch port
- DSCP remarking

Multicast

- Supports IGMP snooping v1, v2, and v3
- Supports MLD snooping v1 and v2
- Querier mode support
- IGMP snooping port filtering
- MLD snooping port filtering
- Multicast VLAN Registration (MVR) support

Security

- Authentication
  - IEEE 802.1x Port-Based / MAC-Based network access authentication
  - Built-in RADIUS client to co-operate with the RADIUS servers
  - TACACS+ login users access authentication
  - RADIUS / TACACS+ users access authentication
- IP-based Access Control List (ACL)
  - MAC-based ACL
- Source MAC / IP address binding
- DHCP snooping to filter distrusted DHCP messages
- Dynamic ARP inspection discards ARP packets with invalid MAC addresses to IP address binding.
- IP source guard prevents IP spoofing attacks.
- Auto DoS rule to defend against DoS attacks.
- IP address access management to prevent unauthorized intruders.

Management

- IPv4 and IPv6 dual stack management
- Switch management interfaces:

  - Console / Telnet Command Line Interface
  - Web switch management
  - SNMP v1 and v2c switch management
  - SSH / SSL and SNMP v3 secure access
- IPv6 IP address/NTP/DNS management
- Built-in Trivial File Transfer Protocol (TFTP) client
- System maintenance
  - Firmware upload/download via HTTP / TFTP
  - Reset button for system reboot or reset to factory default
- BOOTP and DHCP for IP address assignment
- DHCP relay
- DHCP Option 82
- DHCP server
- User privilege levels control
- NTP (Network Time Protocol)
- Link Layer Discovery Protocol (LLDP) and LLDP-MED
- Network diagnostic
  - Cable diagnostic technology provides the mechanism to detect and report potential cabling issues
- SMTP/Syslog remote alarm
- Four RMON groups (history, statistics, alarms and events)
- IPv6 IP Address / NTP / DNS management and ICMPv6
- SNMP trap for interface Linkup and Linkdown notification
- System Log

Product specifications

Model Name	**NS3502-8P-2T-2S-V2**
Hardware Specifications	
Copper Ports	10 10/100/1000BASE-T RJ45 Auto-MDI/MDI-X ports
SFP/mini-GBIC slots	2 x 100/1000BASE-X SFP interfaces with Port-11 to Port-12 Supports 100/1000Mbps dual mode and DDM
PoE Injector Port	Eight ports with 802.3at/af PoE injector function with Port-1 to Port-8
Console	1 x RJ45 serial port (115200, 8, N, 1)

Switch Architecture	Store-and-Forward
Switch Fabric	24 Gbps / non-blocking
Throughput	17.76 Mpps @ 64 bytes
Address Table	8K entries, automatic source address learning and aging
Shared Data Buffer	1392 KB
Flow Control	IEEE 802.3x pause frame for full-duplex Back pressure for half-duplex
Jumbo Frame	9K bytes
Reset Button	< 5 seconds: System reboot > 5 seconds: Factory Default
LED	**System:** Fan Alert (Red) SYS (Green) PWR (Green) **10/100/1000T RJ45 interfaces (Port 1 to Port 8):** PoE in-use (Orange) 10/100/1000 Mbps LNK/ACT (Green) **10/100/1000T RJ45 interfaces (Port 9 to Port 10):** 1000 Mbps (Orange) LNK/ACT (Green) **100/1000 Mbps SFP combo interfaces (Port 11 to Port 12):** 1000 Mbps (Orange) LNK/ACT (Green)
Dimensions	330 x 200 x 43.5 mm, 1U height
Weight	2 kg
Power Requirement	100~240 VAC, 50/60Hz
Power Consumption	320 W/1091.9 BTU (max.)
ESD Protection	6K VDC
Power over Ethernet	
PoE Standard	IEEE 802.3af/802.3at PoE
PoE Power Supply Type	End-span
PoE Power Output	Per port 56 VDC, max. 30 W
Power Pin Assignment	1/2(+), 3/6(-)
PoE Power Budget	240 W (max.) @ 25°C 200 W (max.) @ 50°C

Max. number of Class 2 PD	8
Max. number of Class 3 PD	8
Max. number of Class 4 PD	8
Layer 2 Functions	
Port Configuration	Port disable / enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Flow control disable/enable
Port Status	Display each port's speed duplex mode, link status, flow control status, auto-negotiation status, trunk status.
Port Mirroring	TX / RX / both Many-to-1 monitor
VLAN	802.1Q tagged-based VLAN, up to 255 VLAN groups Q-in-Q tunneling Private VLAN Edge (PVE) MAC-based VLAN Protocol-based VLAN Voice VLAN MVR (Multicast VLAN Registration) Up to 255 VLAN groups, out of 4094 VLAN IDs
Link Aggregation	IEEE 802.3ad LACP/static trunk Six groups with four ports per trunk
QoS	Traffic classification based, strict priority and WRR 8-level priority for switching – Port number – 802.1p priority – 802.1Q VLAN tag – DSCP/ToS field in IP packet
IGMP Snooping	IGMP (v1/v2/v3) snooping, up to 255 multicast groups IGMP querier mode support
MLD Snooping	MLD (v1/v2) snooping, up to 255 multicast groups MLD querier mode support
Access Control List	IP-based ACL / MAC-based ACL Up to 256 entries
Bandwidth Control	Per port bandwidth control – Ingress: 500 Kbps~80 Mbps – Egress: 64 Kbps~80 Mbps
Layer 3 Functions	
IP Interface	Max. eight VLAN interfaces

Routing Table	Max. 32 routing entries
Routing Protocols	IPv4 software static routing IPv6 software static routing
Switch Management	
Basic Management Interfaces	Console; Telnet; Web browser; SNMP v1, v2c
Secure Management Interfaces	SSH, SSL, SNMP v3
SNMP MIBs	RFC 1213 MIB-II IF-MIB RFC 1493 Bridge MIB RFC 1643 Ethernet MIB RFC 2863 Interface MIB RFC 2665 Ether-Like MIB RFC 2737 Entity MIB RFC 2819 RMON MIB (Groups 1, 2, 3 and 9) RFC 2618 RADIUS Client MIB RFC 3411 SNMP-Frameworks-MIB IEEE 802.1X PAE LLDP MAU-MIB
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Stability Testing	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/100BASE-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging IEEE 802.1X Port Authentication Network Control IEEE 802.1ab LLDP IEEE 802.3af Power over Ethernet IEEE 802.3at Power over Ethernet Plus RFC 768 UDP RFC 793 TFTP RFC 791 IP

	RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2 RFC 3376 IGMP version 3 RFC 2710 MLD version 1 FRC 3810 MLD version 2
Environment	
Operating	Temperature: 0 to 50°C Relative Humidity: 5 to 95% (non-condensing)
Storage	Temperature: -10 to 70°C Relative Humidity: 5 to 95% (non-condensing)

Chapter 2
Installation

This section describes the hardware features of the managed switch. For easier management and control of the managed switch, familiarize yourself with its display indicators and ports. Front panel illustrations in this chapter display the unit LED indicators. Please read this chapter completely before connecting any network device to the managed switch,.

Hardware description

The managed switch provides three different running speeds – 10Mbps, 100Mbps, and 1000Mbps, and automatically distinguishes the speed of the incoming connection.

Front panel

Gigabit TP interface

10/100/1000BASE-T copper, RJ45 twisted-pair: Up to 100 meters.

SFP slots

100/1000BASE-X mini-GBIC slot, SFP (Small Factor Pluggable) transceiver module: From 550 meters (multi-mode fiber) to up to 10/30/50/70/120 kilometers (single-mode fiber).

Reset button

Located on the front panel near the console port, the reset button is designed to reboot the managed switch without turning the power off and on. The following is the summary table of the reset button functions:

Reset button pressed and released	Function
< 5 seconds: System reboot	Reboots the managed switch
> 5 seconds: Factory default	Resets the managed switch to factory default configuration. The switch then reboots and loads the default settings as shown below: Default Username: **admin** Default Password: **admin** Default IP address: **192.168.0.100** Subnet mask: **255.255.255.0** Default Gateway: **192.168.0.254**

LED indicators

The front panel LEDs indicate port link status, fan status, PoE-in-use, data activity, and system power.

System

LED	Color	Function
Fan Alert	Red	**Lit**: indicates that the fan is not working.
SYS	Green	**Lit:** indicates that the system is working. **Off**: indicates that the system is booting.
PWR	Green	**Lit**: indicates that the switch has power.

Per 10/100/1000BASE-T PoE+ port

LED	Color	Function
LNK/ACT	Green	**Lit**: indicates the port has successfully connected to the network. **Blinking**: indicates that the switch is actively sending or receiving data over that port.
PoE in use	Orange	**Lit**: indicates the port is providing 54 VDC in-line power. **Off**: indicates that the connected device is not a PoE powered device (PD).

10/100/1000BASE-T interfaces (Port 9 to Port 10)

LED	Color	Function
LNK/ACT	Green	**Lit**: indicates the port has successfully connected to the network. **Blinking**: indicates that the switch is actively sending or receiving data over that port.

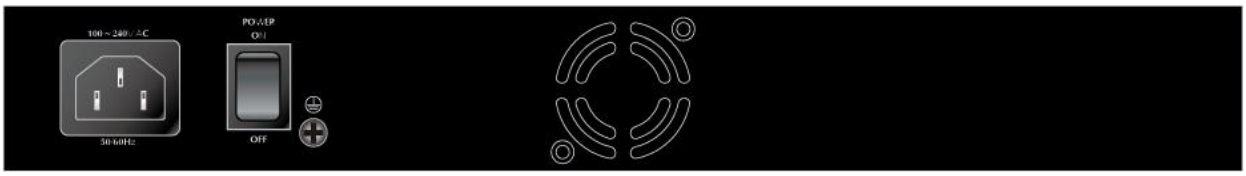
1000	Orange	**Lit**: indicates the port is operating at 1000 Mbps. **Off**: If LNK/ACT LED is lit, it indicates that the port is operating at 10/100 Mbps. If LNK/ACT LED is off, it indicates that the port is link-down.

10/100/1000BASE-X SFP interfaces (Port 11 to Port 12)

LED	Color	Function
LNK/ACT	Green	**Lit**: indicates the port has successfully connected to the network. **Blinking**: indicates that the switch is actively sending or receiving data over that port.
1000	Orange	**Lit**: indicates the port has successfully connected to the network at 1000 Mbps. **Off**: If LNK/ACT LED is lit, it indicates that the port is operating at 100 Mbps. If LNK/ACT LED is off, it indicates that the port is link-down.

Switch rear panel

The rear panel of the managed switch contains an AC inlet power socket and power on/off switch.



AC power receptacle

For compatibility with electrical supplies in most areas of the world, the managed switch's power supply automatically adjusts to line power in the range of 100-240 VAC and 50/60 Hz.

Plug the female end of the power cord firmly into the receptacle on the rear panel of the managed switch and the other end of the power cord into an electrical outlet and then power it on.

Note: The device is a power-required device, meaning it will not work until it is powered on. If your network needs to be active at all times, consider using a UPS (Uninterrupted Power Supply) for the device to help to prevent network data loss or network downtime. In some areas, installing a surge suppression device may also help to protect the managed switch from an unregulated surge or current to the switch or the power adapter.

Installing the switch

This section describes how to install and make connections to the managed switch. Read the following topics and perform the procedures in the order presented.

To install the managed switch on a desktop or shelf:

1. Attach the rubber feet to the recessed areas on the bottom of the managed switch.
2. Place the managed switch on the desktop or the shelf near an AC power source, as shown below:

3. Keep enough ventilation space between the managed switch and the surrounding objects.

   Note: When choosing a location, please keep in mind the environmental restrictions indicated in “Product specifications” on page 14.

4. Connect one end of a standard network cable to the 10/100/1000 RJ45 ports on the front of the managed switch and the other end of the cable to the network devices such as printer servers, workstations or routers.

   Note: Connection to the managed switch requires UTP Category 5 network cabling with RJ45 tips. For more information, see Appendix A “Networking connection” on page 468.

5. Connect one end of the power cable to the managed switch.
6. Connect the power plug of the power cable to a standard wall outlet.
7. When the managed switch receives power, the power LED illuminates solid green.

Rack mounting

To install the managed switch in a 19-inch standard rack:

1. Place the managed switch on a hard, flat surface with the front panel positioned towards the front side.
2. Attach the rack-mount bracket to each side of the managed switch with the supplied screws as shown below.

Caution: You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws will invalidate the warranty.

3. Secure the brackets tightly.
4. Follow the same steps to attach the second bracket to the opposite side.
5. After the brackets are attached to the managed switch, use suitable screws to securely attach the brackets to the rack, as shown below.

6. Follow steps 4 through 7 under “To install the managed switch on a desktop or shelf” in this section to connect the network cabling and supply power to the managed switch.

Cabling

10/100/1000BASE-T and 100BASE-FX/1000BASE-SX/LX

All 10/100/1000BASE-T ports come with auto-negotiation capability. They automatically support 1000BASE-T, 100BASE-TX, and 10BASE-T networks. Users only need to plug a working network device into one of the 10/100/1000BASE-T ports, and then turn on the managed switch. The port will automatically run in 10 Mbps, 20 Mbps, 100 Mbps, or 200 Mbps, and 1000 Mbps or 2000 Mbps after negotiating with the connected device.

The managed switch has eight SFP interfaces that support 100/1000 Mbps dual speed mode (optional multi-mode/single-mode 100BASE-FX/1000BASE-SX/LX SFP module)

Cabling

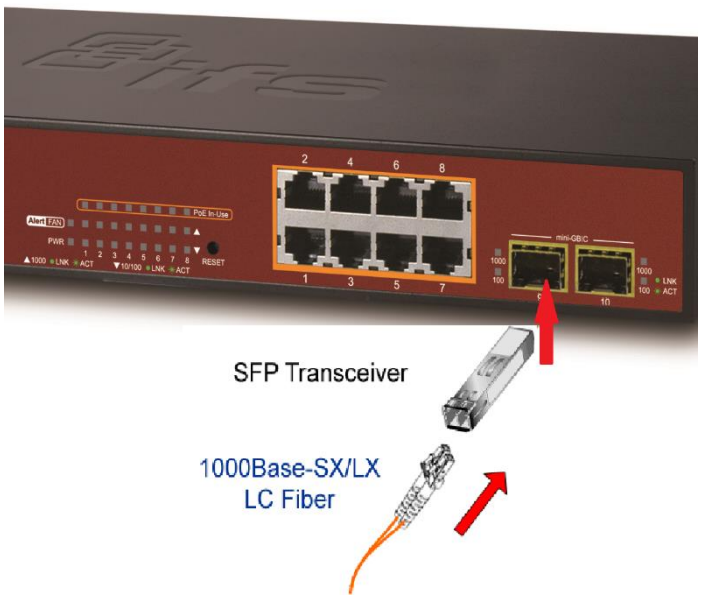
Each 10/100/1000BASE-T port uses an RJ45 socket (similar to phone jacks) for connection of unshielded twisted-pair cable (UTP). The IEEE 802.3/802.3u 802.3ab Fast/Gigabit Ethernet standard requires Category 5 UTP for 100 Mbps 100BASE-TX. 10BASE-T networks can use Cat.3, 4, 5, or 1000BASE-T use 5/5e/6 UTP (see table below). Maximum distance is 100 meters (328 feet). The 100BASE-FX/1000BASE-SX/LX SFP slot uses an LC connector with optional SFP module. The table below provides cable specification details.

Port Type	Cable Type	Connector
10BASE-T	Cat3, 4, 5, 2-pair	RJ45
100BASE-TX	Cat5 UTP, 2-pair	RJ45
1000BASE-T	Cat5/5e/6 UTP, 2-pair	RJ45
100BASE-FX	50/125 µm or 62.5/125 µm multi-mode 9/125 µm single-mode	LC (multi/single mode)
1000BASE-SX/LX	50/125 µm or 62.5/125 µm multi-mode 9/125 µm single-mode	LC (multi/single mode)

Ethernet devices like hubs and PCs can connect to the managed switch by using straight-through wires. The two 10/100/1000Mbps ports are auto-MDI/MDI-X and can be used on straight-through or crossover cable.

Installing the SFP/SFP+ transceiver

SFP transceivers are hot-pluggable and hot-swappable. They can be plugged in and removed to/from any SFP port without having to power down the managed switch (see below).



Approved IFS SFP transceivers

The managed switch supports both single mode and multi-mode SFP transceivers. The following list of approved IFS SFP transceivers is valid as of the time of publication:

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivity (dBm)	Operating Temperature
Twisted Pair SFP 1000Base TX									
S30-RJ	RJ 45	1	Cat5e	100M (328 ft.)					0 to +50°C (32 to 122°F)
Fast Ethernet 100Base FX									
S20-2MLC2	LC	2	Multi-mode	2 km (1.2 mi.)	1310 nm	12	-20 ~ -14	-32	0 to +50°C (32 to 122°F)
S25-2MLC2	LC	2	Multi-mode	2 km (1.2 mi.)	1310 nm	12	-20 ~ -14	-32	-40 to +75°C (-40 to 167°F)
Fast Ethernet 100Base LX									
S20-2SLC20	LC	2	Single Mode	20 km (12 mi.)	1310 nm	19	-15 ~ -8	-34	0 to +50°C (32 to 122°F)
S25-2SLC20	LC	2	Single Mode	20 km (12 mi.)	1310 nm	19	-15 ~ -8	-34	-40 to +75°C (-40 to 167°F)
Fast Ethernet 100Base BX									
S20-1SLC/A-20	LC	1	Single Mode	20 km (12 mi.)	1310 / 1550 nm	18	-14 ~ -8	-32	0 to +50°C (32 to 122°F)
S25-1SLC/B-20	LC	1	Single Mode	20 km (12 mi.)	1550 / 1310 nm	18	-14 ~ -8	-32	-40 to +75°C (-40 to 167°F)
Gigabit Ethernet 1000Base SX									
S30-2MLC	LC	2	Multi-mode	220/550 m (720 / 1800 ft.)	850 nm	7.5	-9.5 ~ -1	-17	0 to +50°C (32 to 122°F
S35-2MLC	LC	2	Multi-mode	220/550 m (720 / 1800 ft.)	850 nm	7.5	-14 ~ -8	-17	-40 to +75°C (-40 to 167°F)
OM1 Multimode fiber @ 200/500 MHz-km OM2 Multimode fiber @ 500.500 MHZ-km Laser Rated for GbE LANs									
S30-2MLC-2	LC	2	Multi-mode	2 km (1.2 mi.)	1310 nm	10	-9 ~ -1	-19	0 to +50°C (32 to 122°F)
OM3 Multimode fiber @ 2000/500MHz-km Optimized got 850 nm VCSELs									
Gigabit Ethernet 1000 Base LX									
S30-2SLC-10	LC	2	Single Mode	10 km (6.2 mi.)	1310 nm	18	-9.5 ~ -3	-20	0 to +50°C (32 to 122°F)
S35-2SLC-10	LC	2	Single Mode	10 km (6.2 mi.)	1310 nm	18	-9.5 ~ -3	-20	-40 to +75°C (-40 to 167°F)
S30-2SLC-30	LC	2	Single Mode	30 km (18.6 mi.)	1310 nm	18	-2 ~ +3	-23	0 to +50°C (32 to 122°F)

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivity (dBm)	Operating Temperature
S35-2SLC-30	LC	2	Single Mode	30 km (18.6 mi.)	1310 nm	18	-2 ~ +3	-23	-40 to +75°C (-40 to 167°F)
Gigabit Ethernet 1000 Base ZX									
S30-2SLC-70	LC	2	Single Mode	70 km (43 mi.)	1550 nm	19*	-15 ~ -8	-34	0 to +50°C (32 to 122°F)
S35-2SLC-70	LC	2	Single Mode	70 km (43 mi.)	1550 nm	19*	-15 ~ -8	-34	-40 to +75°C (-40 to 167°F)
Gigabit Ethernet 1000 Base BX									
S30-1SLC/A-10	LC	1	Single Mode	10 km (6.2 mi.)	1310 / 1490 nm	11	-9 ~ -3	-20	0 to +50°C (32 to 122°F)
S30-1SLC/B-10	LC	1	Single Mode	10 km (6.2 mi.)	1490 / 1310 nm	11	-9 ~ -3	-20	0 to +50°C (32 to 122°F)
S30-1SLC/A-20	LC	1	Single Mode	20 km (12 mi.)	1310 / 1490 nm	15	-8 ~ -2	-23	0 to +50°C (32 to 122°F)
S30-1SLC/B-20	LC	1	Single Mode	20 km (12 mi.)	1490 / 1310 nm	15	-8 ~ -2	-23	0 to +50°C (32 to 122°F)
S30-1SLC/A-60	LC	1	Single Mode	60 km (37 mi.)	1310 / 1490 nm	24	0 ~ +5	-24	0 to +50°C (32 to 122°F)
S30-1SLC/B-60	LC	1	Single Mode	60 km (37 mi.)	1490 / 1310 nm	24	0 ~ +5	-24	0 to +50°C (32 to 122°F)

* Note: High Power Optic. There must be a minimum of 5 dB of optical loss to the fiber for proper operation.

Note: We recommend the use of IFS SFPs on the managed switch. If you insert an SFP transceiver that is not supported, the managed switch will not recognize it.

Note: Choose a SFP transceiver that can be operated under -40 to 75°C temperature if the managed switch is working in a 0 to 50°C temperature environment.

1000Base-SX/LX

Before connecting other switches, workstation, or media converter:

1. Make sure both sides of the SFP transceiver are with the same media type. For example, 1000BASE-SX to 1000BASE-SX, 1000BASE-LX to 1000BASE-LX.
2. Check if the fiber-optic cable type matches the SFP transceiver requirement.
   - To connect to 1000BASE-SX SFP transceiver, use the multi-mode fiber cable with one side being male duplex LC connector type.
   - To connect to 1000BASE-LX SFP transceiver, use the single-mode fiber cable with one side being male duplex LC connector type.

To connect the fiber cable:

1. Attach the duplex LC connector on the network cable to the SFP transceiver.
2. Connect the other end of the cable to a device with the SFP transceiver installed.
3. Check the LNK/ACT LED of the SFP slot on the front of the managed switch. Ensure that the SFP transceiver is operating correctly.

100Base-FX

Before connecting other switches, workstation, or media converter:

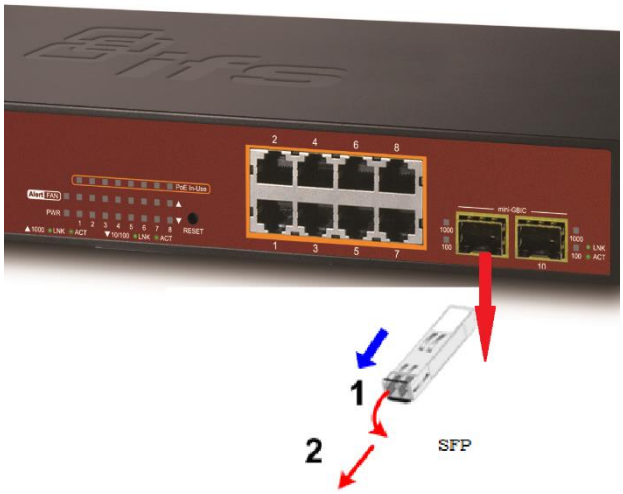
1. Make sure both sides of the SFP transceiver are with the same media type. For example, 100BASE-FX to 100BASE-FX, 100BASE-BX-20-U to 100BASE-BX-20-D.
2. Check if the fiber-optic cable type matches the SFP transceiver requirement.
   - To connect to a SFP transceiver, use the multi-mode fiber cable with one side being male duplex LC connector type.
   - To connect to a SFP transceiver, use the single-mode fiber cable with one side being male duplex LC connector type.

To connect the fiber cable:

1. Attach the duplex LC connector on the network cable to the SFP transceiver.
2. Connect the other end of the cable to a device with the SFP transceiver installed.
3. Check the LNK/ACT LED of the SFP slot on the front of the managed switch. Ensure that the SFP transceiver is operating correctly.
4. Check the link mode of the SFP port if the link fails. Set the link mode to “100-Force” if required.

To remove the transceiver module:

1. Make sure there is no network activity by checking with the network administrator. Or, through the management interface of the switch/converter (if available), disable the port in advance.
2. Carefully remove the fiber optic cable.
3. Turn the lever of the transceiver module to a horizontal position.
4. Pull out the module gently through the lever.



Note: Never pull out the module without making use of the lever or the push bolts on the module. Removing the module with force could damage the module and the SFP module slot of the managed switch.

Chapter 3
Switch management

This chapter explains the methods that can be used to configure management access to the managed switches. It describes the types of management applications and the communication and management protocols that deliver data between the management device (workstation or personal computer) and the system. It also contains information about port connection options.

Requirements

- Workstations must have Windows XP or later, Mac OS9 or later, Linux, Fedora, Ubuntu , or other platforms compatible with TCP/IP protocols.
- Workstations must have an Ethernet NIC (Network Interface Card) installed.
- Ethernet port connection. Use standard network (UTP) cables with RJ45 connectors.
- Workstations must have a web browser and Java runtime environment plug-in installed.

Note: We recommend the use of Internet Explorer 11.0 or later to access the managed switch.

Management access overview

The managed switch provides the flexibility to access and manage it using any or all of the following methods:

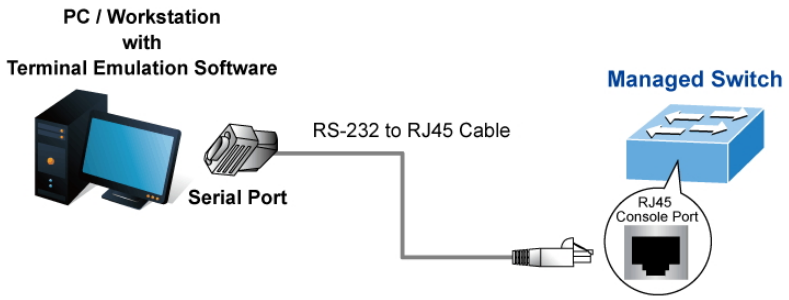
- Remote Telnet interface
- Web browser interface
- An external SNMP-based network management application

The administration console and web browser interface support are embedded in the managed switch software and are available for immediate use. The advantages of these management methods are described below:

Method	Advantages	Disadvantages
Console	• No IP address or subnet needed. • Text-based • Telnet functionality and HyperTerminal built into Windows operating systems. • Secure	• Must be near the switch or use dial-up connection. • Not convenient for remote users. • Modem connection may prove to be unreliable or slow.
Web browser	• Ideal for configuring the switch remotely. • Compatible with all popular browsers. • Can be accessed from any location. • Most visually appealing.	• Security can be compromised (hackers need only know the IP address and subnet mask). • May encounter lag times on poor connections.
SNMP agent	• Communicates with switch functions at the MIB level. • Based on open standards.	• Requires SNMP manager software • Least visually appealing of all three methods. • Some settings require calculations. • Security can be compromised (hackers need to only know the community name).

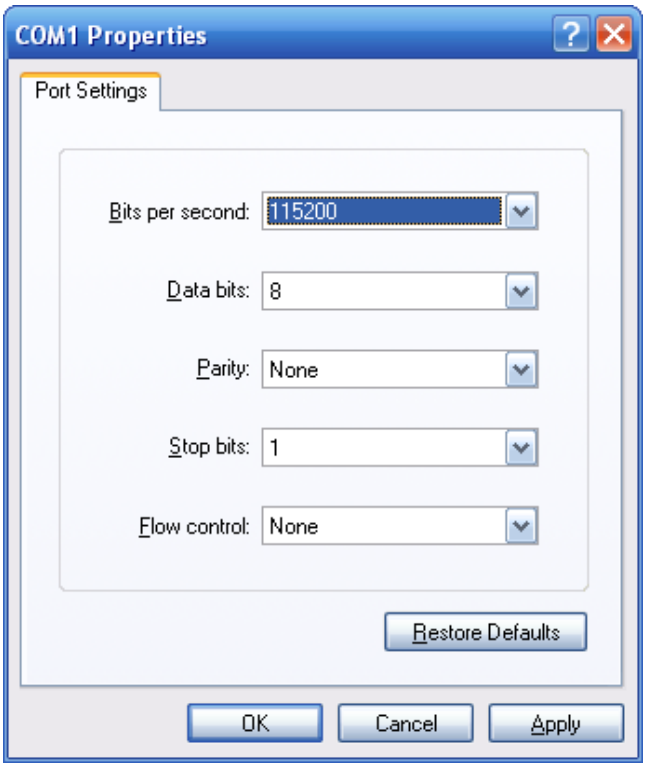
Administration console

The administration console is an internal, character-oriented, and command line user interface for performing system administration such as displaying statistics or changing option settings. Using this method, you can view the administration console from a terminal, a computer, or workstation connected to the managed switch's console (serial) port.



Direct access

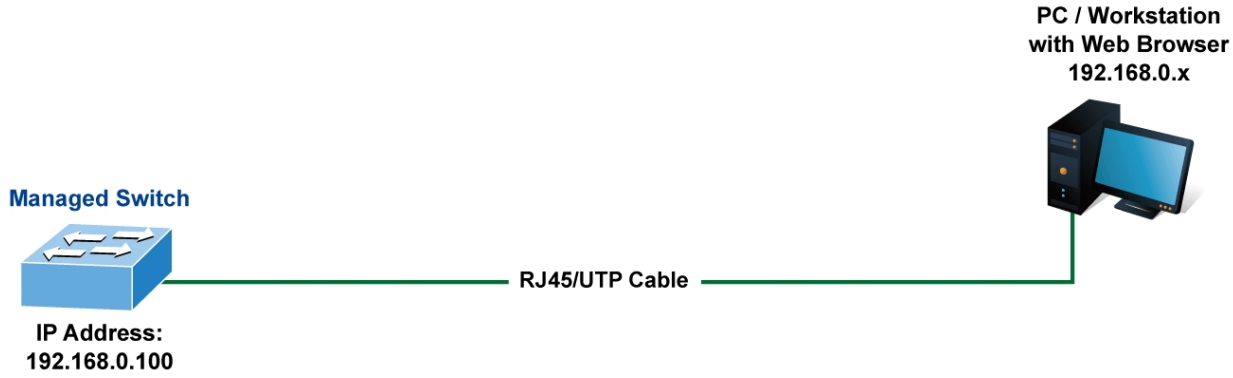
Direct access to the administration console is achieved by directly connecting a terminal or a computer equipped with a terminal-emulation program (such as HyperTerminal) to the managed switch console (serial) port. When using this management method, a straight DB9 RS-232 cable is required to connect the switch to the computer. After making this connection, configure the terminal-emulation program to use the following parameters:



These settings can be changed after log on, if required. This management method is often preferred because the user can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A computer attachment can use any terminal emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

Web management

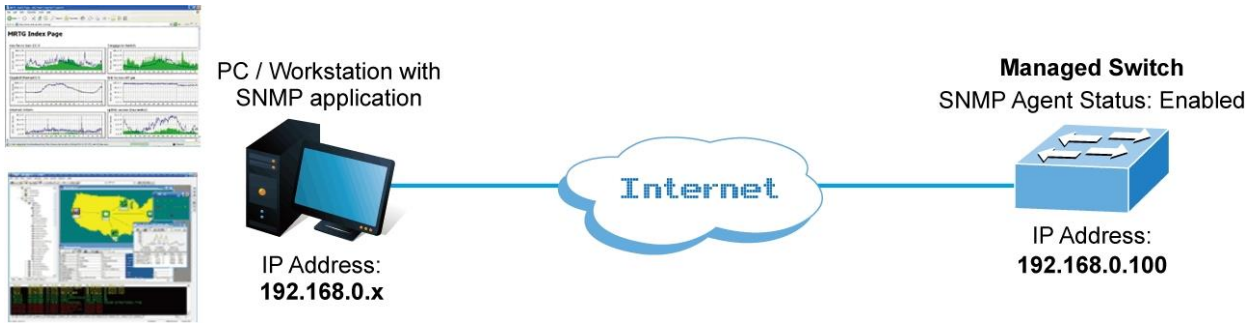
The managed switch provides features that allow users to manage it from anywhere on the network through a standard browser such as Microsoft Internet Explorer. After setting up the IP address for the switch, you can access the managed switch's web interface applications directly in the web browser by entering the IP address of the managed switch.



You can use a web browser to list and manage the managed switch configuration parameters from one central location, just as if you were directly connected to the managed switch's console port. Web management requires Microsoft Internet Explorer 11.0 or later.

SNMP-based network management

Use an external SNMP-based application to configure and manage the managed switch, such as SNMP Network Manager, HP Openview Network Node Management (NNM), or What's Up Gold. This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the same community string. This management method uses two community strings: the get community string and the set community string. If the SNMP Network Management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default get and set community strings for the managed switch are public.



Chapter 4
Web configuration

This section introduces the configuration and functions of the web-based management interface for the managed switch.

About web-based management

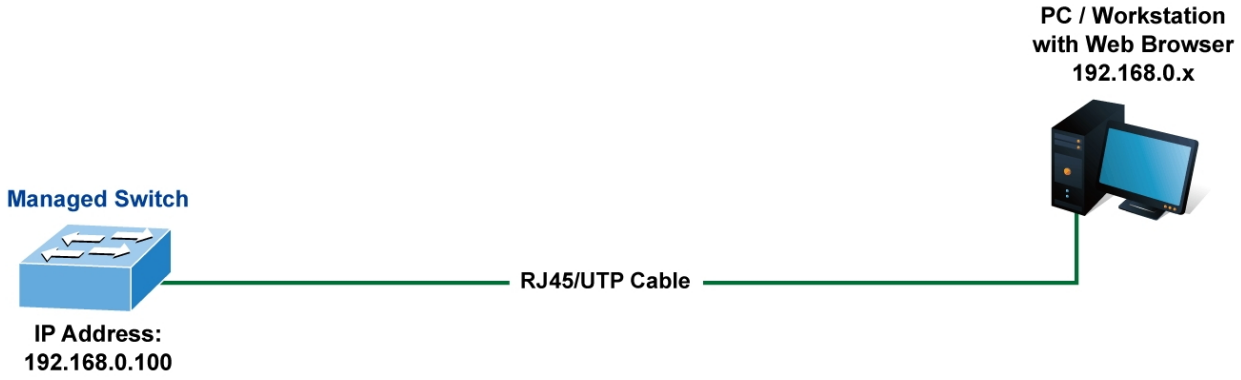
Web-based management of the managed switches supports Internet Explorer 11.0 or later, and can be performed from any location on the network. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed, and present an easy viewing screen.

Note: By default, IE 11.0 and above does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

The managed switches can be configured through an Ethernet connection when the manager computer is set to the same IP subnet address as the managed switch.

For example, if the default IP address of the managed switch is 192.168.0.100, then the administrator computer should be set at 192.168.0.x (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

If the default IP address of the managed switch has been changed to 192.168.1.1 with subnet mask 255.255.255.0 via the console, then the administrator computer should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on a manager computer.

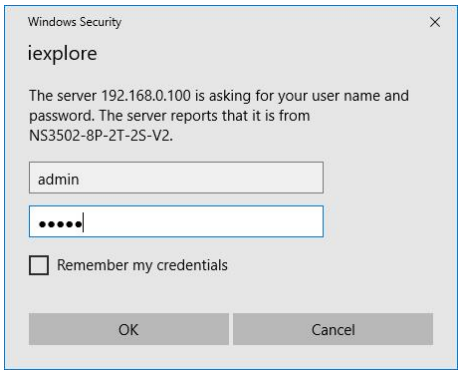


To log into the managed switch for the first time:

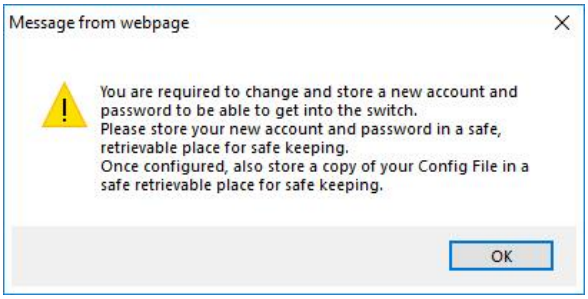
1. Launch the Internet Explorer 11.0 or later web browser and type the factory default IP address **http://192.168.0.100** to access the web interface.

   Note: Before connecting to a TruVision Navigator video surveillance system network, the default IP address must be changed to the IP address assigned for TruNav by the network administrator.

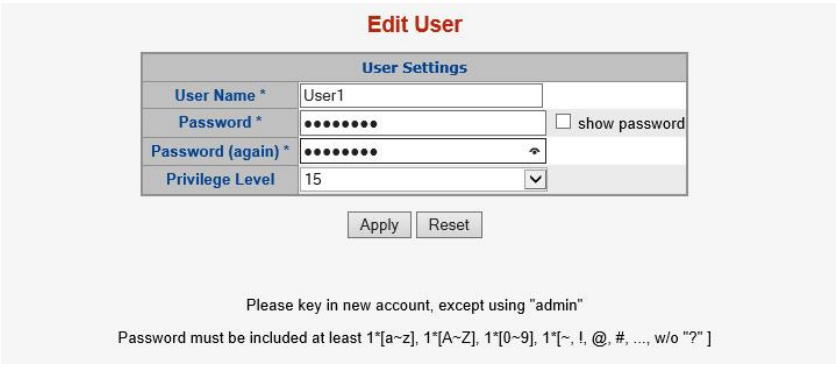
2. When the following login screen appears, type the default username "**admin**" with password "**admin**" and click **OK**.



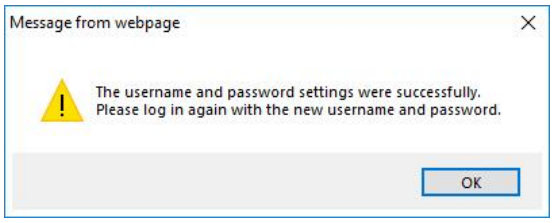
3. Click **OK** to begin the process of changing the default username and password.



4. Type a new username and password in the Edit User page, following the guidelines as shown. Click **Apply**.



5. When the success window appears, click **OK**.

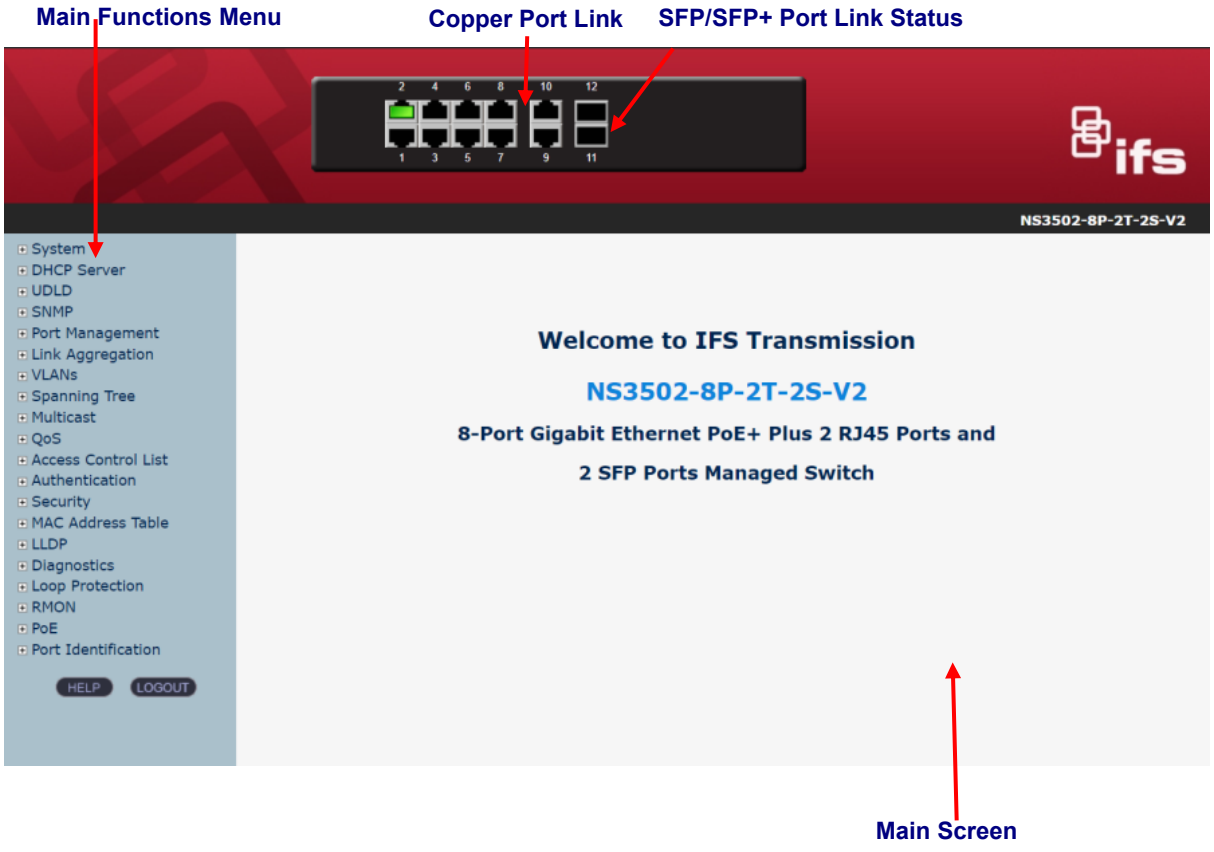


6. After typing the new username and password in the login window, the main UI screen appears. The main menu on the left side of the web page permits access to all the functions and status provided by the managed switch.

Note: For added security, a logged in user is automatically logged out after five minutes of inactivity.

Main web page

This section describes how to use the managed switch's web browser interface for configuration and management.



Panel display

The web interface displays an image of the managed switch's ports. The mode can be set to display different information for the ports, including Link up or Link down. Clicking on the image of a port opens the Port Statistics page.

Port status is indicated as follows:

State	Disabled	Down	Link
RJ45 Ports			
SFP Ports			

Main menu

Using the web interface, you can define system parameters, manage, and control the managed switch and all its ports, or monitor network conditions. The administrator can set up the managed switch by making selections from the main functions menu. Clicking on a main menu item opens sub menus.

System

Use the System menu items to display and configure basic administrative details of the managed switch. Under the System list, the following topics are provided to configure and view the system information. This list contains the following items:

System information

The System Infomation page provides information on the current device such as the hardware MAC address, software version, and system uptime.

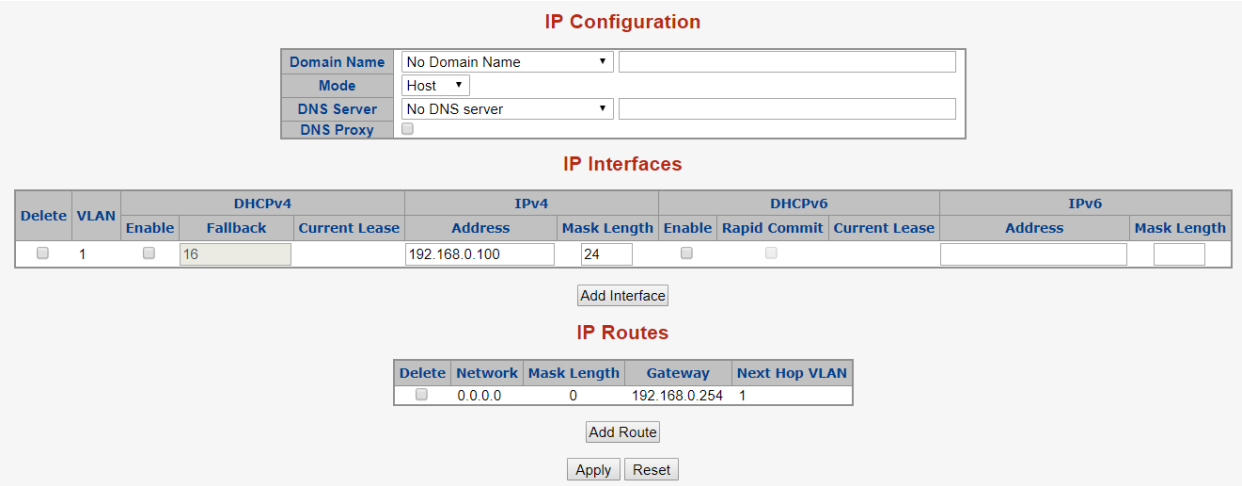
The page includes the following fields:

Item	Function
Contact	The system contact configured in SNMP > System Information.
Name	The system name configured in SNMP > System Information.
Location	The system location configured in SNMP > System Information.
MAC Address	The MAC Address of this managed switch.
Power Status	Indicates the type of power applied to the managed switch.
Temperature	Indicates chipset temperature.
System Date	The current (GMT) system time and date. The system time is obtained through the configured NTP server, if present.
System Uptime	The period of time the device has been operational.
Software Version	The software version of the managed switch.
Software Date	The date when the managed switch software was produced.

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page automatically. This will undo any changes made locally.

IP configuration

This page includes the IP Configuration, IP Interface, and IP Routes. The configured column is used to view or change the IP configuration. The maximum number of interfaces supported is 128 and the maximum number of routes is 32.



The current column is used to show the active IP configuration.

Object		Description
IP Configurations	**Mode**	Set the IP stack to 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.
	Domain Name	The name string of local domain where the device belongs. Most queries for names within this domain can use short names relative to the local domain. The system then appends the domain name as a suffix to unqualified names. For example, if the domain name is set as 'example.com' and you specify the PING destination by the unqualified name as 'test', then the system will qualify the name to be 'test.example.com'. The following modes are supported: **No Domain Name** – No domain name will be used. **Configured Domain Name** – Explicitly specify the name of local domain. Make sure the configured domain name meets your organization's given domain. **From any DHCPv6 interfaces** – The first domain name offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used. **From this DHCPv6 interface** – Specify from which DHCPv6-enabled interface a provided domain name should be preferred.
	DNS Server	This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. The following modes are supported: **No DNS server** – No DNS server will be used. **Configured IPv4** – Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server is reachable (e.g., via PING) for activating DNS service.

Object			Description
			Configured IPv6 – Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server. Make sure the configured DNS server is reachable (e.g., via PING6) for activating DNS service. **From any DHCPv4 interfaces** – The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used. **From this DHCPv4 interface** – Specify from which DHCPv4-enabled interface a provided DNS server should be preferred. **From any DHCPv6 interfaces** – The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used. **From this DHCPv6 interface** – Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.
	DNS Proxy		When DNS proxy is enabled, the system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.
IP Address	**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.
	DHCPv4	**Enabled**	Enable the DHCP client by selecting this check box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup
		Fallback	The number of seconds for trying to obtain a DHCP lease. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.
		Current Lease	For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.
	IPv4	**Address**	Provides the IP address of this managed switch 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 required, or if no DHCP fallback address is required
		Mask Length	The IPv4 network mask, in number of bits (*prefix length*). Valid values are between 0 and 30 bits for a 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 required, or if no DHCP fallback address is required.

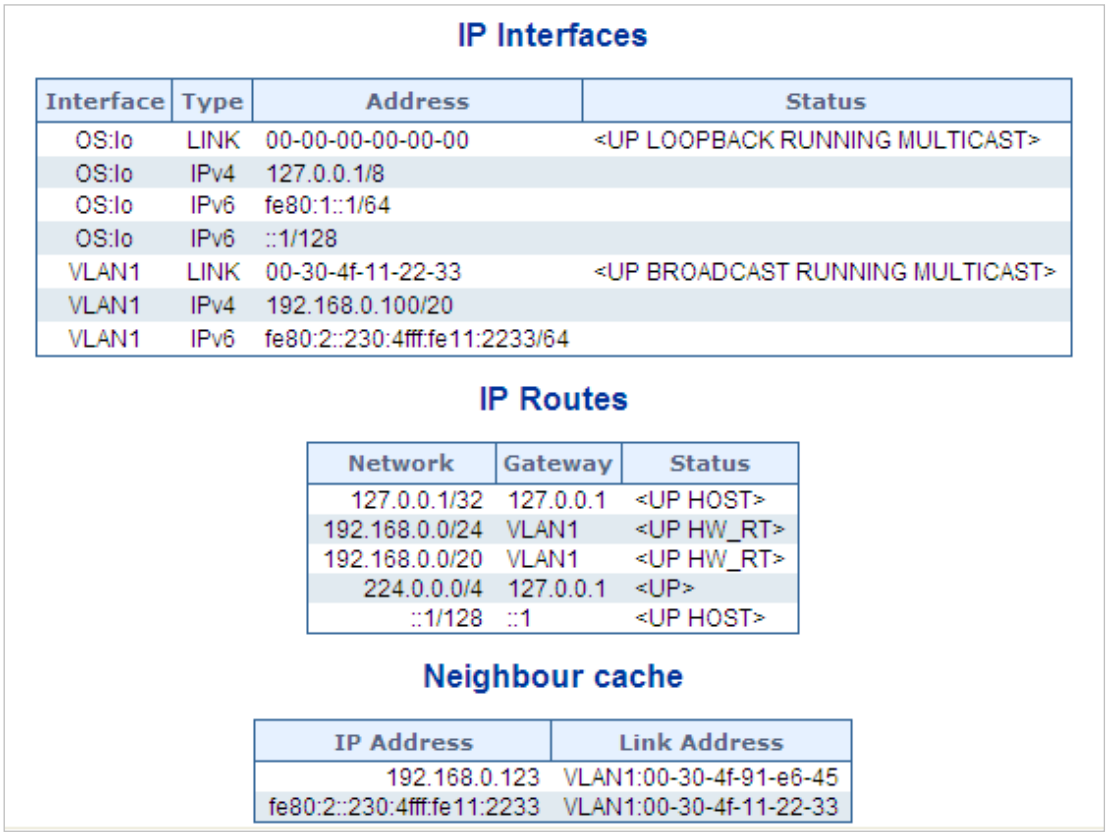
Object			Description
	DHCPv6	Enable	Enable the DHCPv6 client by selecting this check box. If this option is enabled, the system configures the IPv6 address of the interface using the DHCPv6 protocol.
		Rapid Commit	Enable the DHCPv6 Rapid-Commit option by selecting this check box. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received. This option is only manageable when the DHCPv6 client is enabled.
		Current Lease	For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.
	IPv6	Address	Provides the IP address of this managed switch. 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. The system accepts the valid IPv6 unicast address only, except the IPv4-Compatible address and IPv4-Mapped address. The field may be left blank if IPv6 operation on the interface is not required.
		Mask Length	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 required.
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 **0.0.0.0** or 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 notation or a valid IPv6 notation. Gateway and Network must be of the same type.
	Next Hop VLAN		The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4095 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, the system ignores the next hop VLAN for the gateway.

Buttons

- Click **Add Interface** to add a new IP interface. A maximum of 128 interfaces is supported.
- Click **Add Route** to add a new IP route. A maximum of 32 routes is supported.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

IP status

IP status 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	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80:1::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-30-4f-11-22-33	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.100/20	
VLAN1	IPv6	fe80:2::230:4fff:fe11:2233/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
192.168.0.0/24	VLAN1	<UP HW_RT>
192.168.0.0/20	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
192.168.0.123	VLAN1:00-30-4f-91-e6-45
fe80:2::230:4fff:fe11:2233	VLAN1:00-30-4f-11-22-33

The page includes the following fields:

Object		Description
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.
Neighbor Cache	**IP Address**	The IP address of the entry.
	Link Address	The link (MAC) address for which a binding to the IP address given exists.

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page automatically. This will undo any changes made locally.

Users configuration

This page provides an overview of the current users. Close and reopen the browser to log in as another user on the web server. After setup is complete, click the **Apply** button and log in to the web interface with the new user name and password. The following appears:

This page includes the following fields:

Object	Description
User Name	The name identifying the user. This is also a link to **Add/Edit User**.
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., it is granted full control of the device). Other values need to refer to each group privilege level. User privileges should be the same or greater than the group privilege level to have access to that group.

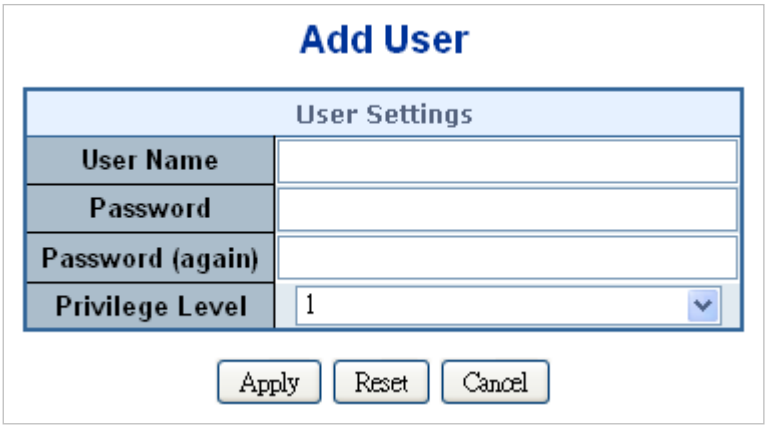
Object	Description
	By default, most groups' privilege level 5 has read-only access and privilege level 10 has read-write access. System maintenance (software upload, factory defaults, etc.) requires user privilege level 15. Generally, privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account, and privilege level 5 for a guest account.

Buttons:

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

Add/edit user

Add, edit, or delete a user in this page.



This page includes the following fields:

Object	Description
User Name	A string identifies the user name that this entry should belong to. The allowed string length is **1** to **32**. 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 **32**.
Password (again)	Type the user password again for confirmation.
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., it is granted full control of the device). But other values need to refer to each group privilege level. User privileges should be the same or greater than the group privilege level to have access to that group. By default, most groups' privilege level 5 has read-only access and privilege level 10 has read-write access. System maintenance (software upload, factory defaults, etc.) requires user privilege level 15. Generally, 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.

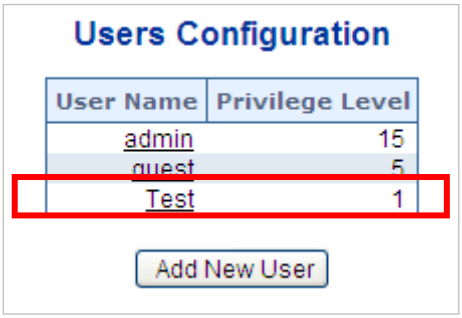
Buttons

- Click **Save** to save changes.

- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Cancel** to undo changes and return to the Users Configuration page.
- Click **Delete User** to delete the current user. This function is not available for new configurations (i.e., add new user).

Note: By default, most groups' privilege level 5 has read-only access and privilege level 10 has read-write access. System maintenance (software upload, factory defaults, etc.) requires user privilege level 15. Generally, 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.

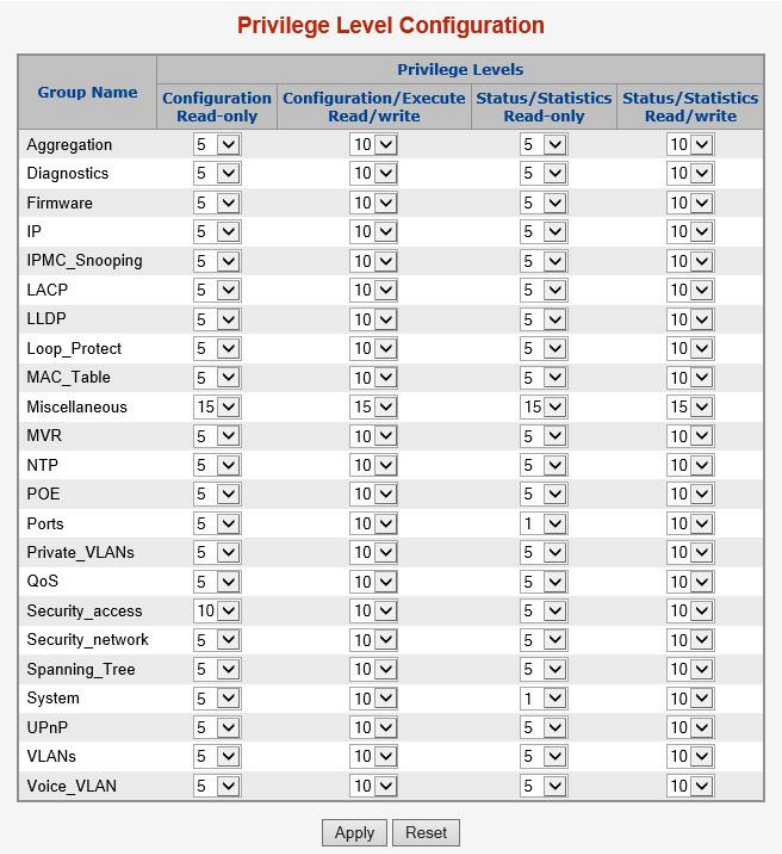
After a new user is added, the new user entry appears in the Users Configuration page.



Note: The new password must be at least eight characters and must include one lowercase letter [a~z], one uppercase letter [A~Z], one number [0~9], and one special character [~,!,@,#,...,w/o"?"]. If a password is forgotten after changing the default password, press the reset button on the front panel of the managed switch for over 10 seconds and then release it. The current settings, including VLAN, will be erased and the managed switch restores to default mode.

Privilege levels

This page provides an overview of the privilege levels. After setup is complete, click the **Save** button and log in to the web interface with the new user name and password. The following appears:



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
Diagnostics	5	10	5	10
Firmware	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Miscellaneous	15	15	15	15
MVR	5	10	5	10
NTP	5	10	5	10
POE	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
Security_access	10	10	5	10
Security_network	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
UPnP	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10

Apply Reset

This page includes the following fields:

Object	Description
Group name	The name identifies the privilege group. In most cases, a privilege level group consists of a single module (e.g., LACP, RSTP, or QoS), but a few of them contain more than one. The following description defines these privilege level groups in detail: **System**: Contact, Name, Location, Timezone, Log. **Security**: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, and 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 Level	Every privilege level group has an authorization 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)

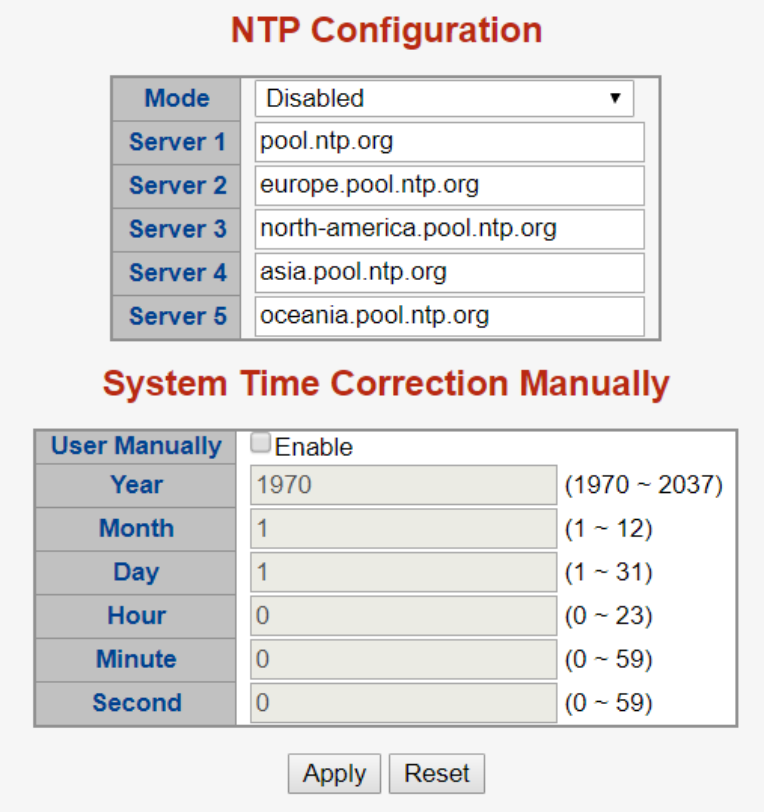
Object	Description
	User privilege should be the same or greater than the authorization privilege level to have the access to that group

Buttons

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

NTP configuration

Configure NTP on this page. NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (data grams) as a transport layer. You can specify NTP servers and GMT time zone in this page.



This page includes the following fields:

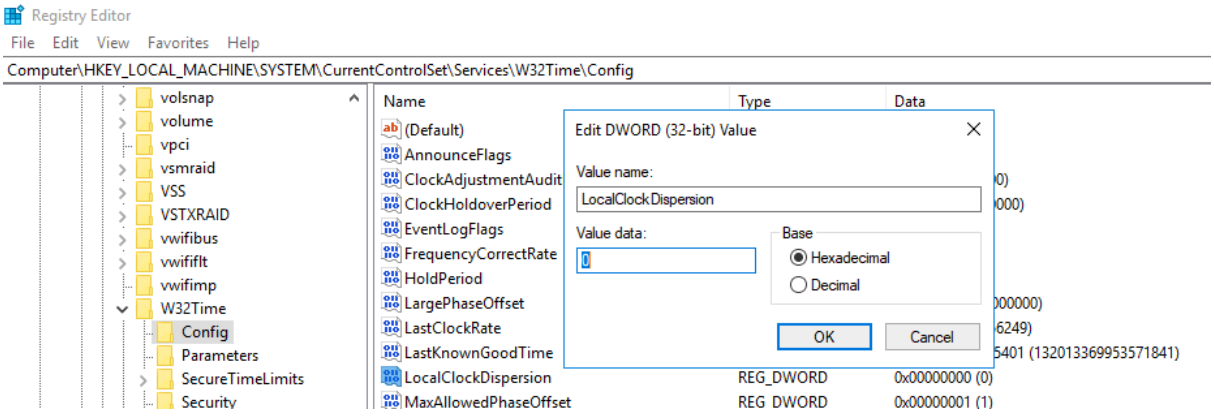
Object	Description
Mode	Indicates the NTP mode operation. Possible modes are: **Enabled**: Enable NTP mode operation. When enabling NTP mode operation, the agent forwards and transfers NTP messages between the clients and the server when they are not on the same subnet domain. **Disabled**: Disable NTP mode operation.

Object	Description
Time zone	Permits time zone selection according to current location of the switch.
Server#	Provides the NTP IPv4 or IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). **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 only appear once. It also uses an IPv4 address (for example, '::192.1.2.34').
User Manually	Indicates the NTP mode as manual operation. Possible modes are: **Enabled**: Enable NTP manual mode operation. When enabling NTP manual mode operation, the system time will follow the date setting. **Disabled**: Disable NTP manual mode operation.
Date	If user manually is enabled, the year, month, day, and hour can be set on this page.

Buttons

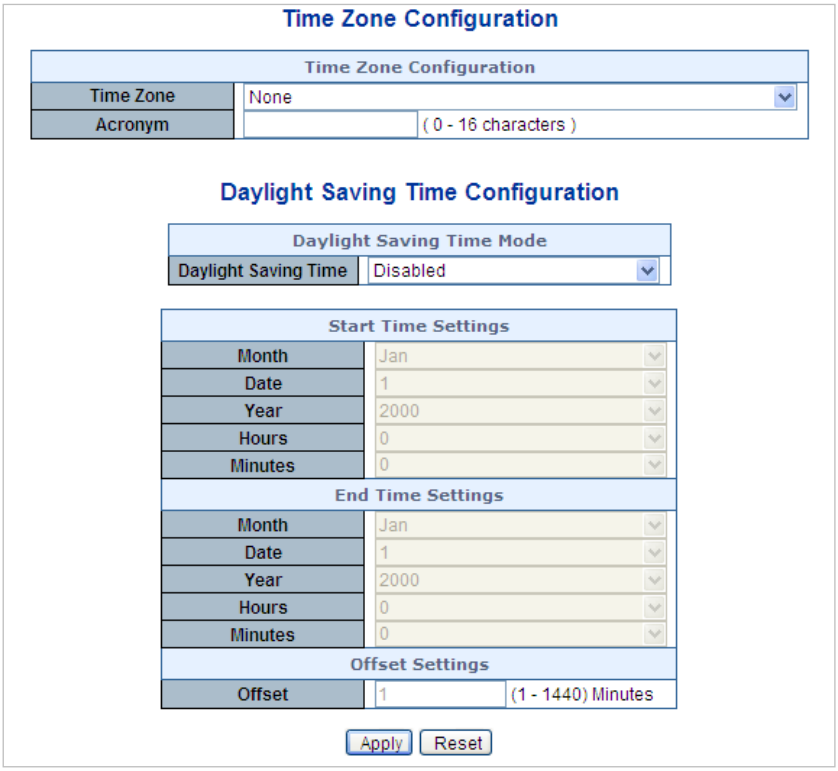
- Click **Save** to save changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Note: According to the specification of the switch chip, the value of root dispersion from the NTP server must be less than 1.5 seconds. If the value of root dispersion is over 1.5 seconds, the switch discards the packet. An internal NTP server like W32Time service in Windows 10 can be used without an internet connection. We recommend changing the value of LocalClockDispersion to 0 (default is 10).



Time configuration

A time zone is a region that has a uniform standard time for legal, commercial, and social purposes. It is convenient for areas in close commercial or other communication to maintain the same time, so time zones tend to follow the boundaries of countries and their subdivisions. Configure the time zone on the Time Zone Configuration page.



This page includes the following fields:

Object	Description
Time Zone	Lists various Time Zones worldwide. Select the appropriate Time Zone from the drop-down list and click **Save**.
Acronym	This is a user configurable acronym (up to 16 characters) used to identify the time zone.
Daylight Saving Time	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select **Disable** to disable the Daylight Saving Time configuration. Select **Recurring** and configure the Daylight Saving Time duration to repeat the configuration every year. Select **Non-Recurring** and configure the Daylight Saving Time duration for single time configuration. (Default: **Disabled**).
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	Enter the number of minutes (1 to 1440) to add during Daylight Saving Time.

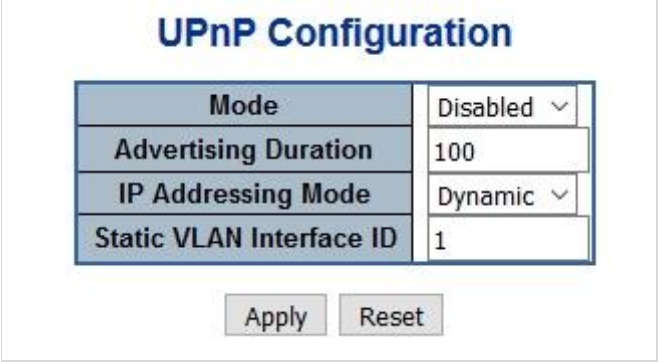
Buttons

- Click **Save** to apply changes.

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

UPnP

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in home (data sharing, communications, and entertainment) and corporate environments for easy installation of computer components. Configure UPnP on the UPnP Configuration page.



This page includes the following fields:

Object	Description
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 the CPU. The ACEs are automatically removed when the mode is disabled.
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 a 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.
IP Address Mode	IP addressing mode provides two ways to determine IP address assignment: **Dynamic**: Default selection for UPnP. UPnP module helps users choosing the IP address of the switch device. It finds the first available system IP address. **Static**: The user specifies the IP interface VLAN for choosing the IP address of the switch device.
Static VLAN Interface ID	The index of the specific IP VLAN interface. It will only be applied when IP Addressing Mode is static. Valid configurable values ranges from 1 to 4095. Default value is 1.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

DHCP relay

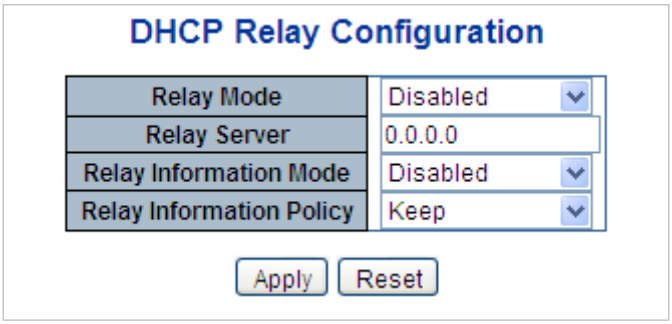
DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

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). This sub-option should include information specific to which circuit the request came in on.
- Remote ID (option 2). This sub-option is designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is four bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes representing the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in a standalone switch it always equals 0; in the switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The remote ID is six bytes in length, and the value equals the DHCP relay agent's MAC address. Configure DHCP relay in the DHCP Relay Configuration page.



This page includes the following fields:

Object	Description
Relay Mode	Indicates the DHCP relay mode operation. Possible modes are: **Enabled**: Enable DHCP relay mode operation. When enabling DHCP relay mode operation, the agent forwards and transfers DHCP messages between the clients and the server when they are not on the same subnet domain and the DHCP broadcast message won't flood due to security settings. **Disabled**: Disable DHCP relay mode operation.

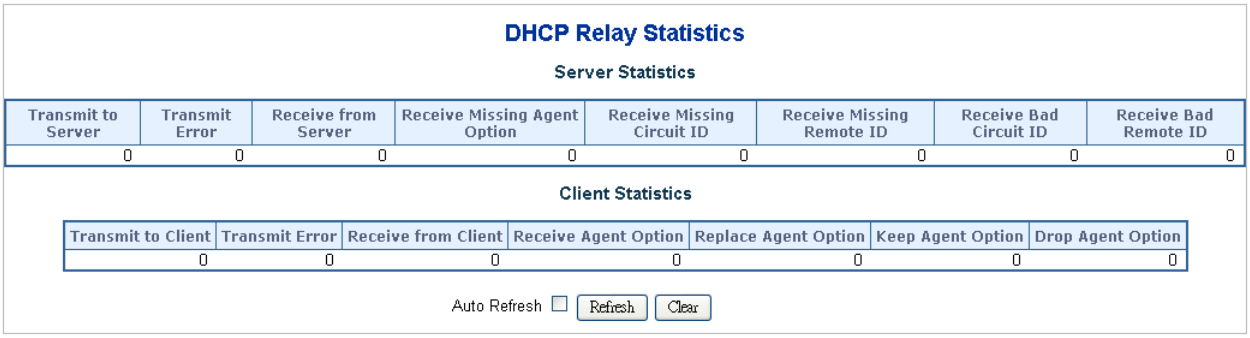
Object	Description
Relay Server	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when they are not on the same subnet domain.
Relay Information Mode	Indicates the DHCP relay information mode option operation. Possible modes are: **Enabled**: Enable DHCP relay information mode operation. When enabling DHCP relay information mode operation, the agent inserts specific information (option82) 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 enabling DHCP relay information mode operation, if the agent receives a DHCP message that already contains relay agent information, it will enforce the policy. This only works when DHCP relay information operation mode is enabled. Options are: **Replace**: Replace the original relay information when receiving a DHCP message that already contains it. **Keep**: Keep the original relay information when receiving a DHCP message that already contains it. **Drop**: Drop the package when receiving a DHCP message that already contains relay information.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

DHCP relay statistics

This page provides statistics for DHCP relay.



Server statistics:

Object	Description
Transmit to Server	The number of packets relayed from client to server.
Transmit Error	The number of packets erroneously sent to clients.
Receive from Server	The number of packets received from the server.

Object	Description
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 in which the Circuit ID option does not match with the known circuit ID.
Receive Bad Remote ID	The number of packets in which the Remote ID option does not match with the known Remote ID.

Client statistics:

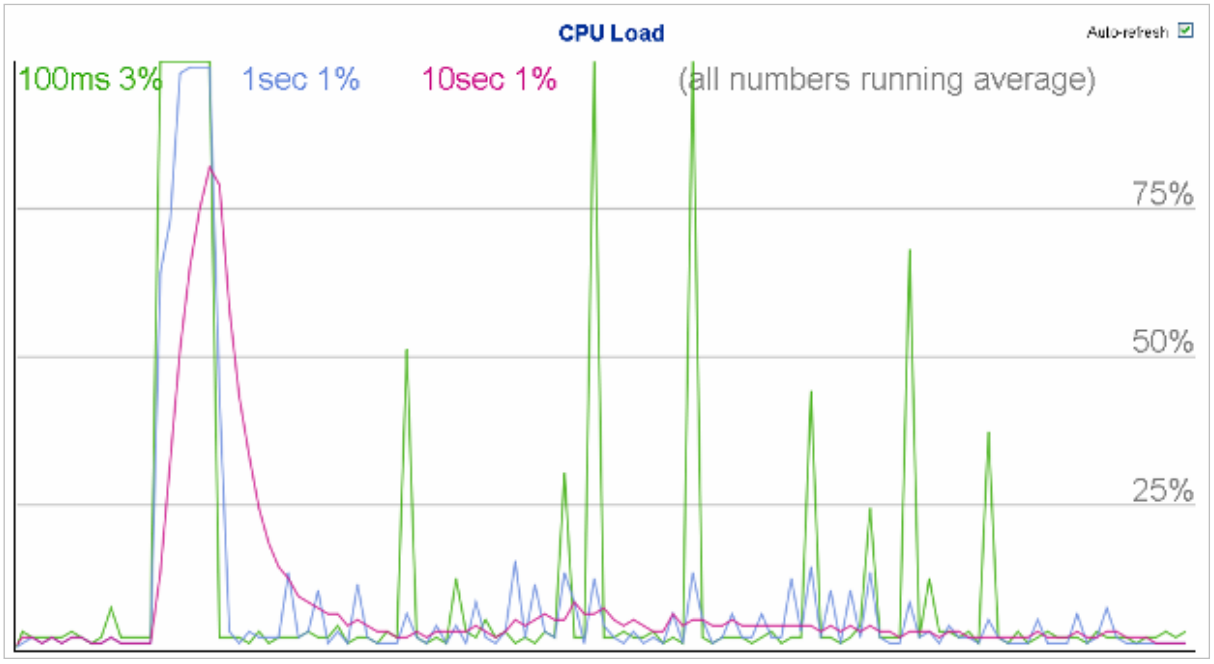
Object	Description
Transmit to Client	The number of packets relayed from server to client.
Transmit Error	The number of packets erroneously sent to servers.
Receive from Client	The number of packets received from the server.
Receive Agent Option	The number of packets received with the relay agent information option.
Replace Agent Option	The number of packets received is replaced with the relay agent information option.
Keep Agent Option	The number of packets received is kept with the relay agent information option.
Drop Agent Option	The number of packets received is dropped with the relay agent information option.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to immediately refresh the page.
- Click **Clear** to clear all statistics.

CPU load

This page displays the CPU load using an SVG graph. The load is measured as average over the last 100 ms, 1 second, and 10 second intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. To display the SVG graph, the browser must support the SVG format. Consult the SVG Wiki for more information on browser support as a plugin may be required.



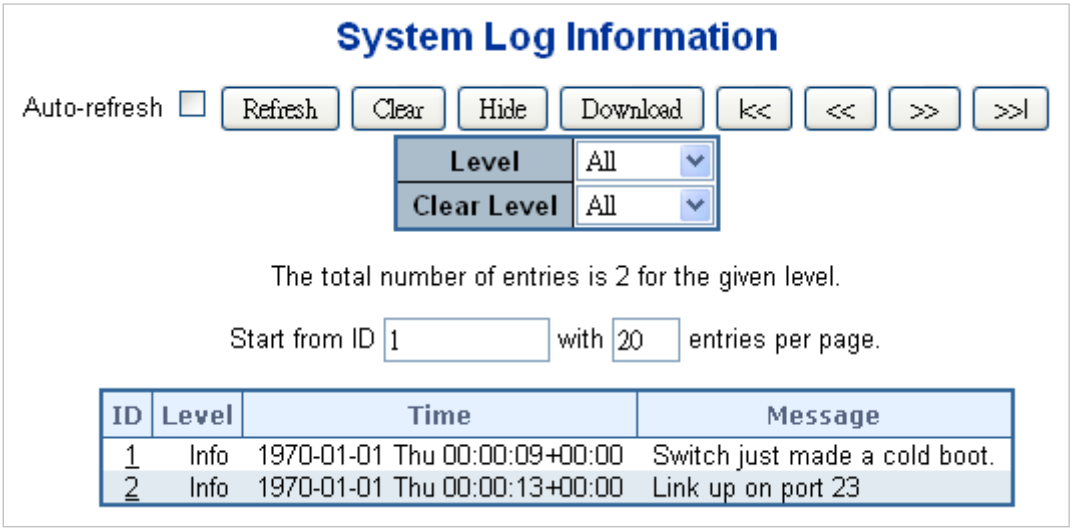
Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.

Note: If the browser does not display anything on this page, download the Adobe SVG tool and install it in the computer.

System log

The System Log Information page shows the managed switch system log information.



The page includes the following fields:

Object	Description
ID	The ID (>= 1) of the system log entry.

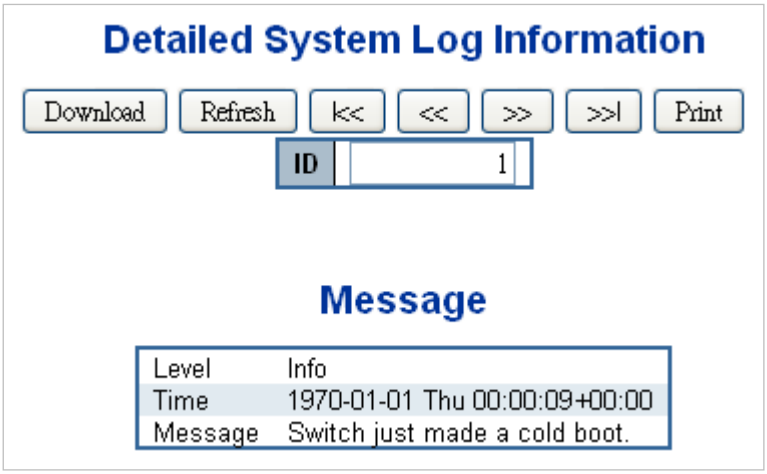
Object	Description
Level	The level of the system log entry. The following level types are supported: **Info**: Information level of the system log. **Warning**: Warning level of the system log. **Error**: Error level of the system log. **All**: All levels.
Clear Level	Clears the system log entry level. 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

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to immediately refresh the page.
- Click **Clear** to clear all statistics.
- Click **Hide** to hide the selected log entries.
- Click **Download** to download the selected log entries.
- Click **I<<** to update the system log entries, starting from the first available entry ID.
- Click **<<** to update the system log entries, ending at the last entry currently displayed.
- Click **>>** to update the system log entries, starting from the last entry currently displayed.
- Click **>>I** to update the system log entries, ending at the last available entry ID.

Detailed log

The Detailed System Log Information page displays the managed switch system log information details.



The page includes the following fields:

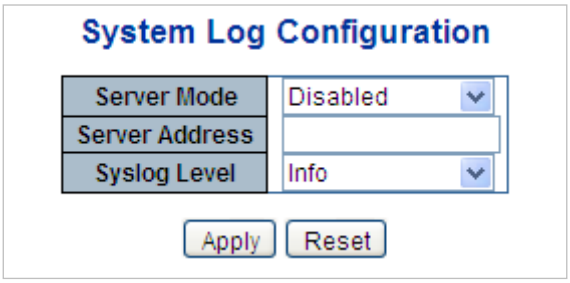
Object	Description
ID	The ID (>= 1) of the system log entry.
Message	The message of the system log entry.

Buttons

- Click **Download** to download the system log entry to the current entry ID.
- Click **Refresh** to update the system log entry to the current entry ID.
- Click **I<<** to update the system log entries, starting from the first available entry ID.
- Click **<<** to update the system log entries, ending at the last entry currently displayed.
- Click **>>** to update the system log entries, starting from the last entry currently displayed.
- Click **>>I** to update the system log entries, ending at the last available entry ID.
- Click **Print** to print the system log entry to the current entry ID.

Remote syslog

The System Log Configuration page displays the managed switch remote system log information details.



The page includes the following fields:

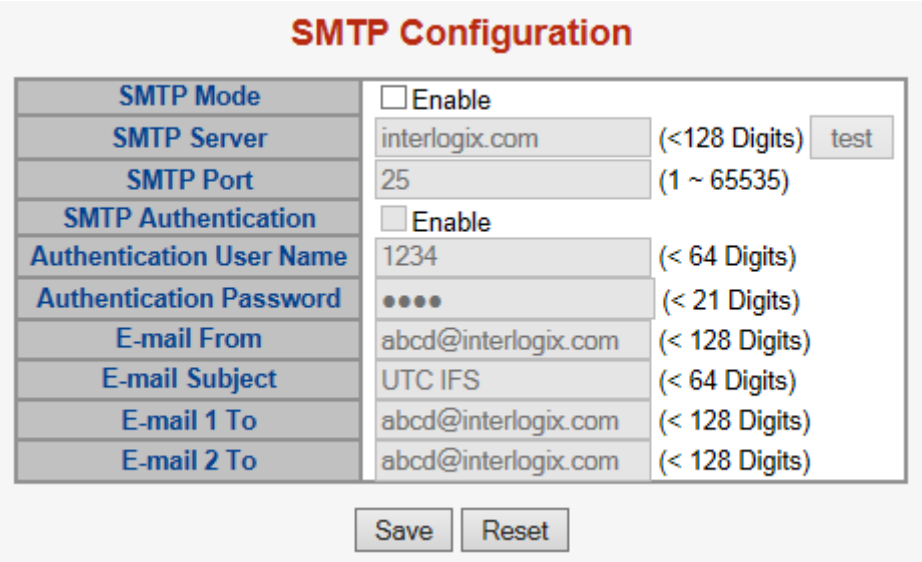
Object	Description
Mode	Indicates the server mode operation. When the mode operation is enabled, the syslog message is sent to the syslog server. The syslog protocol is based on UDP communication and received on UDP port 514. The syslog server will not send acknowledgments back to sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet is always sent out even if the syslog server does not exist. Selections include: **Enabled**: Enable remote syslog mode operation. **Disabled**: Disable remote syslog mode operation.
Syslog Server IP	Indicates the IPv4 host address of syslog server. If the switch provides the DNS feature, it also can be a host name.
Syslog Level	Indicates what kind of message is sent to the syslog server. Selections include: **Info**: Send information, warnings, and errors. **Warning**: Send warnings and errors. **Error**: Send errors.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SMTP configuration

The SMTP Configuration page displays the managed switch SMTP configuration details.



The page includes the following fields:

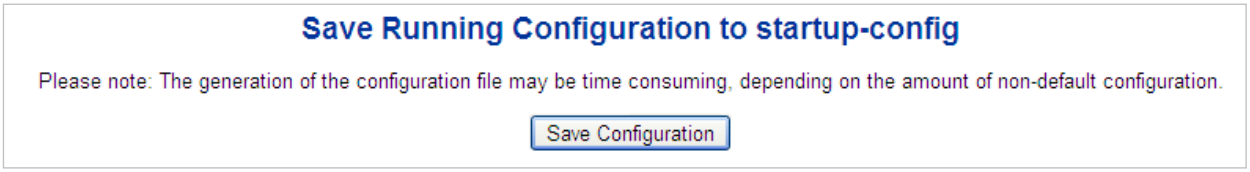
Object	Description
SMTP Mode	Controls whether or not SMTP is enabled on the switch.
SMTP Server	Type the SMTP server name or the IP address of the SMTP server.
SMTP Port	Set the port number of SMTP service.
SMTP Authentication	SMTP authentication is enabled if selected. Authentication is required when an email is sent.
Authentication User Name	Type the user name for the SMTP server if Authentication is **Enable**.
Authentication Password	Type the password for the SMTP server if Authentication is **Enable**.
E-mail From	Type the sender's email address. This address is used for reply emails.
E-mail Subject	Type the subject/title of the email.
E-mail 1 To / E-mail 2 To	Type the receiver's email address.

Buttons

- Click **test** to send a test mail to the mail server to indicate if the account is available.
- Click **Save** to save changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Save startup configuration

This function ensures that the current active configuration can be used after the next reboot.



After clicking **Save Configuration**, the following screen appears.

Configuration download

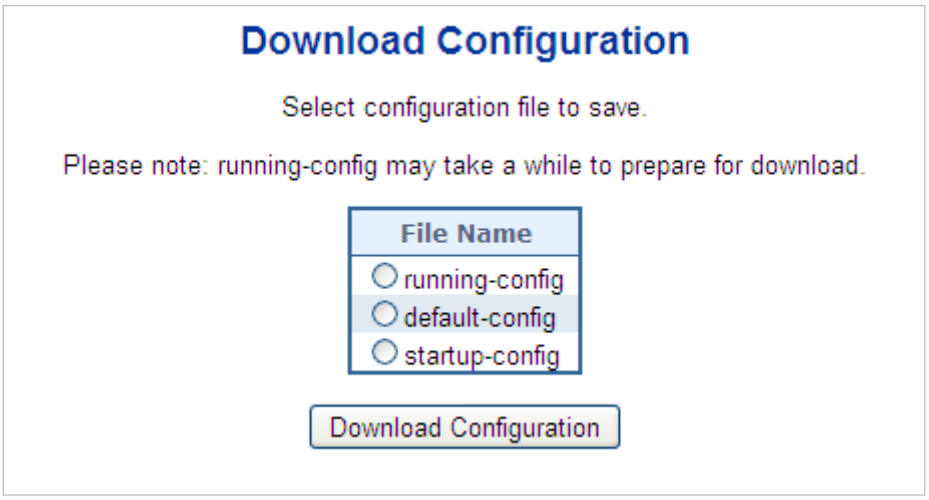
The managed switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

There are three system files:

- **running-config**: A virtual file that represents the currently active configuration on the switch. This file is volatile.
- **startup-config**: The startup configuration for the switch, read at boot time.
- **default-config**: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

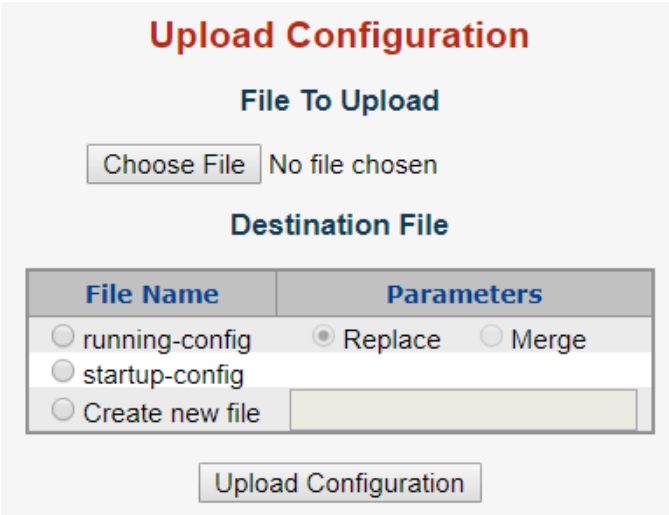
It is also possible to store up to two other files and apply them to running-config, thereby switching configuration.

The Download Configuration page permits the download of the running-config, startup-config, and default-config system files to the switch.



Configuration upload

The Upload Configuration page permits the upload of the running-config and startup-config to the switch.



If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

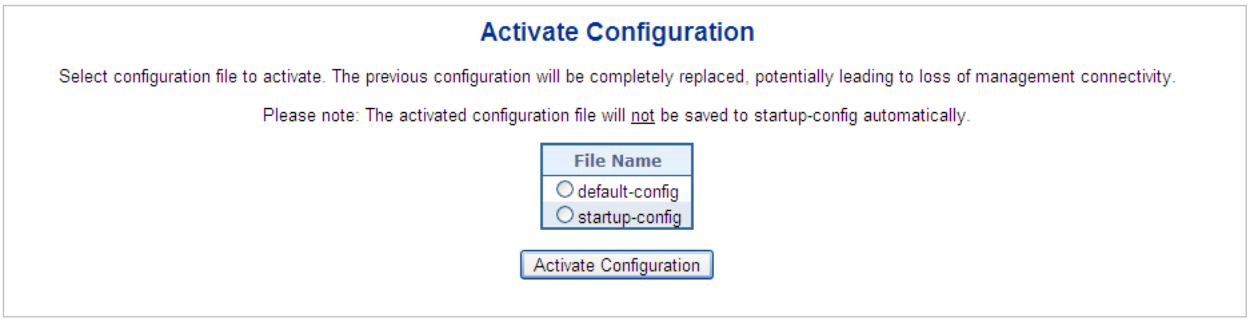
- **Replace** mode: The current configuration is fully replaced with the configuration in the uploaded file.

- **Merge** mode: The uploaded file is merged into running-config.

If the file system is full (i.e., it contains the system files mentioned above plus two other files), it is not possible to create new files unless an existing file is overwritten or another is deleted first.

Configuration activate

The Activate Configuration page permits activation of the startup-config and default-config files on the switch.



It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

Select the file to activate and click **Activate Configuration**. This initiates the process of completely replacing the existing configuration with that of the selected file.

Configuration delete

The Delete Configuration page permits the deletion of the startup-config and default-config files which are stored in Flash memory. If this is performed and the switch is rebooted without a prior save operation, it effectively resets the switch to default configuration.

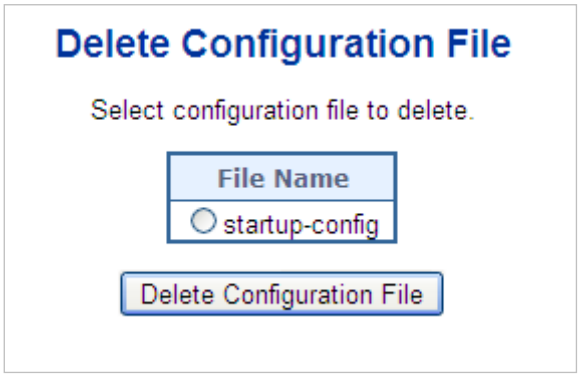


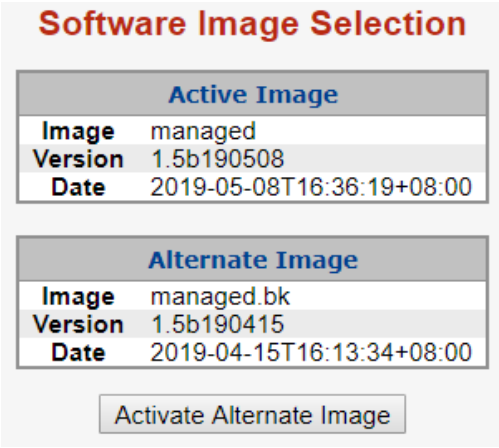
Image select

This page provides information about the active and alternate (backup) firmware images in the device, and permits you to revert to the alternate image. The web page displays two tables with information about the active and alternate firmware images.

Note: If 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.

Note:

1. 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 activate the primary image slot and use it instead.
2. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.



The page includes the following fields:

Object	Description
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 when the firmware was produced.

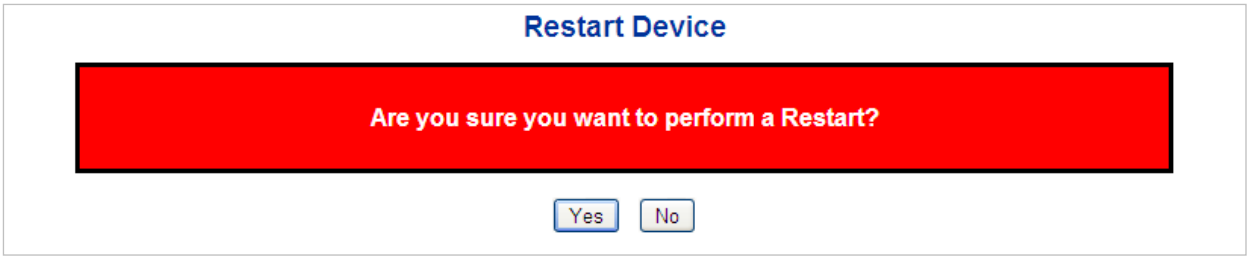
Buttons

- Click **Activate Alternate Image** to use the alternate image. This button may be disabled depending on the system state.

After clicking **Activate Alternate Image**, click OK to restart the system and use the alternate image.

System reboot

The Restart Device page permits the device to be rebooted from a remote location. After clicking the **Yes** button to restart, log in to the web interface about 60 seconds later.



Buttons

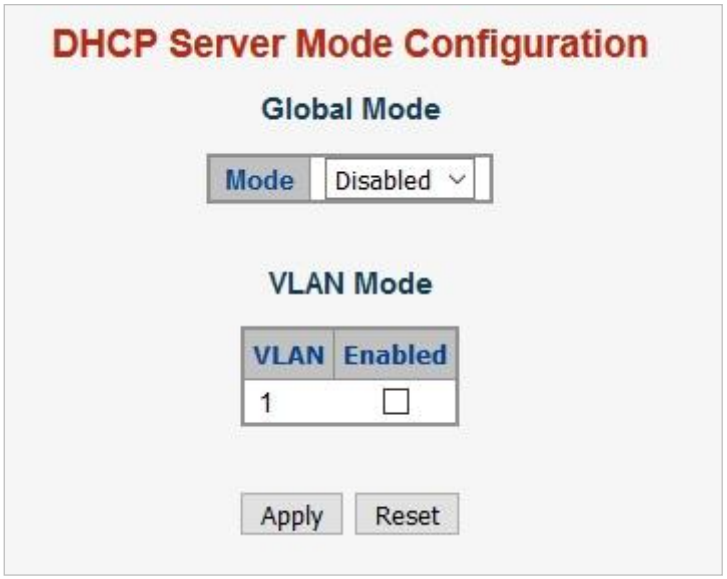
- Click **Yes** to reboot the system.
- Click **No** to return to the main web page without rebooting the system.

Note: If the SYS LED is blinking, then it is in the firmware load stage; if the SYS LED light is on, you can use the web browser to log in to the managed switch.

DHCP server

Mode

The DHCP Server Mode Configuration page permits setting changes for Global Mode and VLAN Mode.



The page includes the following fields:

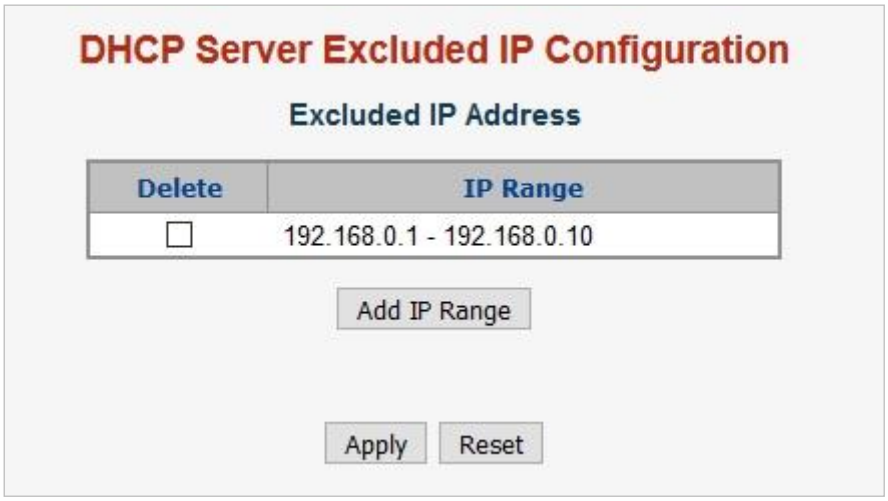
Object	Description
Mode	Enable/disable DHCP server global mode.
VLAN	VLAN ID for enabling the DHCP server service. Additional VLAN interfaces can be added in the IP Configuration page.
Enabled	Enable/disable DHCP server service to the VLAN.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Excluded IP

The DHCP Server Excluded IP Configuration page permits exclusion of IP addresses for static IP address devices, such as servers or routers. The DHCP server will not allocate these excluded IP addresses to the DHCP client.



The page includes the following fields:

Object	Description
Delete	Permits deletion of an IP range.
IP Range	Defines the IP address range to be excluded. The first excluded IP must be smaller than or equal to the second excluded IP. If the IP range contains only 1 excluded IP, input it to either one of the first and second excluded IPs or both.

Buttons

- Click **Add IP Range** to add an IP range.
- Click **Apply** to apply changes.

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

Pool

The DHCP Server Pool Configuration page manages DHCP pools. According to the DHCP pool, the DHCP server will allocate IP addresses and deliver configuration parameters to the DHCP client. Adding a pool and giving it a name creates a new pool with a default configuration. If you want to configure all settings including type, IP subnet mask, and lease time, click the pool name to go into the configuration page.

The page includes the following fields:

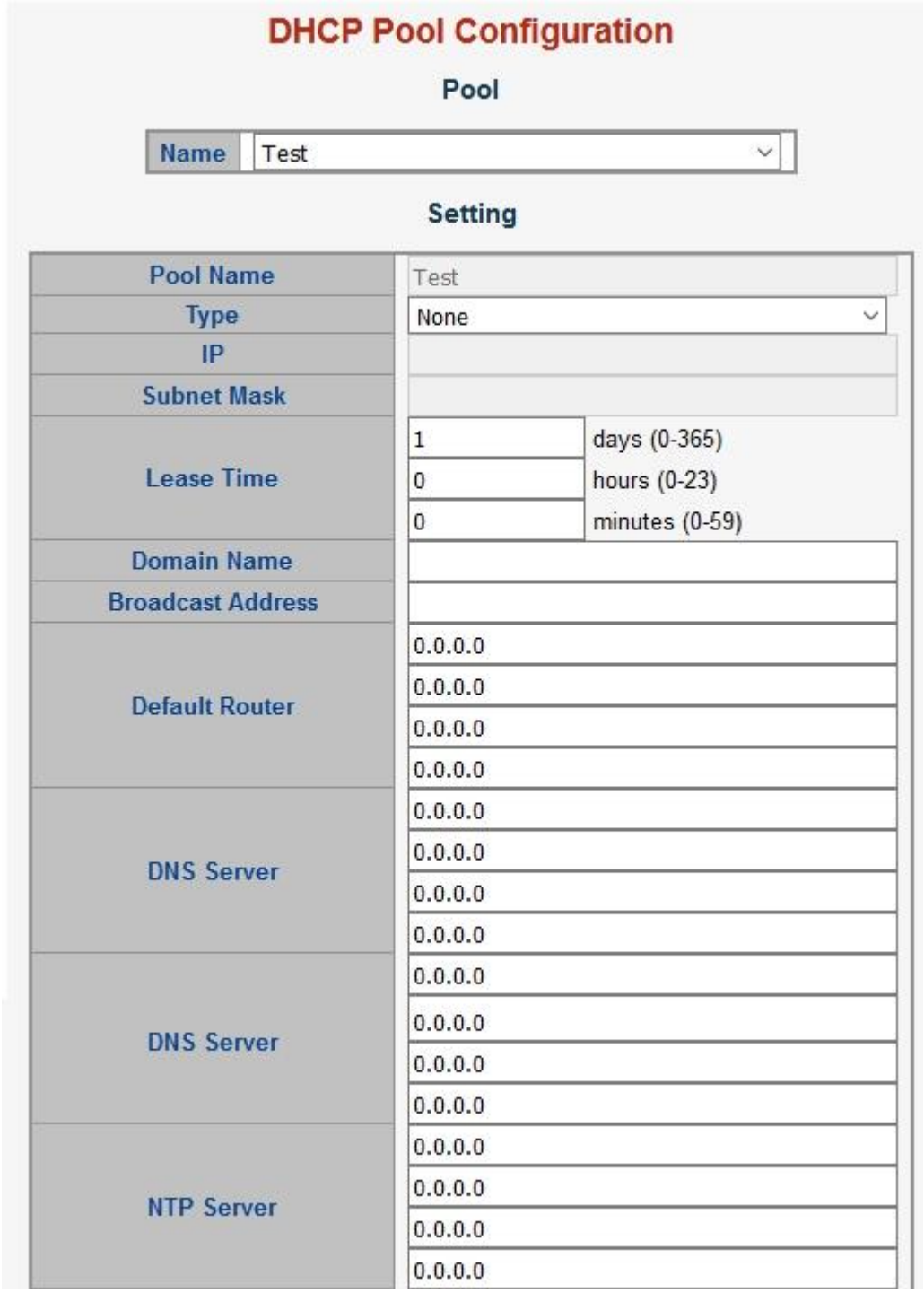
Object	Description
Delete	Permits deletion of pool settings.
Name	Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, click the pool name to go into the configuration page.
Type	Indicates the pool type. **Network**: The pool defines a pool of IP addresses to service more than one DHCP client. **Host**: the pool services for a specific DHCP client identified by client identifier or hardware address. If "-" appears, it means not defined.
IP	Indicates the network number of the DHCP address pool. If "-" appears, it means not defined.
Subnet Mask	Indicates the subnet mask of the DHCP address pool. If "-" appears, it means not defined.
Lease Time	Indicates the lease time of the pool.

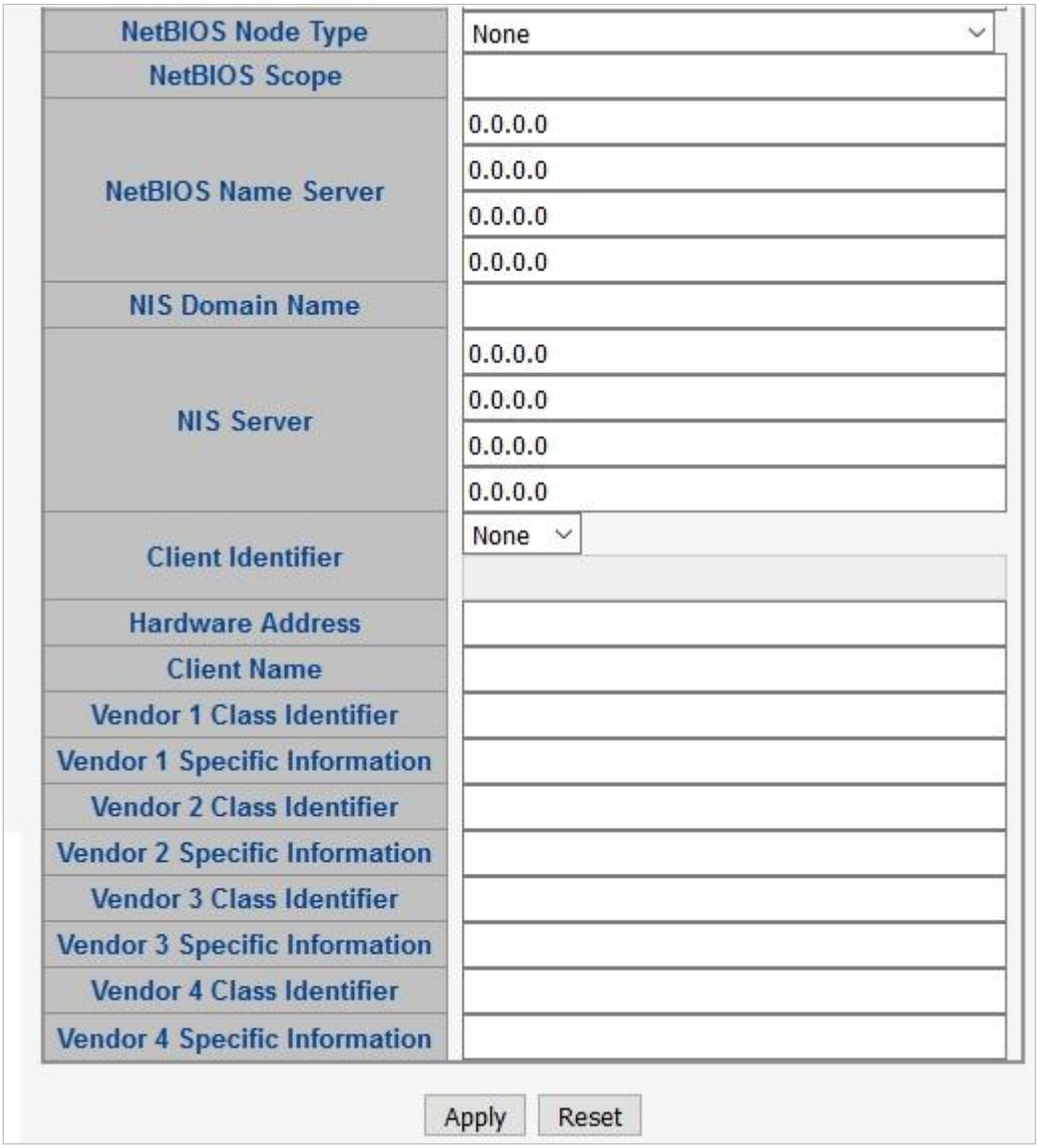
Buttons

- Click **Add New Pool** to add a new DHCP pool.
- Click **Apply** to apply changes.

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

Click a pool name to configure DHCP pool settings on the DHCP Pool Configuration page.





The page includes the following fields:

Object	Description
Name	Select a pool by pool name.
Pool Name	Indicates the selected pool name.
Type	Specifies the pool type. **Network**: the pool defines a pool of IP addresses to service more than one DHCP client. **Host**: the pool services for a specific DHCP client identified by client identifier or hardware address.
IP	Indicates the specific network number of the DHCP address pool.
Subnet Mask	DHCP option 1. Specifies the subnet mask of the DHCP address pool.
Lease Time	DHCP option 51, 58 and 59. Specifies the lease time that allows the client to request a lease time for the IP address. If all are 0's, then it means the lease time is infinite.

Object	Description
Domain Name	DHCP option 15. Specifies a domain name that the client should use when resolving a hostname via DNS.
Broadcast Address	DHCP option 28. Specifies the broadcast address in use on the client's subnet.
Default Router	DHCP option 3. Specifies a list of IP addresses for routers on the client's subnet.
DNS Server	DHCP option 6. Specifies a list of Domain Name System name servers available to the client.
NTP Server	DHCP option 42. Specifies a list of IP addresses indicating NTP servers available to the client.
NetBIOS Node Type	DHCP option 46. Specifies NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable as described in RFC 1001/1002.
NetBIOS Scope	DHCP option 47. Specifies the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.
NetBIOS Name Server	DHCP option 44. Specifies a list of NBNS name servers listed in order of preference.
NIS Domain Name	DHCP option 40. Specifies the name of the client's NIS domain.
NIS Server	DHCP option 41. Specifies a list of IP addresses indicating NIS servers available to the client.
Client Identifier	DHCP option 61. Specifies the client's unique identifier to be used when the pool is the type of host. Select the type of client identifier at first. **None**: client identifier is not specified yet. **Name**: the type of client identifier is other than hardware. **MAC**: the type of client identifier is MAC address.
Hardware Address	Specifies the client's hardware (MAC) address to be used when the pool is the type of host.
Client Name	DHCP option 12. Specifies the name of client to be used when the pool is the type of host.
Vendor 1 Class Identifier	DHCP option 60. Specifies the identifier to be used by the DHCP client to optionally identify the vendor type and configuration of a DHCP client. The DHCP server delivers the corresponding option 43 specific information to the client that sends an option 60 vendor class identifier.

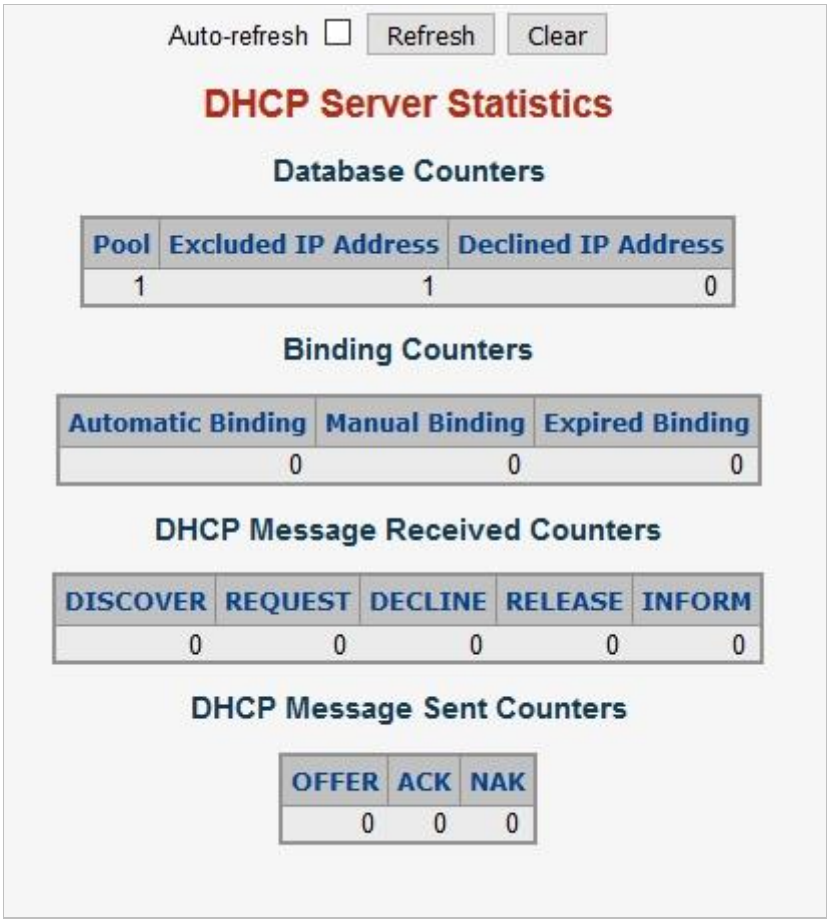
Object	Description
Vendor 1 Specific Information	DHCP option 43. Specifies the vendor specific information according to the option 60 vendor class identifier.
Vendor 2 Class identifier	DHCP option 60. Specifies the identifier to be used by the DHCP client to optionally identify the vendor type and configuration of a DHCP client. The DHCP server delivers the corresponding option 43 specific information to the client that sends the option 60 vendor class identifier.
Vendor 2 Specific Information	DHCP option 43. Specifies vendor specific information according to the option 60 vendor class identifier.
Vendor 3 Class Identifier	DHCP option 60. Specifies the identifier to be used by the DHCP client to optionally identify the vendor type and configuration of a DHCP client. The DHCP server delivers the corresponding option 43 specific information to the client that sends the option 60 vendor class identifier.
Vendor 3 Specific Information	DHCP option 43. Specifies vendor specific information according to the option 60 vendor class identifier.
Vendor 4 Class Identifier	DHCP option 60. Specifies the identifier to be used by the DHCP client to optionally identify the vendor type and configuration of a DHCP client. The DHCP server delivers the corresponding option 43 specific information to the client that sends the option 60 vendor class identifier.
Vendor 4 Specific Information	DHCP option 43. Specify vendor specific information according to the option 60 vendor class identifier.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Statistics

The DHCP Server Statistics page displays the database counters and the number of DHCP messages sent and received by the DHCP server.



The page includes the following fields:

Database counters

Displays the counters of various databases.

Object	Description
Pool	Number of pools.
Excluded IP Address	Number of excluded IP address ranges.
Declined IP Address	Number of declined IP addresses.

Binding counters

Displays the counters of various bindings.

Object	Description
Automatic Binding	Number of bindings with network-type pools.
Manual Binding	Number of bindings that the administrator assigns an IP address to a client (host pool type).
Expired Binding	Number of bindings in which the lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP message received counters

Displays the counters of DHCP messages received by the DHCP server.

Object	Description
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

Displays the counters of DHCP messages sent by the DHCP server.

Object	Description
Offer	Number of DHCP OFFER messages sent.
Ack	Number of DHCP ACK messages sent.
Nak	Number of DHCP NAK messages sent.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear DHCP message received and sent counters.

Binding

The DHCP Server Binding IP page displays bindings generated for DHCP clients.

The page includes the following fields:

Binding IP address

Displays all bindings.

Object	Description
IP	IP address allocated to the 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 that services the binding.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **Clear Selected** to clear the selected bindings. If the selected binding is Automatic or Manual, then it is changed to Expired. If the selected binding is Expired, then it is freed.
- Click **Clear Automatic** to clear all automatic bindings and change them to Expired bindings.
- Click **Clear Manual** to clear all manual bindings and change them to Expired bindings.
- Click **Clear Expired** to clear all expired bindings and free them.

Declined IP

The DHCP Server Declined IP page displays declined IP addresses.

The page includes the following fields:

Declined IP address

Displays IP addresses declined by DHCP clients.

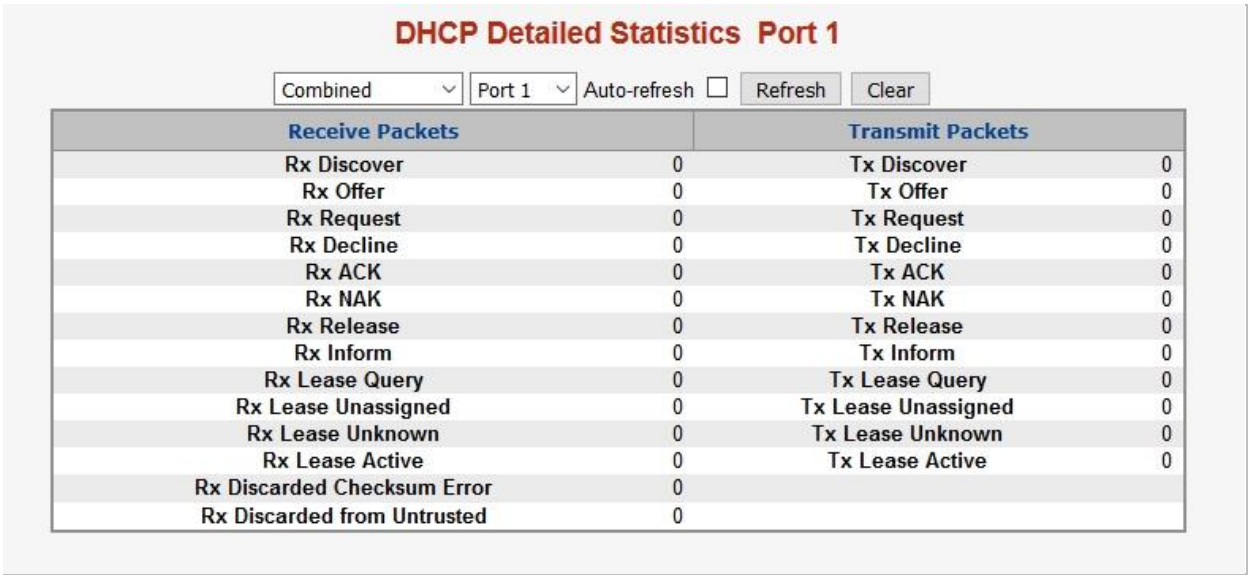
Object	Description
Declined IP	List of IP addresses declined.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Detailed statistics

The DHCP Detailed Statistics page provides statistics for DHCP snooping. Note that the normal forward per-port TX statistics are not increased if the incoming DHCP packet is done by a L3 forwarding mechanism. Clearing the statistics on a specific port may not affect global statistics since it gathers a different layer overview.



The page includes the following fields:

Object	Description
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 amd 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.

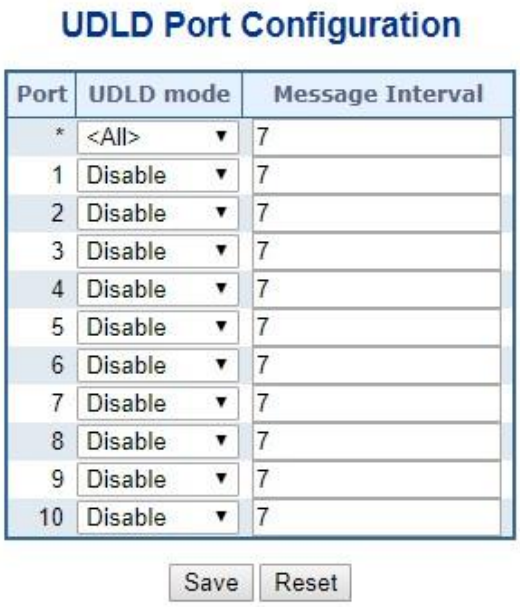
Object	Description
RX and TX Inform	The number of inform (option 53 with value 8) packets received and transmitted.
RX and TX Lease Query	The number of lease query (option 53 with value 10) packets received and transmitted.
RX and TX Lease Unassigned	The number of lease unassigned (option 53 with value 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 discarded packets where IP/UDP checksum is in error.
RX Discarded from Untrused	The number of discarded packets that are coming from an untrusted port.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear the counters for the selected port.

UDLD

The UDLD Port Configuration page permits the user to inspect and change the current Unidirectional Link Detection (UDLD) configurations.



The page includes the following fields:

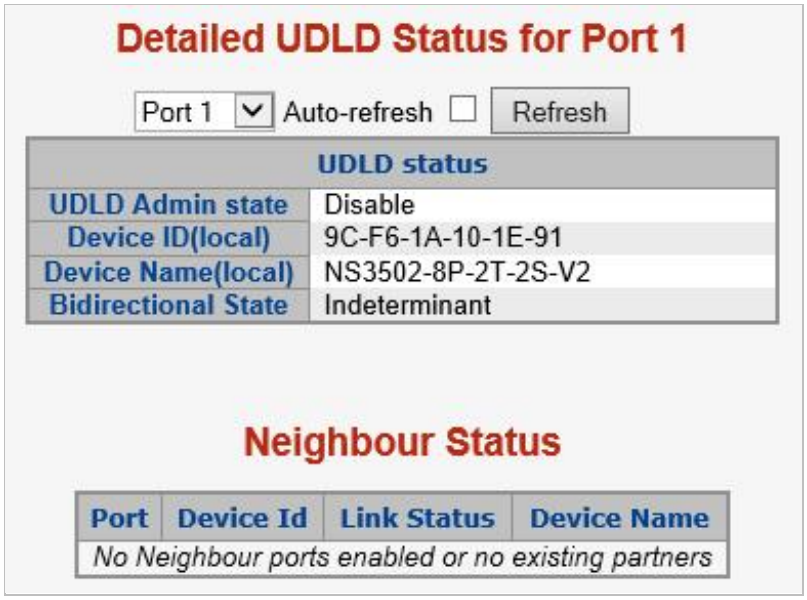
Object	Description
Port	Port number of the switch.
UDLD Mode	Configures the UDLD mode on a port. Selections inlcude **Disable**, **Normal** and **Aggressive**. Default mode is **Disable**. **Disable** – In disabled mode, UDLD functionality doesn't exist on the port. **Normal** – In normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state. **Aggressive** – In aggressive mode, unidirectional detected ports will get shut down. To bring back the ports up, disable UDLD on the ports.
Message Interval	Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds (default value is 7 seconds). Currently, the default time interval is supported due to lack of detailed information in RFC 5171.

Buttons

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

UDLD status

The Detailed UDLD Status/Neighbor Status page displays the UDLD status of the ports.



UDLD port status

The page includes the following fields:

Object	Description
UDLD Admin State	The current port state of the logical port, Enabled if any of state(Normal,Aggressive) is Enabled.
Device ID (Local)	The ID of Device.
Device Name (Local)	Name of the Device.
Bidirectional State	The current state of the port.

Neighbor status

The page includes the following fields:

Object	Description
Port	The current port of the neighbor device.
Device ID	The current ID of the neighbor device.
Link Status	The current link status of the neighbor port.
Device Name	Name of the neighbor device.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Simple Network Management Protocol (SNMP)

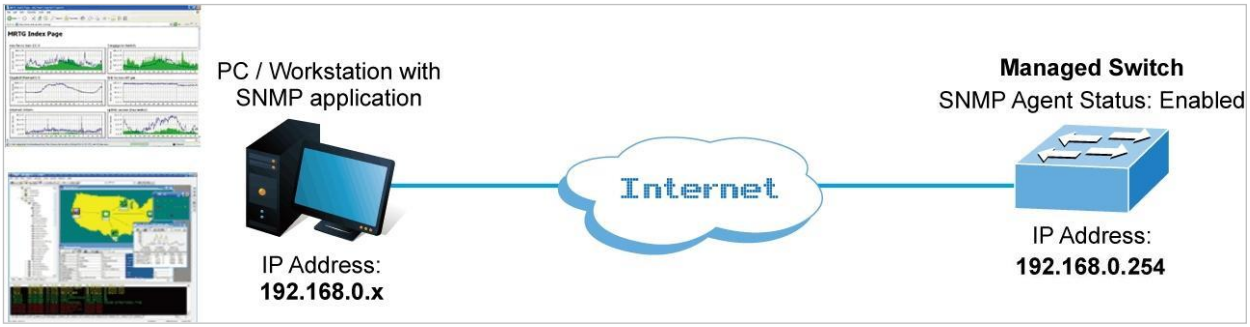
SNMP overview

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP permits network administrators to manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network consists of the following:

- **Network management stations (NMSs)**: Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.

- **Agents**: Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB)**: An MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **Network-management protocol**: A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.



SNMP operations

SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response.

- **Get** – Allows the NMS to retrieve an object instance from the agent.
- **Set** – Allows the NMS to set values for object instances within an agent.
- **Trap** – Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

SNMP community

An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. An SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are:

- Write (private)
- Read (public)

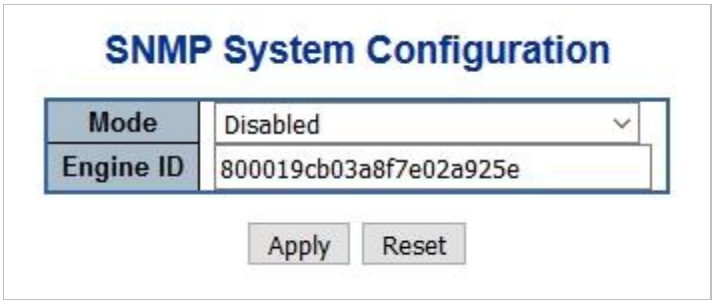
Use the SNMP Menu to display or configure the managed switch's SNMP function. This section has the following items:

System Configuration	Configure SNMP on this page.
System Information	The system information is provided here.
SNMPv3 Communities	Configure SNMPv3 communities table on this page.
SNMPv3 Users	Configure SNMPv3 users table on this page.
SNMPv3 Groups	Configure SNMPv3 groups table on this page.

SNMPv3 Views	Configure SNMPv3 views table on this page.
SNMPv3 Access	Configure SNMPv3 accesses table on this page.

SNMP system configuration

Configure SNMP on the SNMP System Configuration page.



The page includes the following fields:

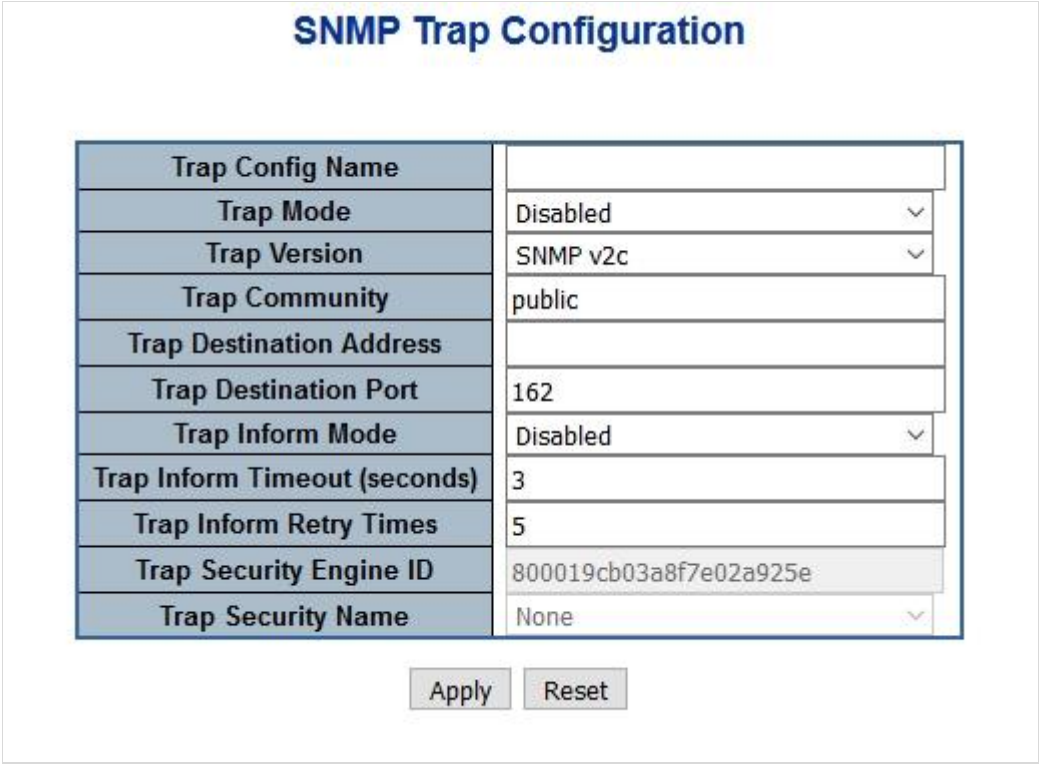
Object	Description
Mode	Indicates the SNMP mode operation. Selections include: **Enabled**: Enable SNMP mode operation. **Disabled**: Disable SNMP mode operation.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SNMP trap configuration

Configure the SNMP trap on the SNMP Trap Configuration page.



The page includes the following fields:

Object	Description
Trap Config	Indicates the trap configuration name. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.
Trap Mode	Indicates the SNMP trap mode operation. Selections include: **Enabled**: Enable SNMP trap mode operation. **Disabled**: Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Selections include: **SNMP v1**: Set SNMP trap supported version 1. **SNMP v2c**: Set SNMP trap supported version 2c. **SNMP v3**: Set SNMP trap supported version 3.
Write Community	Indicates the community write access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when the SNMP version is SNMPv1 or SNMPv2c. If the SNMP version is SNMPv3, the community string will be associated with the SNMPv3 communities table. It provides more flexibility to configure a security name than a SNMPv1 or SNMPv2c community string. In addition to the community string, a particular range of source addresses can be used to restrict the source subnet.
Trap Community	Indicates the community access string when sending the SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.
Trap Destination Address	Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w') as well as 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'.
Trap Destination Port	Indicates the SNMP trap destination port. The SNMP agent sends an SNMP message via this port. The port range is 1~65535.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Selections include: **Enabled**: Enable SNMP trap authentication failure. **Disabled**: Disable SNMP trap authentication failure.
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**.

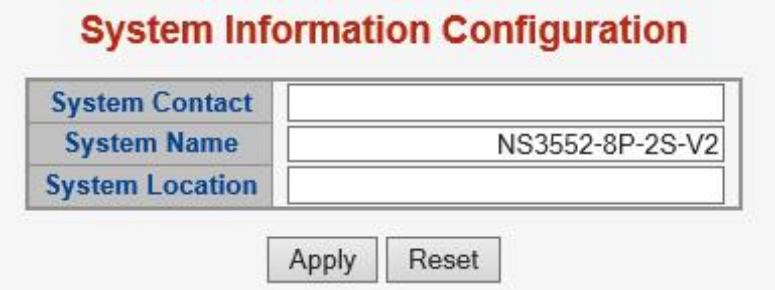
Object	Description
Trap Probe Security Engine ID	Indicates the SNMPv3 trap probe security engine ID mode of operation. Selections include: **Enabled**: Enable SNMP trap probe security engine ID mode of operation. **Disabled**: Disable SNMP trap probe security engine ID mode of operation.
Trap Security 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

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SNMP system information

The switch system information is provided in the System Information Configuration page.



The page includes the following fields:

Object	Description
System Contact	The textual identification of the contact person for this managed node and 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.

Object	Description
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-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

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

SNMPv3 configuration

SNMPv3 communities

Configure SNMPv3 communities in the SNMPv3 Community Configuration page. The entry index key is Community.

The page includes the following fields:

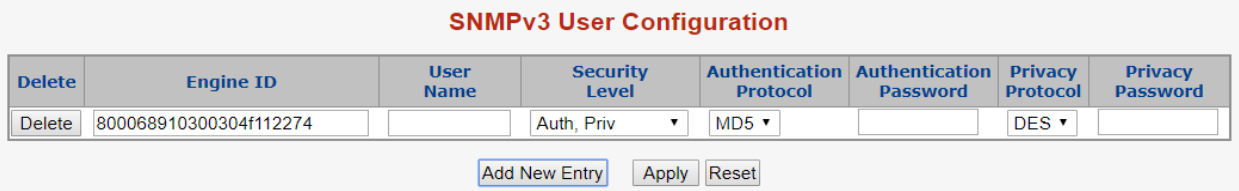
Object	Description
Delete	Select the check box to delete the entry. It will be deleted during the next save.
Community Name	Indicates the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Source IP	Indicates the SNMP access source address. A particular range of source addresses can be used to restrict the source subnet when combined with the source mask.
Source Mask	Indicates the SNMP access source address mask.

Buttons

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

SNMPv3 users

Configure SNMPv3 users on the SNMPv3 User Configuration page. The entry index keys are Engine ID and User Name.



The page includes the following fields:

Object	Description
Delete	Select **Delete** 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 a 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 the same as the snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user, otherwise it is a remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Selections include: **NoAuth, NoPriv**: None authentication and none privacy. **Auth, NoPriv**: Authentication and none privacy. **Auth, Priv**: Authentication and privacy. The value of the security level cannot be modified if the entry already exists. Ensure that the value is set correctly.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Selections include: **None**: None authentication protocol. **MD5**: An optional flag to indicate that this user using MD5 authentication protocol. **SHA**: An optional flag to indicate that this user using SHA authentication protocol.

Object	Description
	The value of security level cannot be modified if the entry already exists. Ensure that the value is set correctly.
Authentication Password	A string identifying the authentication pass 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 the ASCII characters from 33 to 126.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Selections include: **None**: None privacy protocol. **DES**: An optional flag to indicate that this user using DES authentication protocol. **AES**: An optional flag to indicate that this user uses AES authentication protocol.
Privacy Password	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

Buttons

- Click **Add New Entry** to add a new user entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SNMPv3 groups

Configure SNMPv3 groups on the SMNPv3 Group Configuration page. The entry index keys are Security Model and Security Name.

The page includes the following fields:

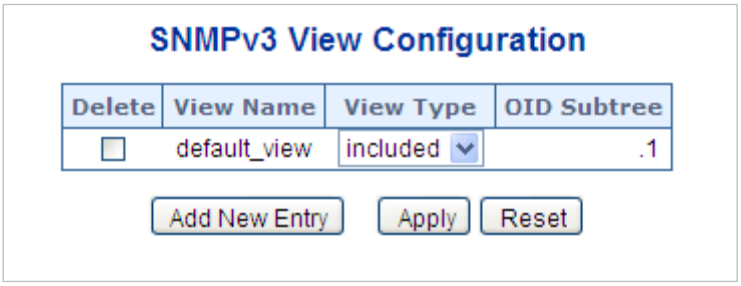
Object	Description
Delete	Select **Delete** to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Selections include: **v1**: Reserved for SNMPv1. **v2c**: Reserved for SNMPv2c. **usm**: User-based Security Model (USM).
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 the 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 the ASCII characters from 33 to 126.

Buttons

- Click **Add New Entry** to add a new group entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SNMPv3 views

Configure SNMPv3 views table in the SNMPv3 View Configuration page. The entry index keys are View Name and OID Subtree.



The page includes the following fields:

Object	Description
Delete	Select **Delete** to delete the entry. It will be deleted during the next save.
View Name	A string identifies the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Selections include: **included**: An optional flag to indicate that this view subtree should be included.

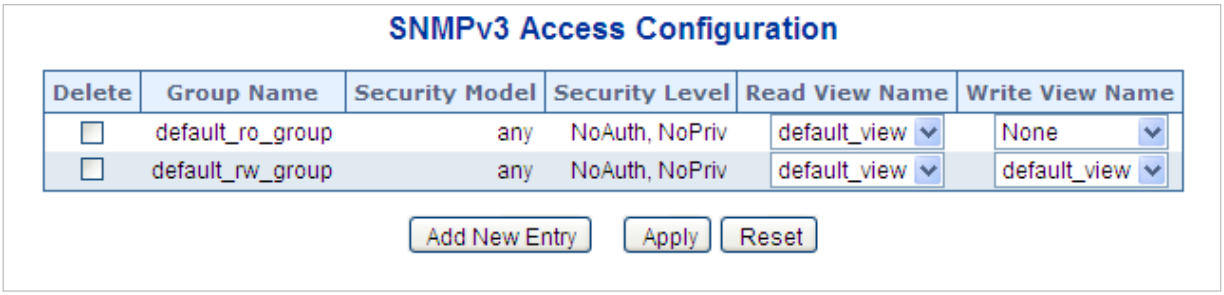
Object	Description
	excluded: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is excluded, it should exist in another view entry in which the view type is included and it's OID subtree overrides the excluded view entry.
OID Subtree	The OID 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

- Click **Add New Entry** to add a new view entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SNMPv3 access

Configure SNMPv3 access on the SNMPv3 Access Configuration page. The entry index keys are Group Name, Security Model, and Security Level.



The page includes the following fields:

Object	Description
Delete	Select **Delete** to delete the entry. It will be deleted during the next save.
Group Name	A string identifies the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Selections include: **any**: Accepted any security model (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. Selections include: **NoAuth, NoPriv**: None authentication and none privacy. **Auth, NoPriv**: Authentication and none privacy. **Auth, Priv**: Authentication and privacy.

Object	Description
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 the 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 the ASCII characters from 33 to 126.

Buttons

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

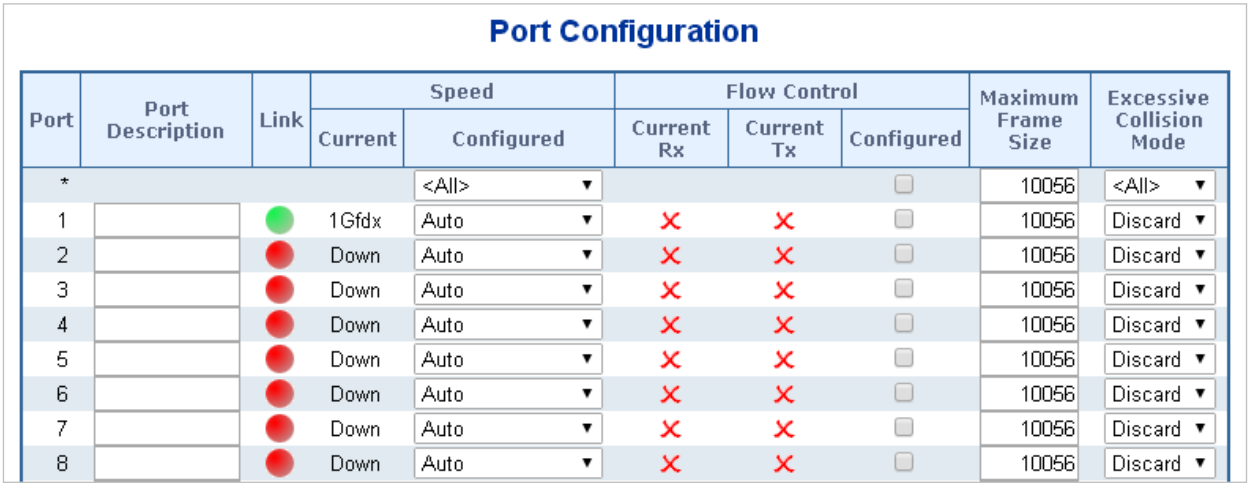
Port management

Use the Port menu to display or configure the managed switch ports. This section has the following items:

Port Configuration	Configures port connection settings
Port Statistics Overview	Lists Ethernet and RMON port statistics
Port Statistics Detail	Lists Ethernet and RMON port statistics
SFP Module Information	Displays SFP information
Port Mirror	Sets the source and target ports for mirroring

Port configuration

Ports can be configured on the Port Configuration page.



The page includes the following fields:

Object	Description
Port	This is the logical port number for this row.
Port Description	Indicates the per port description.
Link	The current link state is displayed graphically. Green indicates the link is up and red is down.
Current Link Speed	Provides the current link speed of the port.
Configured Link Speed	Select any available link speed for the given switch port. Draw the menu bar to select the mode. **All**: Set up all ports with the same setting. **Auto**: Set up auto negotiation for the copper interface. **10Mbps HDX**: Force sets 10 Mbps/Half-Duplex mode. **10Mbps FDX**: Force sets 10 Mbps/Full-Duplex mode. **100Mbps HDX**: Force sets 100 Mbps/Half-Duplex mode. **100 Mbps FDX**: Force sets 100 Mbps/Full-Duplex mode. **1Gbps FDX**: Force sets 1000 Mbps/Full-Duplex mode. **10Gbps FDX**: Force sets 10 Gbps/Full-Duplex mode. **Disable**: Shut down the port manually.
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 if 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. The allowed range is 1518 bytes to 9600 bytes.
Excessive Collision Mode	Configure port transmit collision behavior. **Discard**: Discard frame after 16 collisions (default). **Restart**: Restart back off algorithm after 16 collisions.

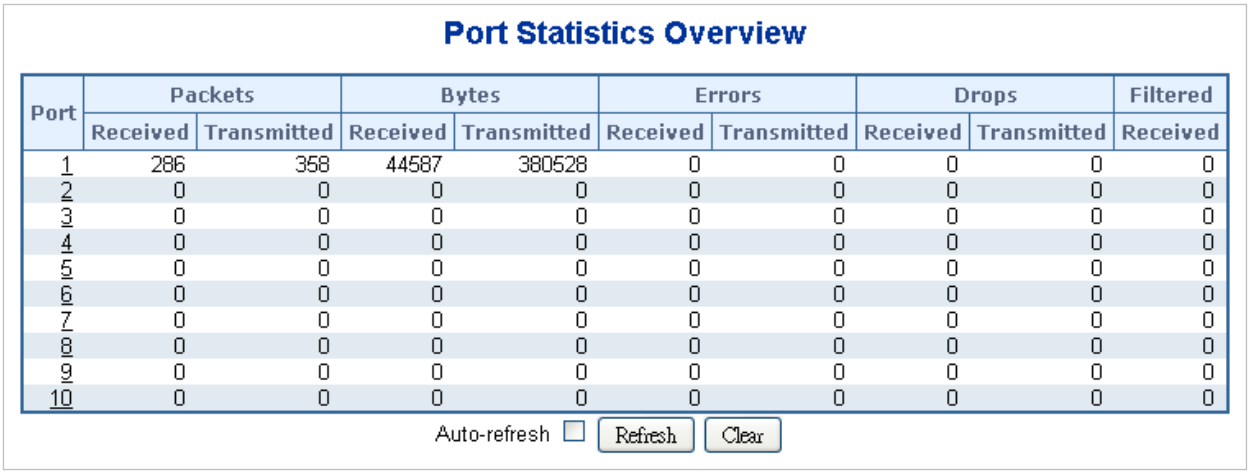
Note: If setting each port to run at 100M full-, 100M half-, 10M full-, and 10M half-speed modes, the auto-MDIX function will be disabled.

Buttons

- Click **Save** to save changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Refresh** to refresh the page and undo all local changes.

Port statistics overview

The Port Statistics Overview page provides an overview of general traffic statistics for all switch ports.



The displayed counters are:

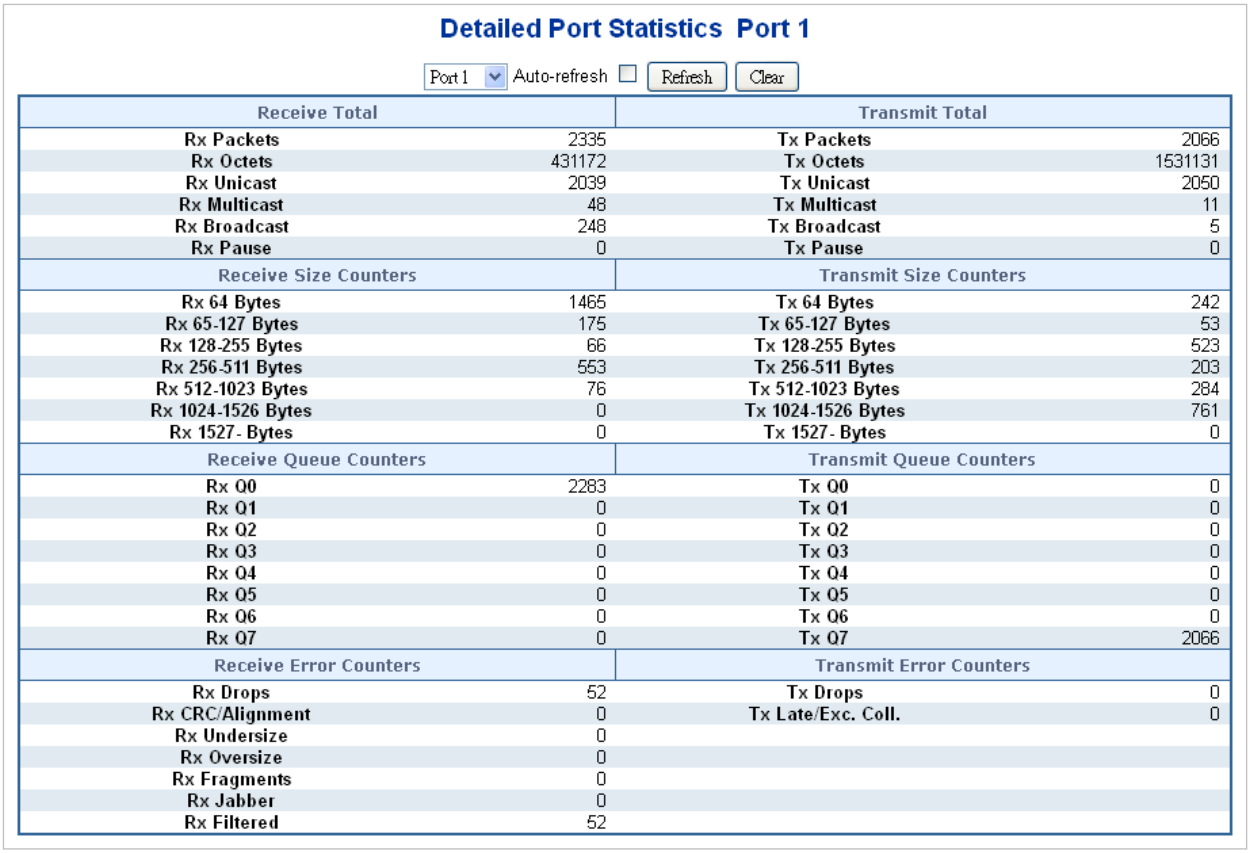
Object	Description
Port	The logical port for the settings contained in the same row.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per 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

- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear the counters for all ports.
- Select the **Auto-refresh** check box to enable an automatic refresh of the page at regular intervals.

Port statistics detail

The Port Statistics Detail 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 current 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.



Detailed Port Statistics Port 1

Port 1 | Auto-refresh | Refresh | Clear

Receive Total		Transmit Total	
Rx Packets	2335	Tx Packets	2066
Rx Octets	431172	Tx Octets	1531131
Rx Unicast	2039	Tx Unicast	2050
Rx Multicast	48	Tx Multicast	11
Rx Broadcast	248	Tx Broadcast	5
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	1465	Tx 64 Bytes	242
Rx 65-127 Bytes	175	Tx 65-127 Bytes	53
Rx 128-255 Bytes	66	Tx 128-255 Bytes	523
Rx 256-511 Bytes	553	Tx 256-511 Bytes	203
Rx 512-1023 Bytes	76	Tx 512-1023 Bytes	284
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	761
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	2283	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	2066
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	52	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	52		

The page includes the following fields:

Receive total and transmit total

Object	Description
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, including FCS, but excluding 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 has 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

Object	Description
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short[1] frames received with valid CRC.
Rx Oversize	The number of long[2] frames received with valid CRC.
Rx Fragments	The number of short[1] frames received with invalid CRC.
Rx Jabber	The number of long[2] frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.

[1] Short frames are frames that are smaller than 64 bytes.

[2] Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit error counters

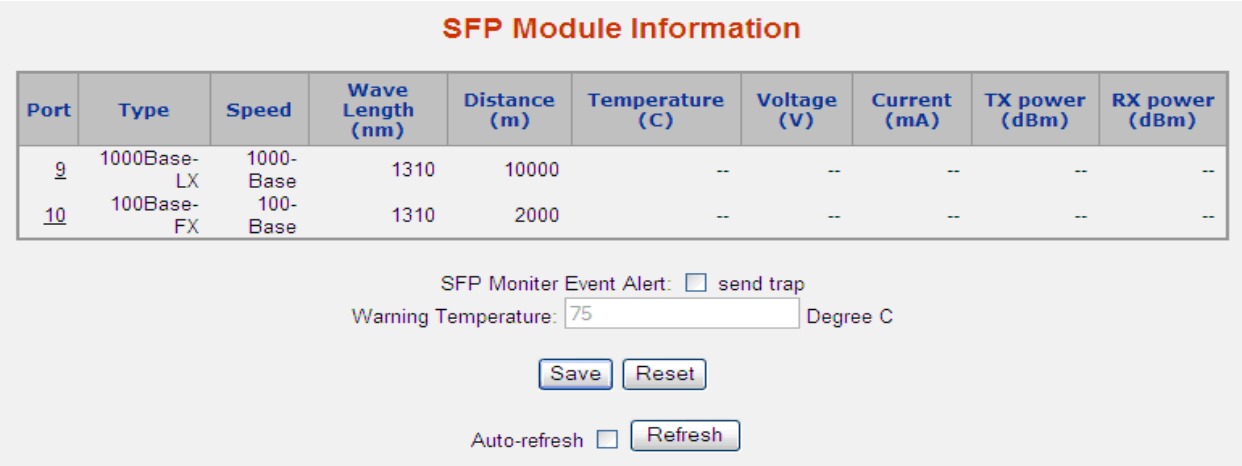
Object	Description
Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late/Exc. Coll.	The number of frames dropped due to excessive or late collisions.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear the counters for all ports.
- Select the **Auto-refresh** check box to enable an automatic refresh of the page at regular intervals.

SFP module information

You can check the physical or operational status of an SFP module via the SFP Module Information page. This page shows the operational status such as the transceiver type, speed, wavelength, optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage in real time. You can also use the port number hyperlinks to check the statistics on a specific interface.



The page includes the following fields:

Object	Description
Type	Displays the type of current SFP module. The possible types are: • 1000Base-SX • 1000Base-LX • 100Base-FX
Speed	Displays the speed of the current SFP module. Different vendors' SFP modules might show different speed information.
Wave Length(nm)	Displays the wavelength of current SFP module. Use this column to check if the wavelength values of two nodes are matched when the fiber connection fails.
Distance(m)	Displays the supported distance of the current SFP module.
Temperature(C)	Displays the temperature of the current SFP module.
Voltage(V)	Displays the voltage of the current SFP module.
Current(mA)	Displays the Ampere of the current SFP module.
TX power(dBm)	Displays the TX power of the current SFP module.
RX power(dBm)	Displays the RX power of the current SFP module.

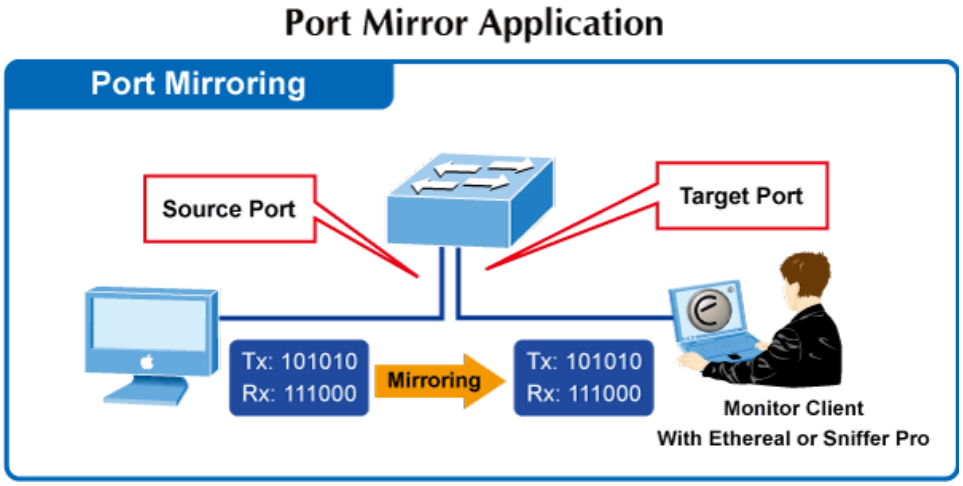
Buttons

- Select the **SFP Monitor Event Alert** check box. The switch will be in accordance with the **Warning Temperature** setting and allows users to record message out via SNMP Trap.
- Click **Save** to save changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Refresh** to refresh the page immediately.
- Select the **Auto-refresh** check box to enable an automatic refresh of the page at regular intervals.

Port mirror

Configure port mirroring on the Mirror & RMirror Configuration Table page. This function provides the monitoring of network traffic that forwards a copy of each incoming or outgoing packet from one port of a network switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.

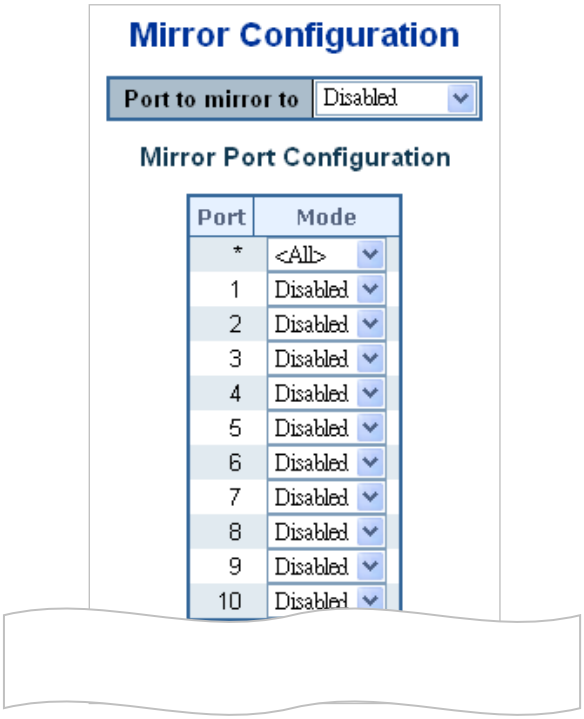
- To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.
- The managed switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.



The traffic to be copied to 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).

Mirror port configuration



The page includes the following fields:

Object	Description
Port to mirror on	Port to mirror is 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.
Port	The logical port for the settings contained in the same row, * indicates that all ports are selected.
Mode	Select mirror mode. **Rx only**: Frames received at this port are mirrored to the mirroring port. Frames transmitted are not mirrored. **Tx only**: Frames transmitted from this port are mirrored to the mirroring port. Frames received are not mirrored. **Disabled**: Neither frames transmitted or frames received are mirrored. **Both**: Frames received and frames transmitted are mirrored to the mirror port.

Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, the mode for the selected mirror port is limited to **Disabled** or **Rx only**.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Link aggregation

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Group (LAG). Port aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

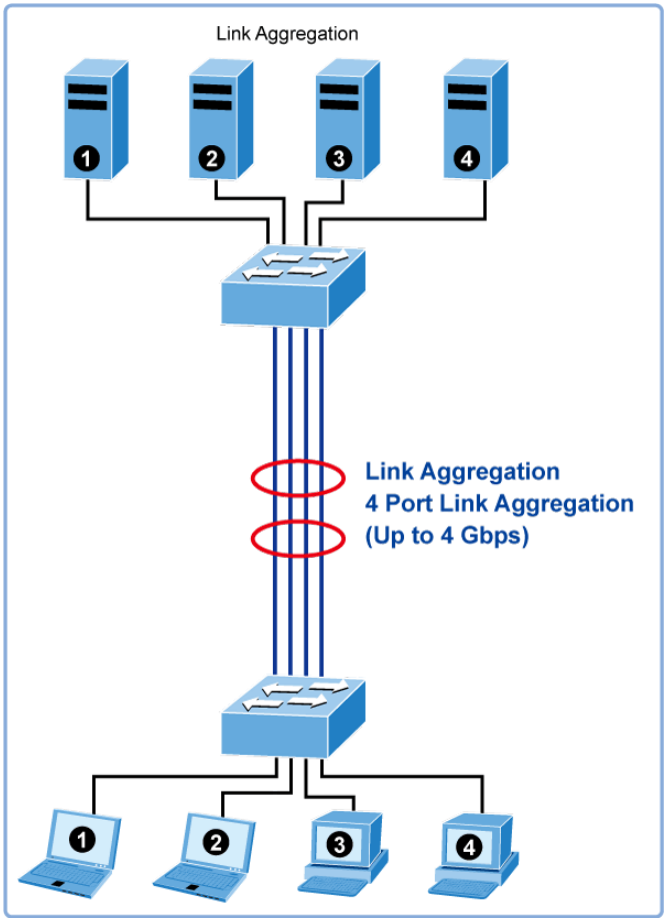
Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

Aggregated links can be assigned manually (Port Trunk) or automatically by enabling Link Aggregation Control Protocol (LACP) on the relevant links.

Aggregated links are treated by the system as a single logical port. Specifically, the aggregated link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, duplex setting, etc.

The managed switch supports the following aggregation links :

- Static LAGs (Port Trunk) – Force aggregated selected ports to be a trunk group.
- Link Aggregation Control Protocol (LACP) LAGs – LACP LAGs negotiate aggregated port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.



The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between partner systems that require high speed redundant links. Link aggregation permits grouping up to eight consecutive ports into a single

dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode (refer to the IEEE 802.3ad standard for further details).

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation permits grouping up to four consecutive ports into a single dedicated connection between any two managed switches or other Layer 2 switches. However, before making any physical connections between devices, use the link aggregation configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

- The ports used in a link aggregation must all be of the same media type (RJ45, 100 Mbps fiber).
- The ports that can be assigned to the same link aggregation have certain other restrictions (see below).
    - Ports can only be assigned to one link aggregation.
    - The ports at both ends of a connection must be configured as link aggregation ports.
    - None of the ports in a link aggregation can be configured as a mirror source port or a mirror target port.
    - All of the ports in a link aggregation have to be treated as a whole when moved from/to, added or deleted from a VLAN.
    - The Spanning Tree Protocol will treat all the ports in a link aggregation as a whole.
    - Enable the link aggregation prior to connecting any cable between the switches to avoid creating a data loop.
    - Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to avoid creating a data loop.

It allows a maximum of 10 ports to be aggregated at the same time. The managed switch supports Gigabit Ethernet ports (up to five groups). If the group is defined as a LACP static link aggregationing group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregationing group, then the number of ports must be the same as the group member ports.

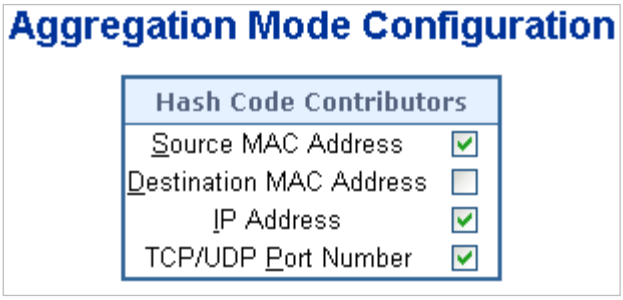
The aggregation code ensures that frames belonging to the same frame flow (for example, a TCP connection) are always forwarded on the same link aggregation member port. Reording of frames within a flow is therefore not possible. The aggregation code is based on the following information:

- Source MAC
- Destination MAC
- Source and destination IPv4 address.
- Source and destination TCP/UDP ports for IPv4 packets

Normally, all five contributions to the aggregation code should be enabled to obtain the best traffic distribution among the link aggregation member ports. Each link aggregation may consist of up to 10 member ports. Any quantity of link aggregations may be configured for the device (they are only limited by the quantity of ports on the device). To configure a proper traffic distribution, the ports within a link aggregation must use the same link speed.

Static aggregation

The Aggregation Mode Configuration page is used to configure the aggregation hash mode and the aggregation group. The aggregation hash mode settings are global, whereas the aggregation group relate to the current device, as reflected by the page header.



The page includes the following fields:

Object	Description
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame. Select the check box to enable the use of the Source MAC address, or uncheck it to disable. By default, the Source MAC Address is enabled.
Destination MAC Address	The Destination MAC Address can be used to calculate the destination port for the frame. Select the check box to enable the use of the Destination MAC Address, or uncheck it to disable. By default, the Destination MAC Address is disabled.
IP Address	The IP address can be used to calculate the destination port for the frame. Select the check box to enable the use of the IP Address, or uncheck it 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. Select the check box to enable the use of the TCP/UDP Port Number, or uncheck it to disable. By default, the TCP/UDP Port Number is enabled.

Static aggregation group configuration

The page includes the following fields:

Object	Description
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.

Buttons

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

LACP configuration

LACP LAG negotiates aggregated port links with other LACP ports located on a different device. LACP allows switches connected to each other to discover automatically whether any ports are member of the same LAG.

This page allows the user to inspect and change the current LACP port configurations. The LACP port settings relate to the current device, as reflected by the page header.

The page includes the following fields:

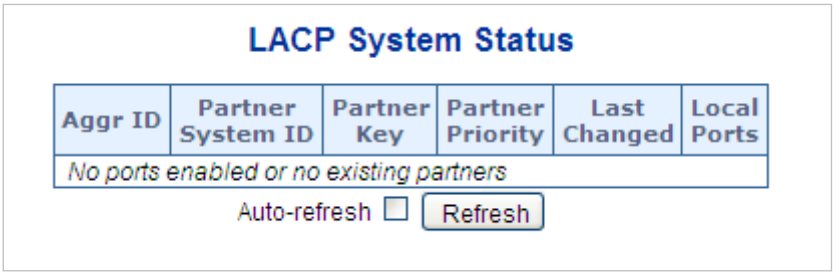
Object	Description
Port	The switch port number.
LACP Enabled	Controls whether or not LACP is enabled on this switch port. LACP will form an aggregation when two or more ports are connected to the same partner.
Key	The Key value incurred by the port, range 1-65535. Selecting **Auto** (default setting) sets 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** selection transmits LACP packets each second, while the **Passive** setting waits for a LACP packet from a partner (speak if spoken to).
Timeout	The Timeout controls the period between BPDU transmissions. **Fast** transmits LACP packets each second, while the **Slow** selection provides a wait for 30 seconds before sending a LACP packet.
Priority	The Priority 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 controls which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

LACP system status

The LACP System Status page provides a status overview of all LACP instances. This page displays the current LACP aggregation groups and LACP port status.



The page includes the following fields:

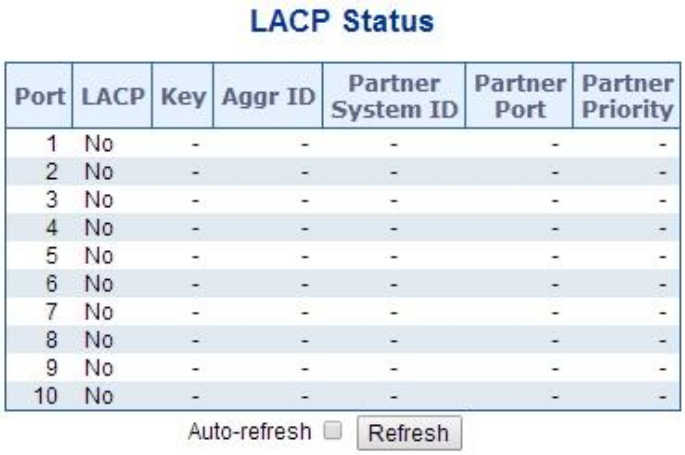
Object	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the ID is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The key that the partner has assigned to this aggregation ID.
Partner Priority	The priority of the aggregation partner.
Last changed	The time since this aggregation changed.
Local Ports	Shows which ports are a part of this aggregation for this switch.

Buttons

- Click **Refresh** to to refresh the page immediately.
- Select the **Auto-refresh** check box to automatically refresh the page every three seconds.

LACP port status

The LACP Status page provides a LACP status overview of all ports. This page displays the current LACP aggregation groups and LACP port status.



The page includes the following fields:

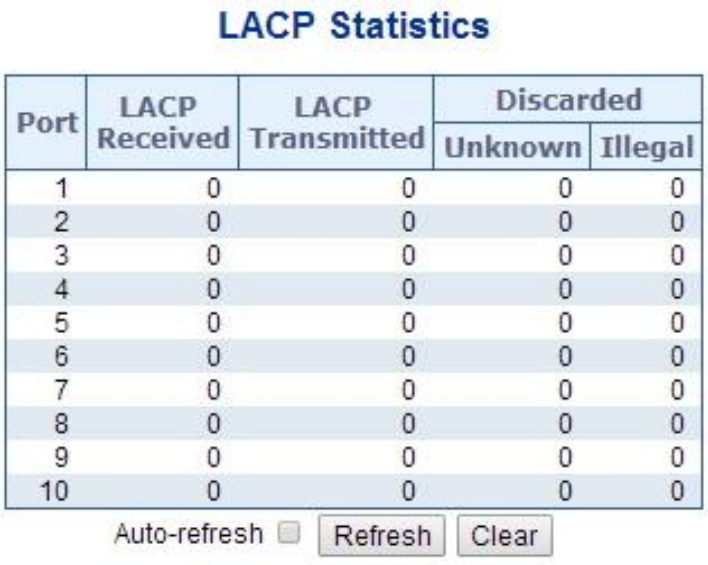
Object	Description
Port	The switch port number.
LACP	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other ports leave. Until that occurs, its LACP status is disabled.
Key	The key is assigned to this port. Only ports with the same key can aggregate together.
Aggregation ID	The aggregation ID assigned to this aggregation group.
Partner System ID	The partner’s system ID (MAC address).
Partner Port	The partner’s port number connected to this port.
Partner Priority	The partner's port priority.

Buttons

- Click **Refresh** to to refresh the page immediately.
- Select the **Auto-refresh** check box to automatically refresh the page every three seconds.

LACP port statistics

The LACP Statistics page provides an overview of LACP statistics for all ports.



The page includes the following fields:

Object	Description
Port	The switch port number.
LACP Received	Shows how many LACP frames have been sent from each port.
LACP Transmitted	Shows how many LACP frames have been received at each port.
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

- Click **Refresh** to to refresh the page immediately.
- Click **Clear** to clear the counters for all ports
- Select the **Auto-refresh** to automatically refresh the page every three seconds.

VLAN

VLAN overview

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily. VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded only to members of the VLAN on which the broadcast was initiated.

Note:

1. Regardless of the method used to uniquely identify end nodes and assign VLAN membership to these nodes, packets cannot cross VLAN without a network device performing a routing function between the VLANs.
2. The managed switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.

Note: The managed switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As a new VLAN is created, the member ports assigned to the new VLAN are removed from the DEFAULT_ VLAN port member list. The DEFAULT_VLAN has a VID = 1.

This section has the following items:

VLAN Port Configuration	Enables VLAN group
VLAN Membership Status	Displays VLAN membership status
VLAN Port Status	Displays VLAN port status
Private VLAN	Creates/removes primary or community VLANs
Port Isolation	Enables/disablse port isolation on port
MAC-based VLAN	Configures the MAC-based VLAN entries
MAC-based VLAN Status	Displays MAC-based VLAN entries
Protocol-based VLAN	Configures the protocol-based VLAN entries
Protocol-based VLAN Membership	Displays the protocol-based VLAN entries

IEEE 802.1Q VLAN

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This managed switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by permitting relocation of devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as email), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and permit network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This managed switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard.
- Port overlapping, allowing a port to participate in multiple VLANs.
- End stations can belong to multiple VLANs.
- Passing traffic between VLAN-aware and VLAN-unaware devices.
- Priority tagging

IEEE 802.1Q standard

IEEE 802.1Q (tagged) VLAN are implemented on the Switch. 802.1Q VLAN require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q compliant).

VLAN allows a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast, and unicast packets from unknown sources.

VLAN can also provide a level of security to the network. IEEE 802.1Q VLAN only delivers packets between stations that are members of the VLAN. Any port can be configured as either tagging or untagging:

- The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers.
- The tagging feature allows VLAN to span multiple 802.1Q compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Some relevant terms:

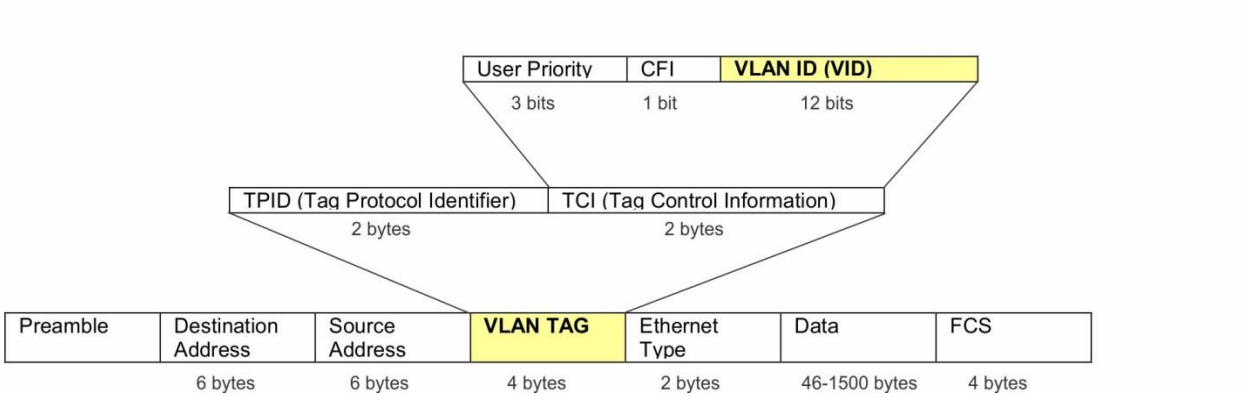
- **Tagging** – The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** – The act of stripping 802.1Q VLAN information out of the packet header.

802.1Q VLAN tags

There are four additional octets inserted after the source MAC address as shown in the following 802.1Q tag diagram. Their presence is indicated by a value of 0x8100 in the Ether Type field. When a packet's Ether Type field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of three bits of user priority: One bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The three bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

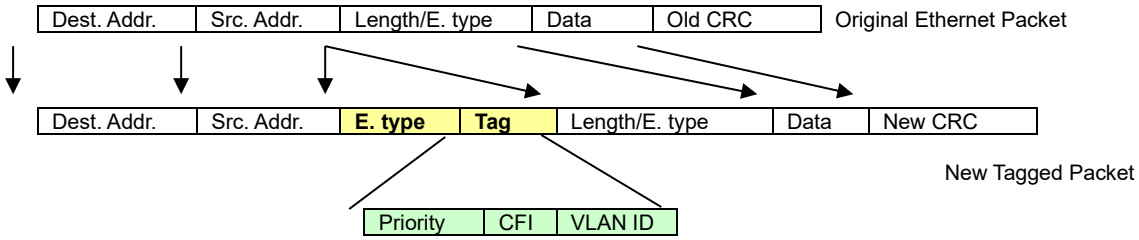
The tag is inserted into the packet header making the entire packet longer by four octets. All of the information originally contained in the packet is retained.

802.1Q tag



The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q tag



Port VLAN ID

Packets that are tagged (carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLAN to span network devices as well as the entire network if all network devices are 802.1Q compliant.

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID for use within the switch. If no VLANs are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the VID, not the PVID, is used to make packet forwarding decisions.

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch compares the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the switch drops the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Default VLANs

The managed switch initially configures one VLAN, VID = 1, called "default." The factory default setting assigns all ports on the Switch to the "default." As new VLANs are configured in port-based mode, their respective member ports are removed from the "default."

Assigning ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default, all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port to have it carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then this port should be added to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing them on to any end-node host that does not support VLAN tagging.

VLAN classification

When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). If the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

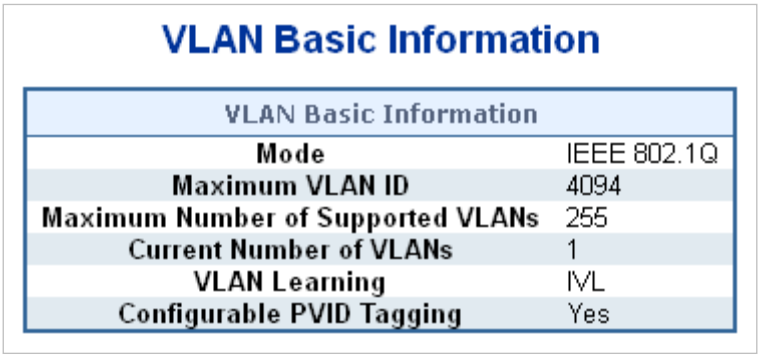
Port overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs that do not overlap but still need to communicate, they can be connected by enabling routing on this switch.

Untagged VLANs

Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

VLAN basic information



The page includes the following fields:

Object	Description
Mode	Displays the current VLAN mode used by the managed switch: Port-Based IEEE 802.1Q VLAN
Maximum VLAN ID	Maximum VLAN ID recognized by the managed switch.
Maximum Number of Supported VLANs	Maximum number of VLANs that can be configured on the managed switch.
Current number of VLANs	Display the current number of VLANs
VLAN Learning	Display the VLAN learning mode. The managed switch supports IVL (IVL Independent vlan learning).
Configurable PVID Tagging	Indicates whether or not configurable PVID tagging is implemented.

VLAN port configuration

The Global VLAN Configuration page is used for configuring the managed switch port VLAN. This page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is also configured on this page. All untagged packets arriving to the device are tagged by the port's PVID.

Managed switch nomenclature:

IEEE 802.1Q tagged and untagged

Every port on an 802.1Q compliant switch can be configured as tagged or untagged.

Tagged: Ports with tagging enabled put the VID number, priority, and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.

Untagged: Ports with untagging enabled strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port have no

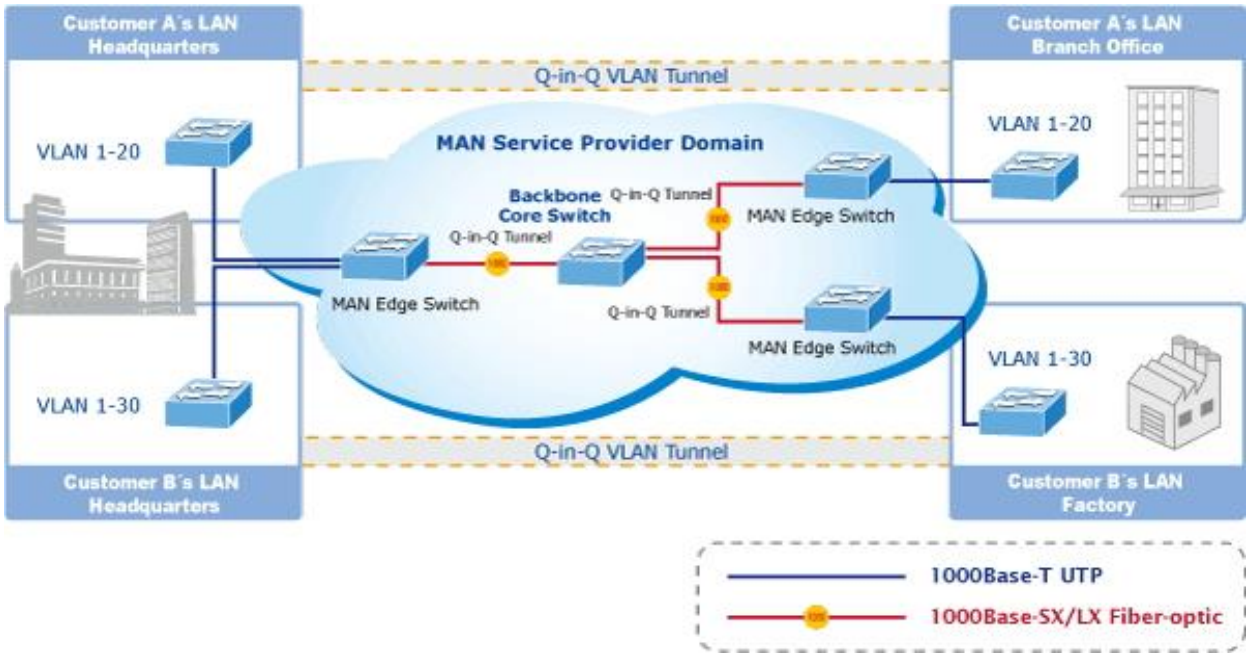
802.1Q VLAN information (remember that the PVID is only used internally within the managed switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Frame Income / Frame Leave	Income Frame is **tagged**	Income Frame is **untagged**
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remains untagged

IEEE 802.1Q tunneling (Q-in-Q)

IEEE 802.1Q tunneling (Q-in-Q) is designed for service providers carrying traffic for multiple customers across their networks. Q-in-Q tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.



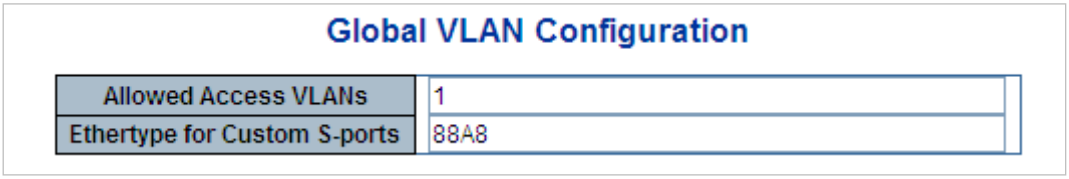
The managed switch supports multiple VLAN tags and can therefore be used in MAN (Metro Access Network) applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the MAN space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving

the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

This provides a tunneling mechanism to connect remote customer VLANs through a common MAN space without interfering with the VLAN tags. All tags use EtherType 0x8100 or 0x88A8, where 0x8100 is used for customer tags and 0x88A8 is used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements are reduced.

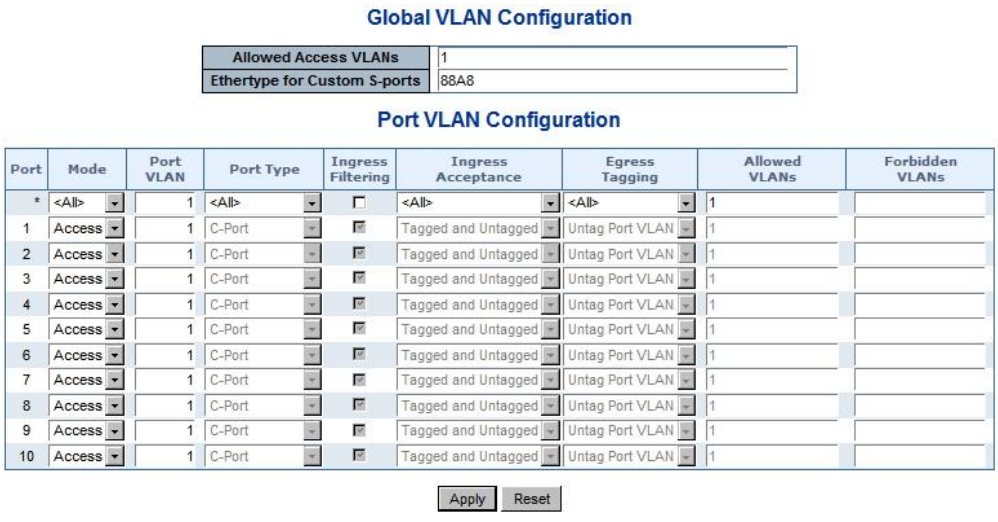
Global VLAN configuration



The page includes the following fields:

Object	Description
Allowed Access VLANs	This field shows the allowed Access VLANs. 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 boundaries. The following example creates 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



The page includes the following fields:

Object		Description
Port		This is the logical port number for this row.
Mode	**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 (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 add 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 (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.

Object	Description
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 (**Ingress Filtering** check box is selected), 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	This option is only available for ports in Hybrid mode. 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.

Object	Description
Allowed VLANs	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. 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 a member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. Such VLANs should be marked 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.

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

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

VLAN membership status

The VLAN Membership Status for Combined users page provides an overview of membership status for VLAN users.

The page includes the following fields:

Object	Description
VLAN User	A VLAN User is a module that uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID and UVID. Currently, we support following VLAN : **Admin** : This is referred to as static.

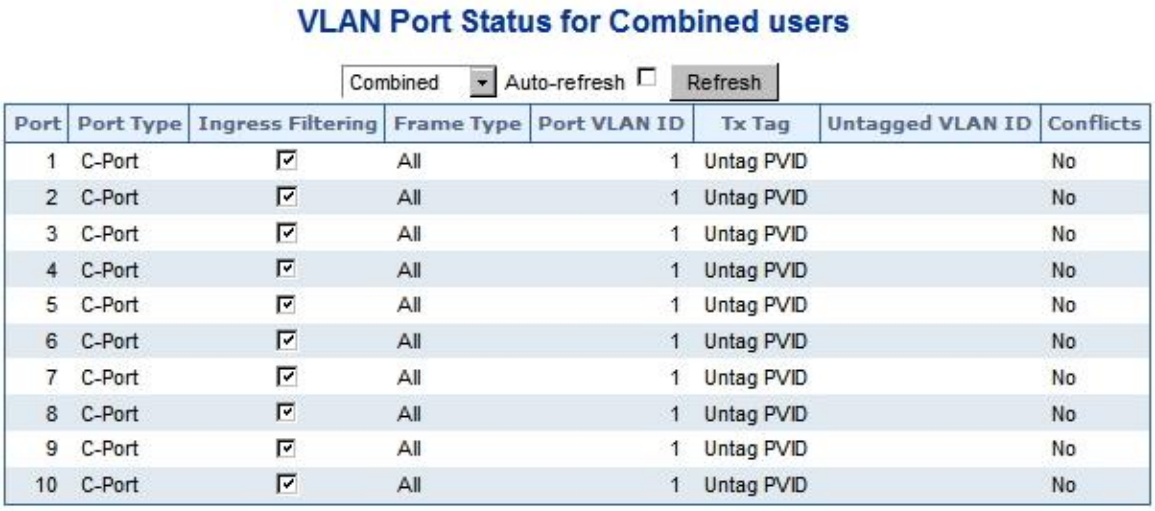
Object	Description
	NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server. **GVRP** : GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network . **Voice VLAN** : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones. **MVR** : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.
Port Members	A row of check boxes for each port appears for each VLAN ID. If a port is included in a VLAN, an image appears. If a port is included in a Forbidden port list, an image appears. If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then the conflict port appears as a conflict port.
VLAN Membership	The VLAN Membership Status Page shows the current VLAN port members for all VLANs configured by a selected VLAN user (selection shall be allowed by a Combo Box). When ALL VLAN users are selected, it shows this information for all the VLAN users by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Buttons

- Select **VLAN Users** from the **Combined** drop-down list.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **I<<** to update the table starting from the first entry in the VLAN Table (i.e., the entry with the lowest VLAN ID).
- Click **>>** to update the table, starting with the entry after the last entry currently displayed.

VLAN port status

The VLAN Port Status for Combined users page provides VLAN port status.



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

The page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row.
Port Type	Shows the VLAN Awareness for the port. If VLAN awareness is enabled, the tag is removed from tagged frames received on the port. VLAN tagged frames are classified to the VLAN ID in the tag. If VLAN awareness is disabled, all frames are classified to the Port VLAN ID and tags are not removed.
Ingress Filtering	Shows the ingress filtering for a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded.
Frame Type	Shows if the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.
Port VLAN ID	Shows the PVID setting for the port.
Tx Tag	Shows egress filtering frame status (tagged or untagged).
Untagged VLAN ID	Shows UVID (untagged VLAN ID). The port's UVID determines the packet's behavior at the egress side.
Conflicts	Shows whether or not conflicts exist. When a Volatile VLAN user requests to set VLAN membership or VLAN port configuration, the following conflicts can occur: • Functional conflicts between features. • Conflicts due to hardware limitations. • Direct conflict between user modules.

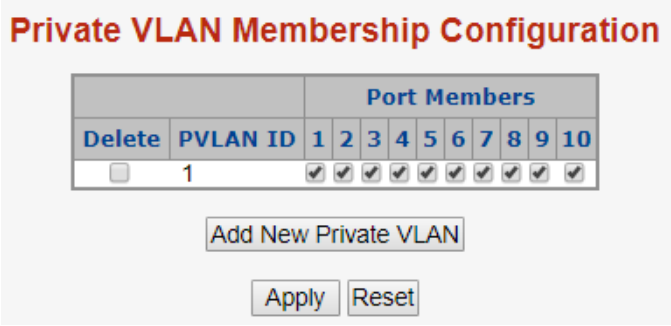
Buttons

- Select **VLAN Users** from the **Static** drop-down list.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.

- Click **Refresh** to refresh the page immediately.

Private VLAN

The Private VLAN Membership Configuration page allows you to configure private VLAN membership. The private VLAN membership configurations for the switch can be monitored and modified here; private VLANs and private VLAN port members can be added or deleted 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 are 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.



The page includes the following fields:

Object	Description
Delete	Select this check box to delete a private VLAN entry. 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, select the check box. To remove or exclude the port from the private VLAN, make sure the box is deselected. By default, no ports are members, and all boxes are deselected.
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 **Apply**. The **Delete** button can be used to undo the addition of new Private VLANs.

Buttons

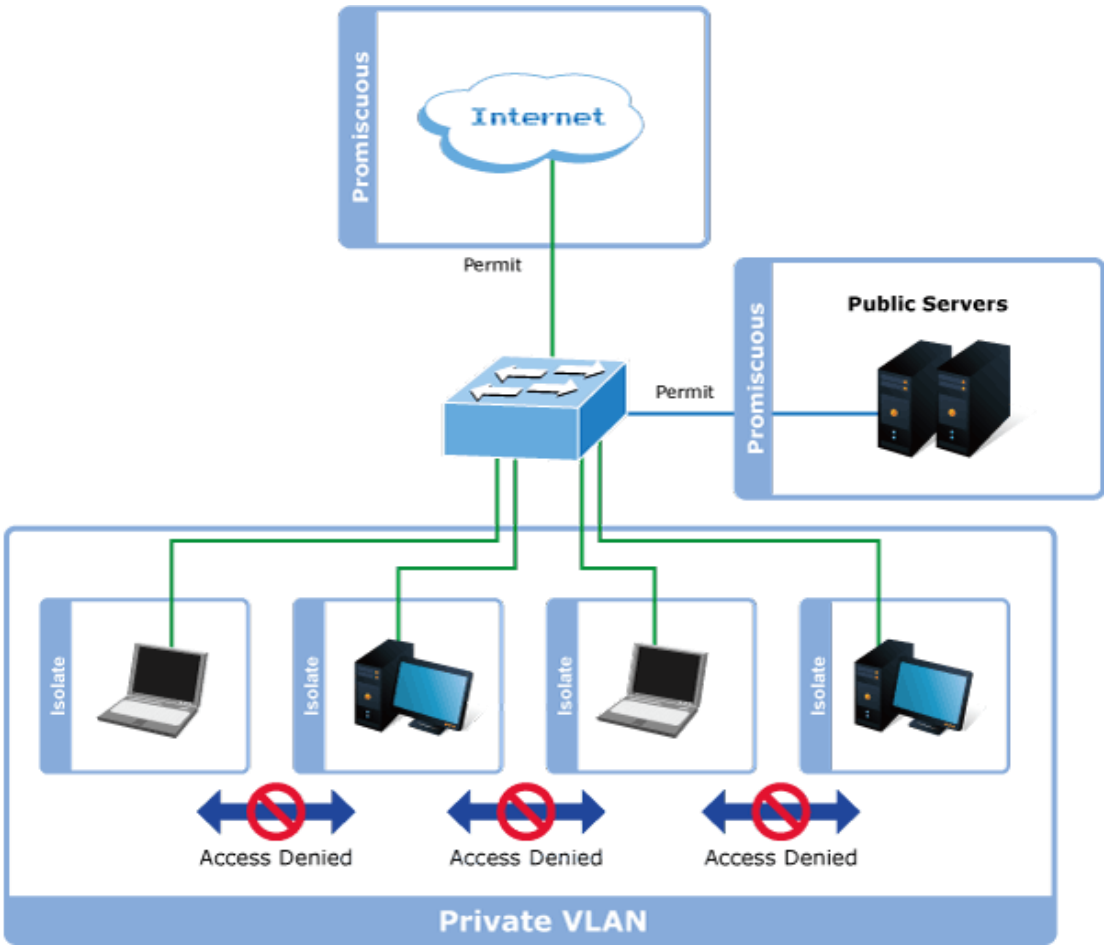
- Click **Add New Private VLAN** to add a new private VLAN ID.

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port isolation

When a VLAN is configured to be a private VLAN, communication between ports within that VLAN can be prevented. Two application examples are provided in this section:

- Customers connected to an ISP can be members of the same VLAN, but they are not allowed to communicate with each other within that VLAN.
- Servers in a farm of web servers in a Demilitarized Zone (DMZ) are allowed to communicate with the outside world and with database servers on the inside segment, but are not allowed to communicate with each other.



For private VLANs to be applied, the switch must first be configured for standard VLAN operation. When this is in place, one or more of the configured VLANs can be configured as private VLANs. Ports in a private VLAN fall into one of these two groups:

Promiscuous ports

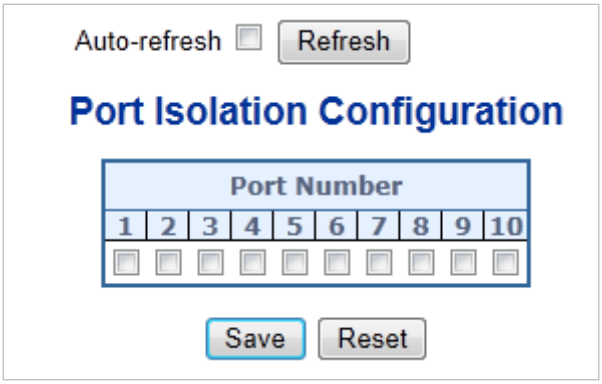
- Ports from which traffic can be forwarded to all ports in the private VLAN.
- Ports that can receive traffic from all ports in the private VLAN.

Isolated ports

- Ports from which traffic can only be forwarded to promiscuous ports in the private VLAN.
- Ports that can receive traffic from only promiscuous ports in the private VLAN.

The configuration of promiscuous and isolated ports applies to all private VLANs. When traffic comes in on a promiscuous port in a private VLAN, the VLAN mask from the VLAN table is applied. When traffic comes in on an isolated port, the private VLAN mask is applied in addition to the VLAN mask from the VLAN table. This reduces the ports to which forwarding can be done to just the promiscuous ports within the private VLAN.

The Port Isolation Configuration 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 and private VLAN.



The page includes the following fields:

Object	Description
Port Members	A check box is provided for each port of a private VLAN. When selected, port isolation is enabled on that port. When deselected, port isolation is disabled on that port. By default, port isolation is **disabled** on all ports.

Buttons

- Click **Save** to save changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

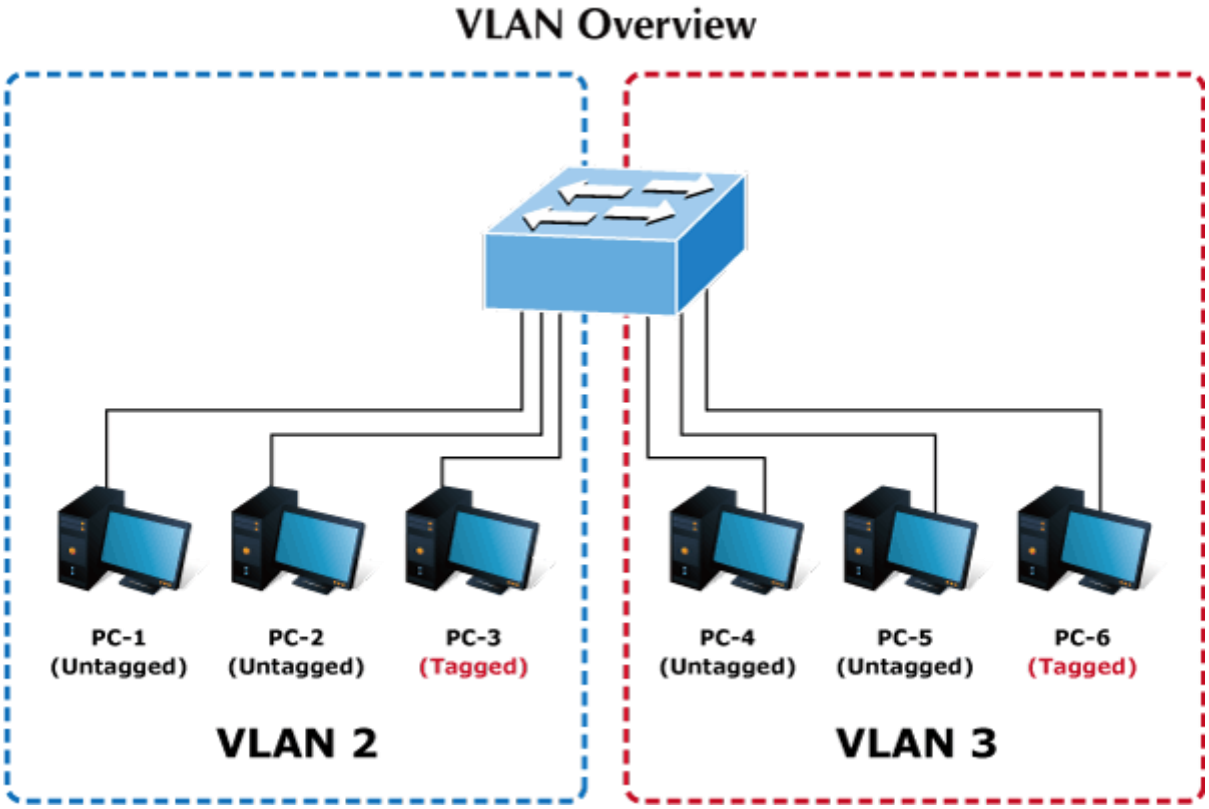
VLAN setting examples

This section covers the following setup scenarios:

- Separate VLAN
- 802.1Q VLAN Trunk
- Port Isolate

Two Separate 802.1Q VLANs

The diagram below shows how the managed switch handles tagged and untagged traffic flow for two VLANs. VLAN Group 2 and VLAN Group 3 are separated VLANs. Each VLAN isolates network traffic, so only members of the VLAN receive traffic from the same VLAN members. The table below describes the port configuration of the managed switches.



VLAN Group	VID	Untagged Members	Tagged Members
VLAN Group 1	1	Port-7 ~ Port-10	N/A
VLAN Group 2	2	Port-1, Port-2	Port-3
VLAN Group 3	3	Port-4, Port-5	Port-6

The scenario is described as follows:

Untagged packet entering VLAN 2

1. While [PC-1], an untagged packet, enters Port-1, the managed switch will tag it with a VLAN Tag=2. [PC-2] and [PC-3] will receive the packet through Port-2 and Port-3.

2. [PC-4],[PC-5] and [PC-6] received no packet.
3. While the packet leaves Port-2, it will be stripped away, becoming an untagged packet.
4. While the packet leaves Port-3, it will remain as a tagged packet with VLAN Tag=2.

Tagged packet entering VLAN 2

1. While [PC-3], a tagged packet with VLAN Tag=2 enters Port-3, [PC-1] and [PC-2] will receive the packet through Port-1 and Port-2.
2. While the packet leaves Port-1 and Port-2, it will be stripped away, becoming an untagged packet.

Untagged packet entering VLAN 3

1. While [PC-4] an untagged packet enters Port-4, the switch will tag it with a VLAN Tag=3. [PC-5] and [PC-6] will receive the packet through Port-5 and Port-6.
2. While the packet leaves Port-5, it will be stripped away, becoming an untagged packet.
3. While the packet leaves Port-6, it will keep as a tagged packet with VLAN Tag=3.

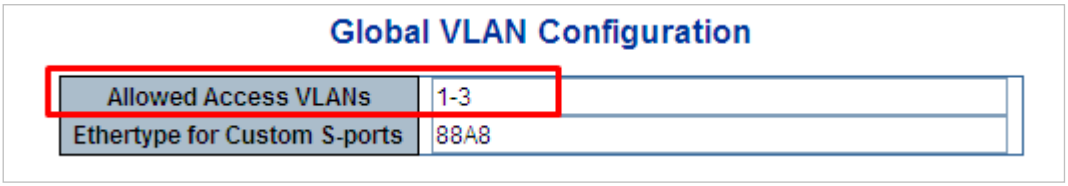
Note: For this example, set VLAN Group 1 as the default VLAN, but only focus on VLAN 2 and VLAN 3 traffic flow.

Setup steps

1. Add VLAN group

   Add two VLANs – VLAN 2 and VLAN 3

   Type 1-3 in an Allowed Access VLANs column, the 1-3 includes VLAN1 and 2 and 3.

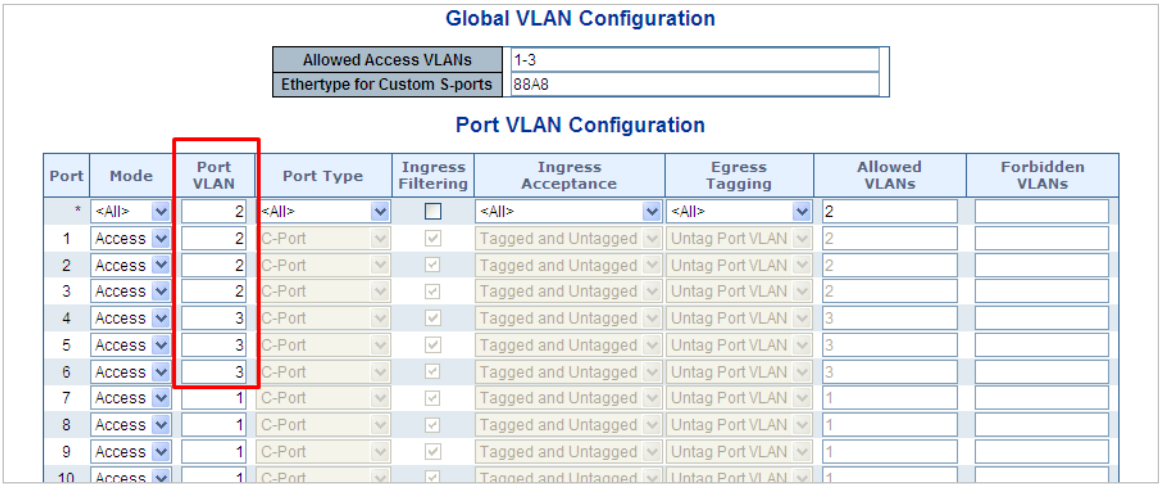


2. Assign VLAN members and PVIDs to each port:

   VLAN 2 : Port-1,Port-2 and Port-3

   VLAN 3 : Port-4, Port-5 and Port-6

   VLAN 1 : All other ports – Port-7~Port-28

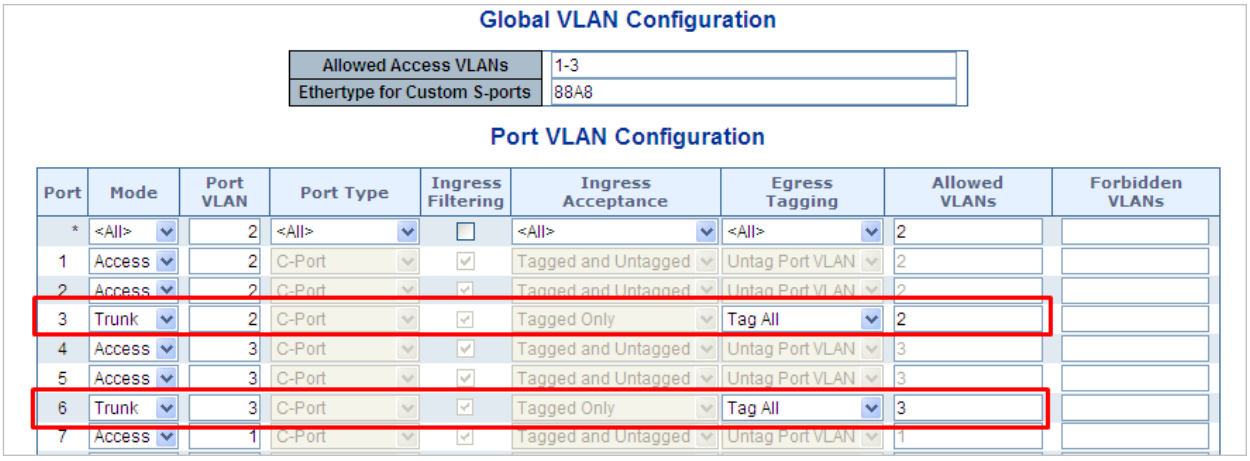


3. Enable VLAN Tag for specific ports

   Link Type: Port-3 (VLAN-2) and Port-6 (VLAN-3)

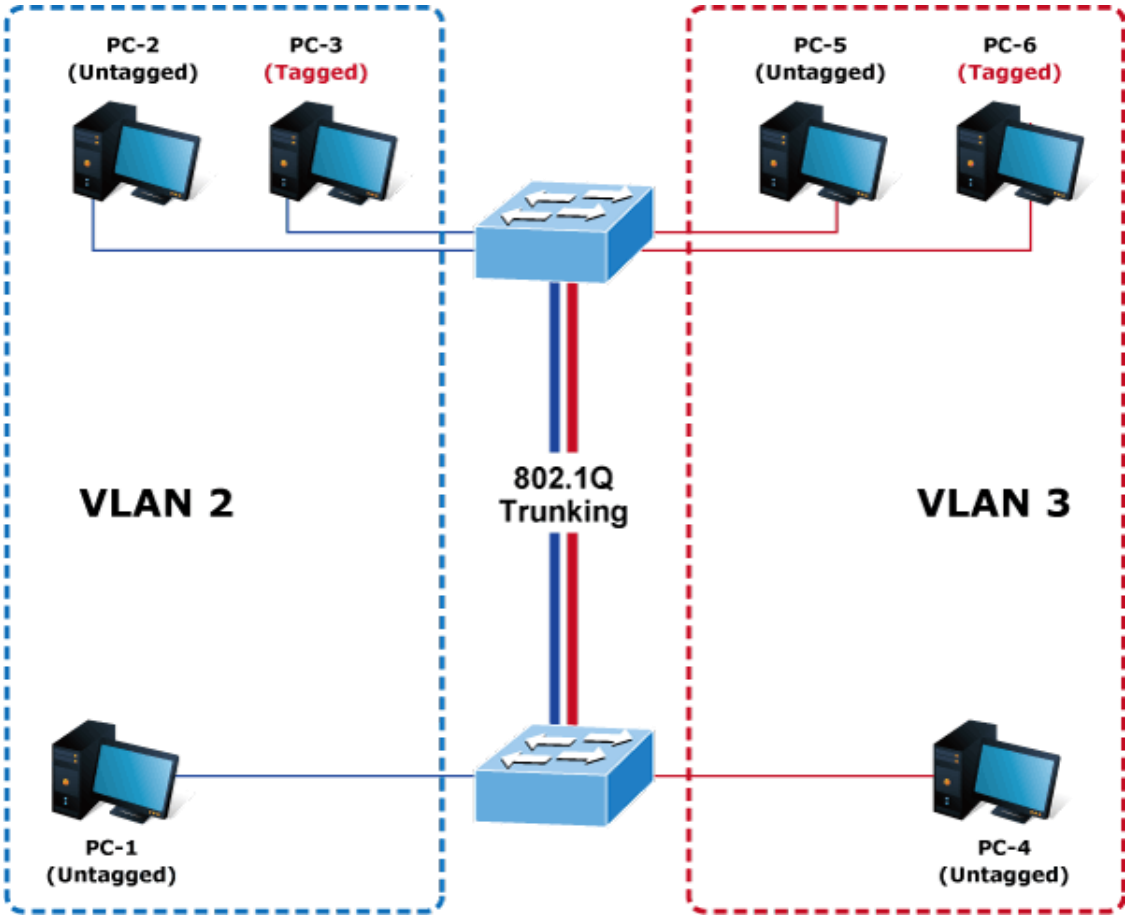
   Change Port 3 Mode as Trunk and select Egress Tagging as **Tag All** and Types 2 in the Allowed VLANs column.

   Change Port 6 Mode as Trunk and select Egress Tagging as **Tag All** and Types 3 in the allowed VLANs column.



VLAN trunking between two 802.1Q-aware switches

In most cases, they are used for “Uplink” to other switches. VLANs are separated at different switches, but they need access to other switches within the same VLAN group.

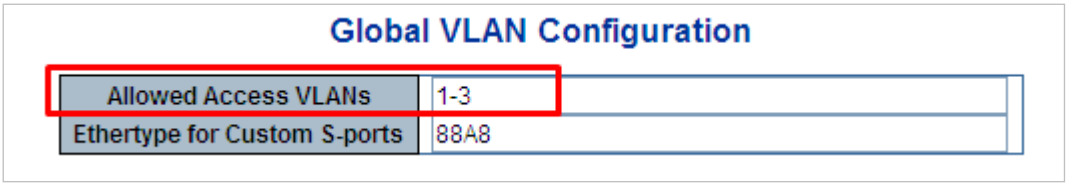


Setup steps

1. Add a VLAN group.

   Add two VLANs – VLAN 2 and VLAN 3

   Type 1-3 in the allowed Access VLANs column; the 1-3 includes VLAN 1 and 2 and 3.

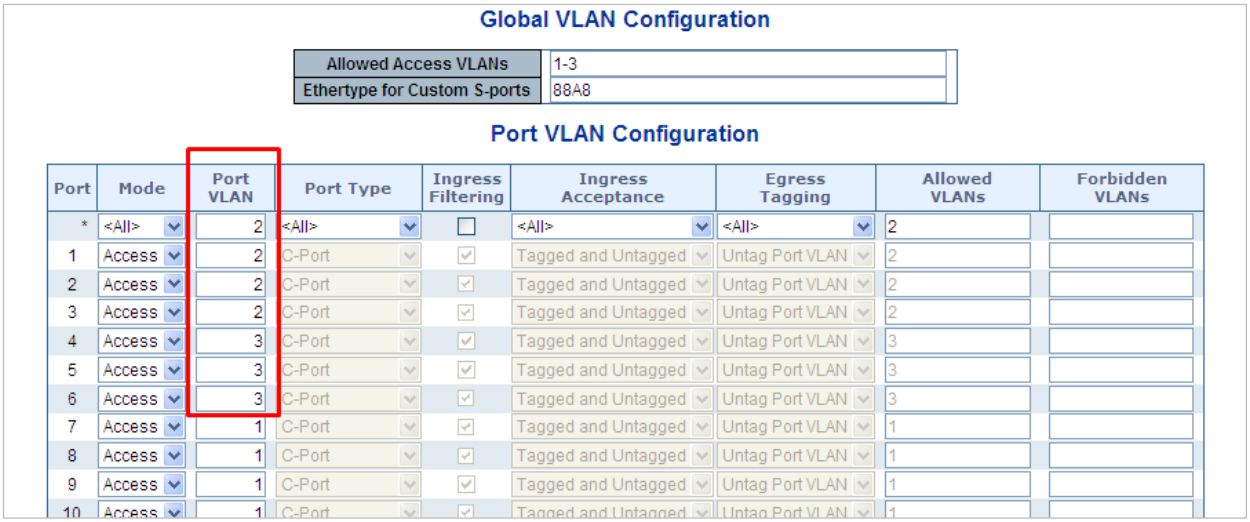


2. Assign VLAN members and PVIDs to each port:

   VLAN 2: Port-1, Port-2 and Port-3

   VLAN 3: Port-4, Port-5 and Port-6

   VLAN 1: All other ports – Port-7~Port-48



Global VLAN Configuration

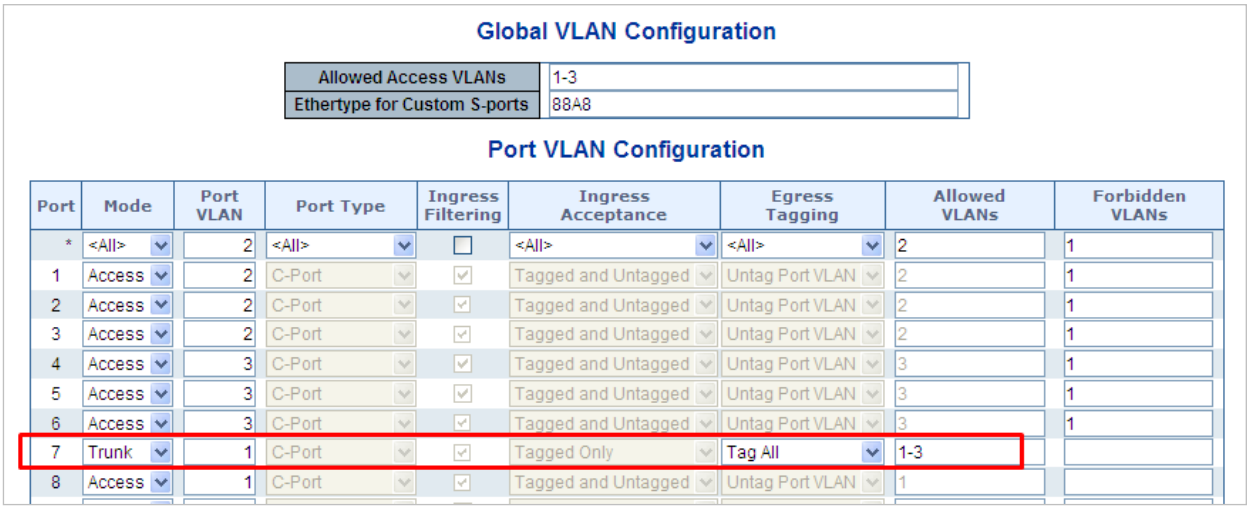
Allowed Access VLANs	1-3
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<All>	2	<All>	☐	<All>	<All>	2	
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
2	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
3	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
4	Access	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	3	
5	Access	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	3	
6	Access	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	3	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

For the VLAN ports connecting to the hosts, see “IP subnet-based VLAN” on page 123 for examples. The following steps focus on the VLAN trunk port configuration.

1. Specify Port-7 to be the 802.1Q VLAN Trunk port.
2. Assign Port-7 to both VLAN 2 and VLAN 3 on the VLAN Member configuration page.
3. Define a VLAN 1 as a “Public Area” that overlaps with both VLAN 2 members and VLAN 3 members.
4. Assign the VLAN Trunk Port to being the member of each VLAN to be aggregated. For example, include Port-7 to be VLAN 2 and VLAN 3 member ports.
5. Specify Port-7 to be the 802.1Q VLAN trunk port, and the trunking port must be a tagged port during egress. The Port-7 configuration is shown below.



Global VLAN Configuration

Allowed Access VLANs	1-3
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

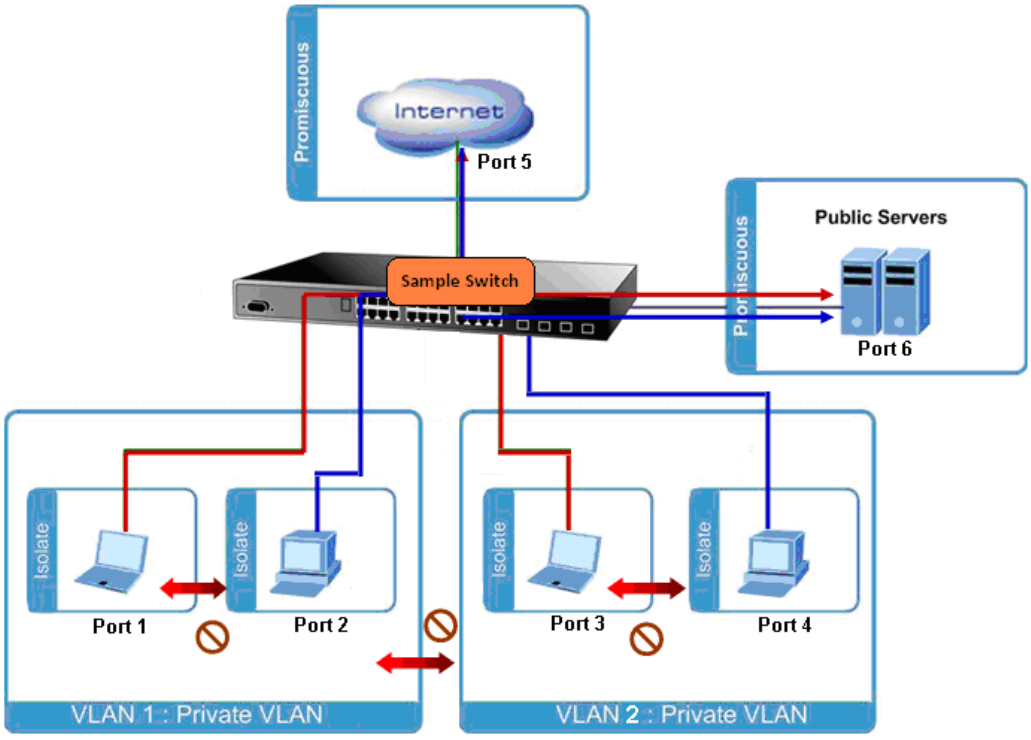
Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<All>	2	<All>	☐	<All>	<All>	2	1
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	1
2	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	1
3	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	1
4	Access	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	3	1
5	Access	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	3	1
6	Access	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	3	1
7	Trunk	1	C-Port	☑	Tagged Only	Tag All	1-3	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Both the VLAN 2 members of Port-1 to Port-3 and VLAN 3 members of Port-4 to Port-6 belong to VLAN 1. But with different PVID settings, packets from VLAN 2 or VLAN 3 are not able to access the other VLAN.

6. Repeat Steps 1 to 5 by setting up the VLAN trunk port at the partner switch and add more VLANs to join the VLAN trunk. Repeat Steps 1 to 3 to assign the trunk port to the VLANs.

Port isolate

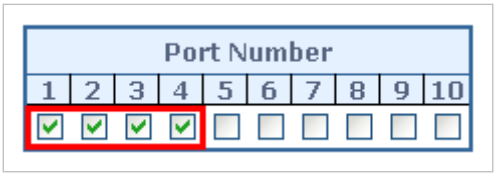
The diagram below shows how the managed switch handles isolated and promiscuous ports, and how computers are not able to access the each other's isolated port. However, each computer requires access to the same server/AP/Printer. This section explains how to configure the port for the server so that it can be accessed by each isolated port.



1. Assign Port Mode

   Set Port-1~Port-4 as isolated.

   Set Port-5 and Port-6 as promiscuous. The Port Isolation Configuration page appears.

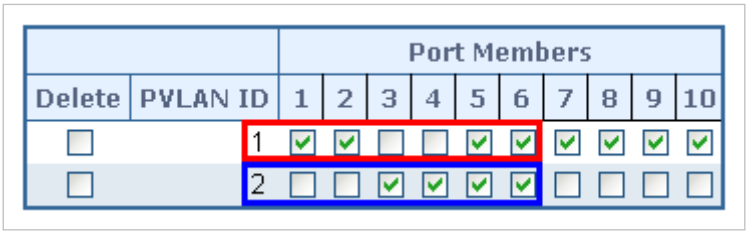


2. Assign VLAN Member:

   VLAN 1 : Port-1, Port-2, Port-5, and Port-3

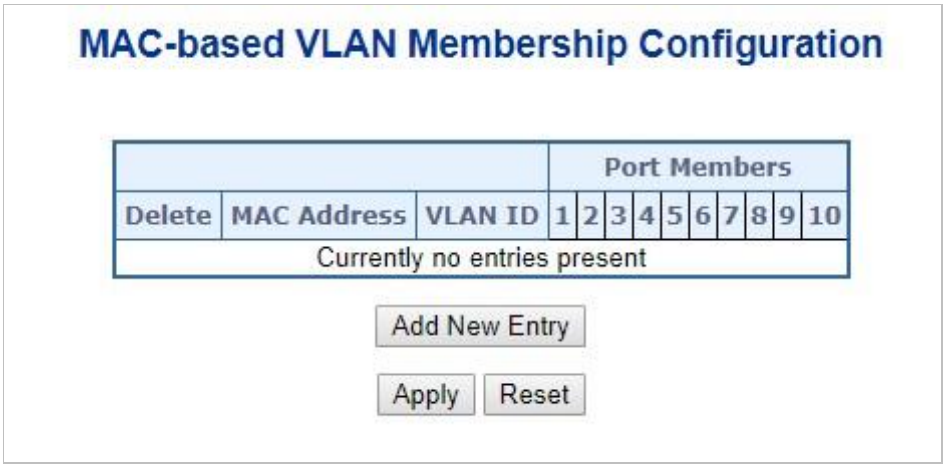
   VLAN 2: Port-3~Port-6.

   The Private VLAN Membership Configuration page appears.



MAC-based VLAN

The MAC-based VLAN entries can be configured on the MAC-based VLAN Membership Configuration page. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.



The page includes the following fields:

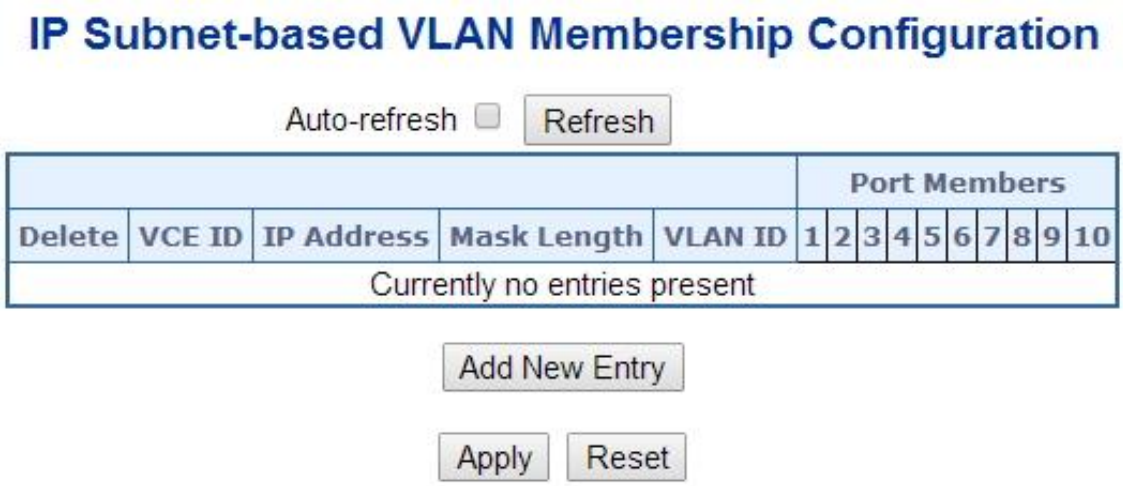
Object	Description
Delete	To delete a MAC-based VLAN entry, select this box and click **Save**.
MAC Address	Indicates the MAC address.
VLAN ID	Indicates the VLAN ID.
Port Members	A row of check boxes for each port appears for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, select the check box. To remove or exclude the port from the MAC-based VLAN, make sure the box is deselected. By default, no ports are members, and all boxes are deselected.
Adding a New MAC-based VLAN	Click **Add 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 when clicking **Save**. A MAC-based VLAN without any port members will be deleted when clicking **Save**. The **Delete** button can be used to undo the addition of new MAC-based VLANs.

Buttons

- Click **Add New Entry** to add a new MAC-based VLAN entry
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **I<<** to update the table starting from the first entry in the MAC-based VLAN table.
- Click **>>** to update the table, starting with the entry after the last entry currently displayed.

IP subnet-based VLAN

The IP subnet-based VLAN entries can be configured on the IP Subnet-based VLAN Membership Configuration page. 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.



The page includes the following fields:

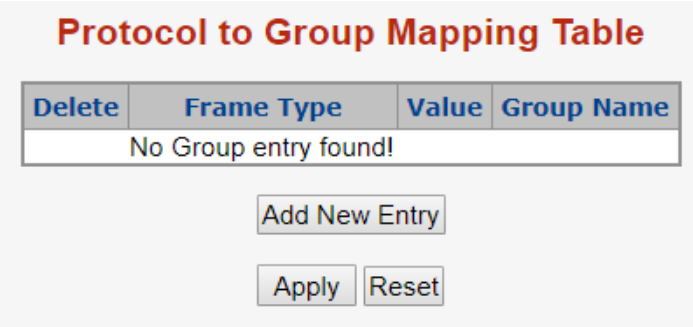
Object	Description
Delete	Select this box to delete a Protocol to Group Name map entry. The entry will be deleted on the switch during the next save.
VCE ID	Indicates the index of the entry. It is user configurable with a value range from 0-256. If a VCE ID is 0, the application will auto-generate the 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 displays for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, select the check box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is deselected. By default, no ports are members, and all boxes are deselected.
Add New Entry	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 when clicking **Save**. The **Delete** button can be clicked to undo the addition of new IP subnet-based VLANs.

Buttons

- Click **Add New Entry** to add a new MAC-based VLAN entry
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Protocol-based VLAN

The Protocol to Group Mapping Table page permits the addition of new protocols to the Group Name (unique for each Group) mapping entries, and allows you to see and delete entries already mapped for the switch.



The page includes the following fields:

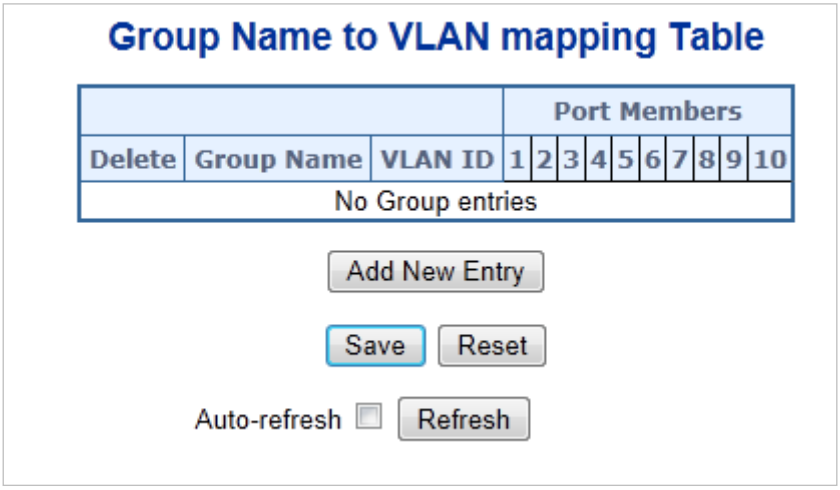
Object	Description
Delete	Select this box to delete a Protocol to Group Name map entry. The entry will be deleted on the switch during the next save.
Frame Type	Frame Type values are as follows: **Ethernet**, **LLC**, **SNAP** **Note**: When changing the Frame Type field, the **Value** field changes depending on the new frame type selected.
Value	Values that can be entered in this text field depend on the option selected in the Frame Type selection menu. Below are the criteria for three different frame types: **For Ethernet:** Values in the text field when Ethernet is selected as a Frame Type is called etype. Values for etype ranges from 0x0600-0xffff **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) **For SNAP**: A valid value in this case 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 the 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 that consists of a combination of alpha characters (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, and Frame Type, Value, and the Group Name can be configured as needed. Click the **Delete** button to undo the addition of a new entry.

Buttons

- Click **Add New Entry** to add a new MAC-based VLAN entry
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Protocol-based VLAN membership

The Group Name to VLAN Mapping Table page permits mapping an already configured Group Name to a VLAN.



The page includes the following fields:

Object	Description
Delete	Select this box to delete a Group Name to VLAN map entry. The entry will be deleted on the switch during the next save.
Group Name	A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alpha characters (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 the Protocol to Group mapping table and must not be used by any other existing mapping entry on this page.
VLAN ID	Indicates the ID to which the 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 to VLAN ID mapping. To include a port in a mapping, select the box. To remove or exclude the port from the mapping, make sure the box is deselected. By default, no ports are members, and all boxes are deselected.
Adding a New Group to VLAN mapping entry	Click the **Add New Entry** to add a new entry in mapping table. An empty row is added to the table, and Frame Type, Value, and the Group Name can be configured as needed. Click the **Delete** button to undo the addition of a new entry.

Buttons

- Click **Add New Entry** to add a new entry in the mapping table.
- Click **Save** to save changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Spanning Tree Protocol (STP)

Theory

STP can be used to detect and disable network loops, and to provide backup links between switches, bridges, or routers. This allows the switch to interact with other bridging devices in the network to ensure that only one route exists between any two stations on the network, and provides backup links that automatically take over when a primary link goes down. The spanning tree algorithms supported by this switch include these versions:

- **STP** – Spanning Tree Protocol (IEEE 802.1D)
- **RSTP** – Rapid Spanning Tree Protocol (IEEE 802.1w)
- **MSTP** – Multiple Spanning Tree Protocol (IEEE 802.1s)

The IEEE 802.1D Spanning Tree Protocol and IEEE 802.1w Rapid Spanning Tree Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the STP is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the spanning tree algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the spanning tree is incorrectly configured. Please read the following before making any changes from the default values.

The switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.

- Creates multiple spanning trees from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge protocol data units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier.
- The path cost to the root associated with each switch port.
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch.
- The path cost to the root from the transmitting port.
- The port identifier of the transmitting port.

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch.
- The shortest distance to the root switch is calculated for each switch.
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a stable STP topology

The goal is to make the root port the fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network becomes the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For example, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP port states

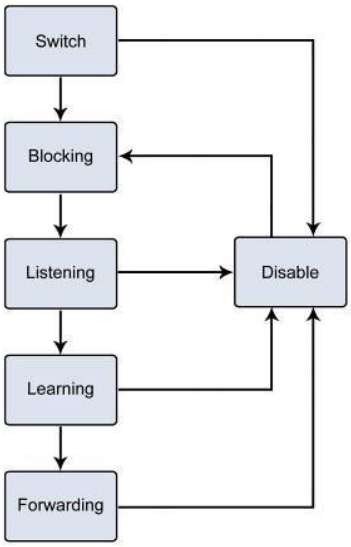
The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a blocking state to a forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists is in one of the following five states:

- **Blocking** – The port is blocked from forwarding or receiving packets.
- **Listening** – The port is waiting to receive BPDU packets that may tell the port to go back to the blocking state.
- **Learning** – The port is adding addresses to its forwarding database, but not yet forwarding packets.
- **Forwarding** – The port is forwarding packets.
- **Disabled** – The port only responds to network management messages and must return to the blocking state first.

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking.
- From blocking to listening or to disabled.
- From listening to learning or to disabled.
- From learning to forwarding or to disabled.
- From forwarding to disabled.
- From disabled to blocking.



You can modify each port state by using management software. When STP is enabled, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP-enabled ports until the forwarding state is enabled for that port.

STP parameters

STP operation levels

The managed switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

Note: On the switch level, STP calculates the bridge identifier for each switch and then sets the root bridge and the designated bridges. On the port level, STP sets the root port and the designated ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier (Not user configurable except by setting priority below)	A combination of the user-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: A 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC.	32768 + MAC
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount of time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port – lower numbers give a higher priority and a greater chance of a given port being elected as the root port	128
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 - Auto

Default spanning-tree configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768

User-changeable STA parameters

The factory default settings for the switch should cover the majority of installations. It is advisable to keep the default settings as set at the factory unless it is absolutely necessary. The user changeable parameters in the switch are as follows:

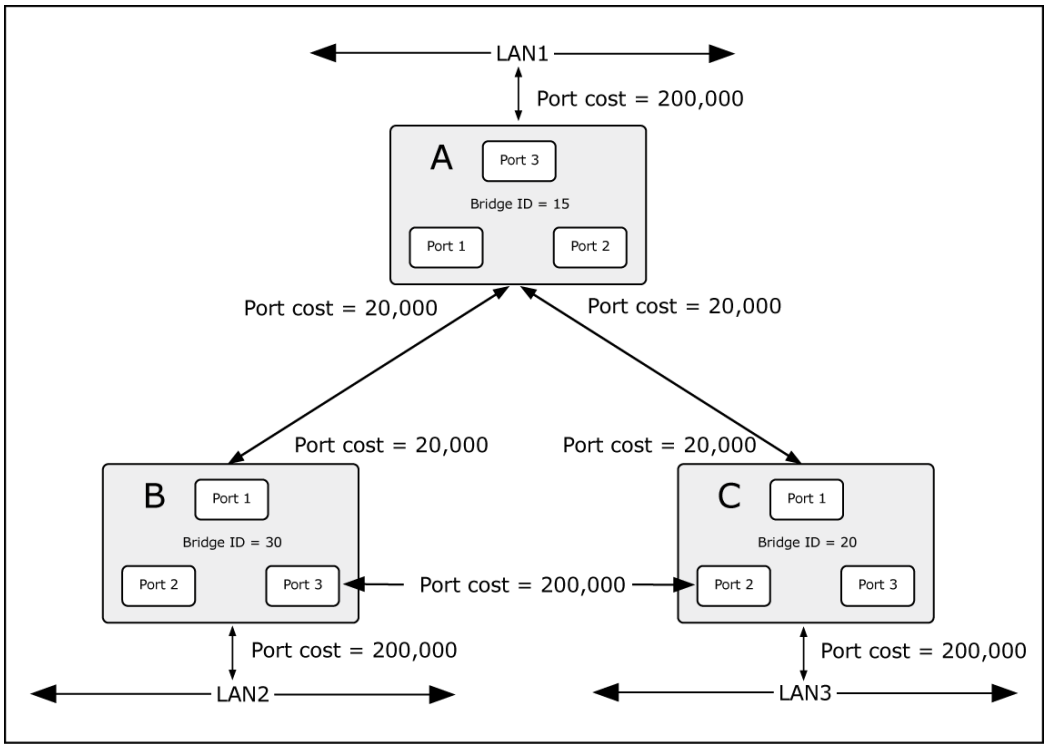
- **Priority** – A priority for the switch can be set from 0 to 65535. 0 is equal to the highest priority.
- **Hello Time** – The hello time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the root bridge to tell all other switches that it is indeed the root bridge. If you set a hello time for the switch and it is not the root bridge, the set hello time will be used if and when the switch becomes the root bridge.

  Note: The hello time cannot be longer than the max. age or a configuration error will occur.
- **Max. Age** – The max. age can be from 6 to 40 seconds. At the end of the max age, if a BPDU has still not been received from the root bridge, the switch starts sending its own BPDU to all other switches for permission to become the root bridge. If the switch has the lowest bridge identifier, it will become the root bridge.
- **Forward Delay Timer** – The forward delay can be from 4 to 30 seconds. This is the time any port on the switch spends in the listening state while moving from the blocking state to the forwarding state.

  Note: Observe the following formulas when setting the above parameters: **Max. Age _ 2 x (Forward Delay - 1 second)**, **Max. Age _ 2 x (Hello Time + 1 second)**.
- **Port Priority** – A port priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the root port.
- **Port Cost** – A port cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

Illustration of STP

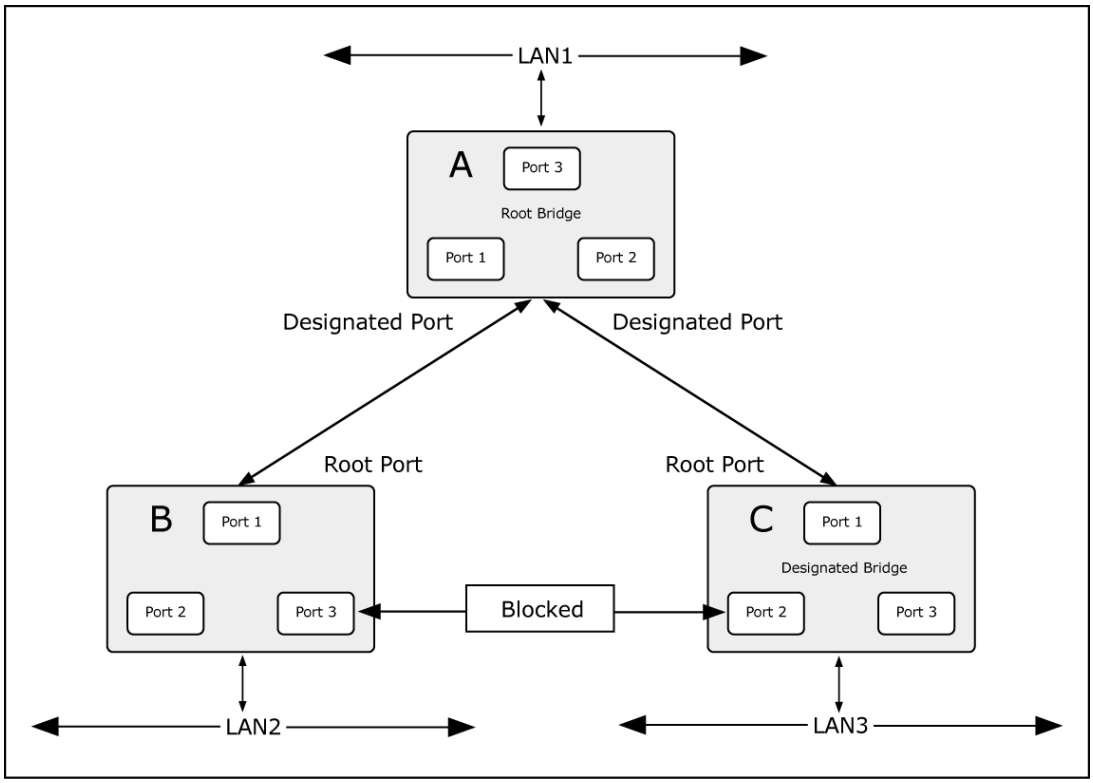
A simple illustration of three switches connected in a loop is depicted in the following diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.



If switch A broadcasts a packet to switch B, switch B broadcasts to switch C, and switch C broadcasts back to switch A and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure. In this example, STP breaks the loop by blocking the connection between switch B and C. The decision to block a particular connection is based on the STP calculation of the most current bridge and port settings.

Now, if switch A broadcasts a packet to switch C, then switch C drops the packet at port 2 and the broadcast ends there. Setting up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the priority setting, or influencing STP to choose a particular port to block using the port priority and port cost settings is, however, relatively straightforward.

In this example, only the default STP values are used:

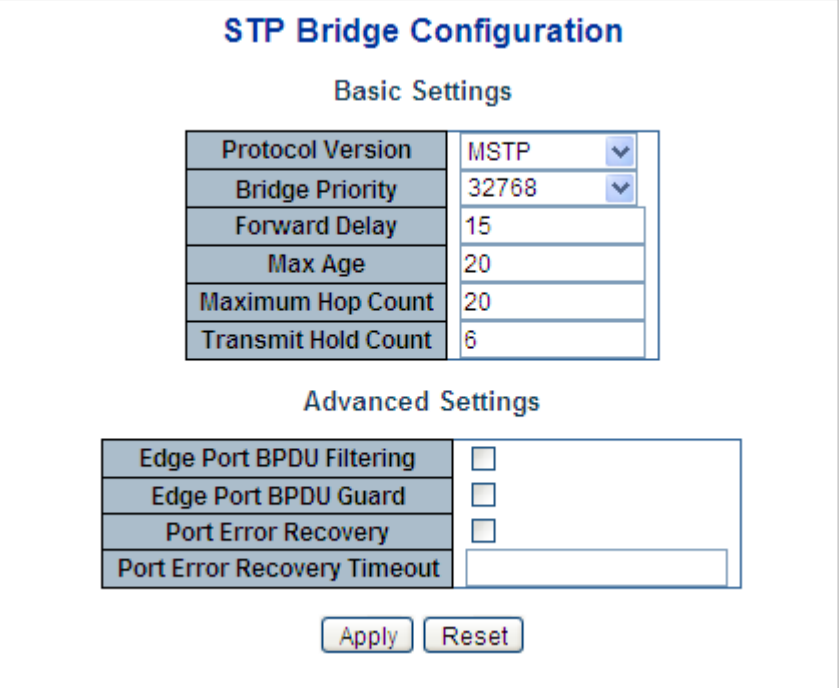


The switch with the lowest bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

STP system configuration

The STP Bridge Configuration page permits configuration of the STP system settings. The settings are used by all STP bridge instances in the switch. The managed switch supports the following spanning tree protocols:

- **Compatible** – Spanning Tree Protocol (STP): Provides a single path between end stations, avoiding and eliminating loops.
- **Normal** – Rapid Spanning Tree Protocol (RSTP) : Detects and uses network topologies that provide faster spanning tree convergence, without creating forwarding loops.
- **Extension** – Multiple Spanning Tree Protocol (MSTP) : Defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" MSTP configures a separate spanning tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree.



The page includes the following fields:

Basic settings

Object	Description
Protocol Version	The STP protocol version setting. Selections are **STP**, **RSTP** and **MSTP**.
Bridge Priority	Controls the bridge priority. Lower numeric values have higher 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 transition root and designated ports to forwarding (used in STP compatible mode). Valid values are in the range of 4 to 30 seconds Default: **15** Minimum: The higher of **4** or [**(Max. Message Age / 2) + 1**] Maximum: **30**
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. Default: **20** Minimum: The higher of **6** or [**2 x (Hello Time + 1)**]. Maximum: The lower of **40** or [**2 x (Forward Delay -1)**]
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. 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 is delayed. Valid values are in the range of **1** to **10** BPDU's per second.

Advanced settings

Object	Description
Edge Port BPDU Filtering	Controls whether a port explicitly configured as Edge will transmit and receive BPDUs.
Edge Port BPDU Guard	Controls whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port enters the error-disabled state, and is removed from the active topology.
Port Error Recovery	Controls 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 that has to pass before a port in the error-disabled state can be enabled. Valid values are between **30** and **86400** seconds (24 hours).

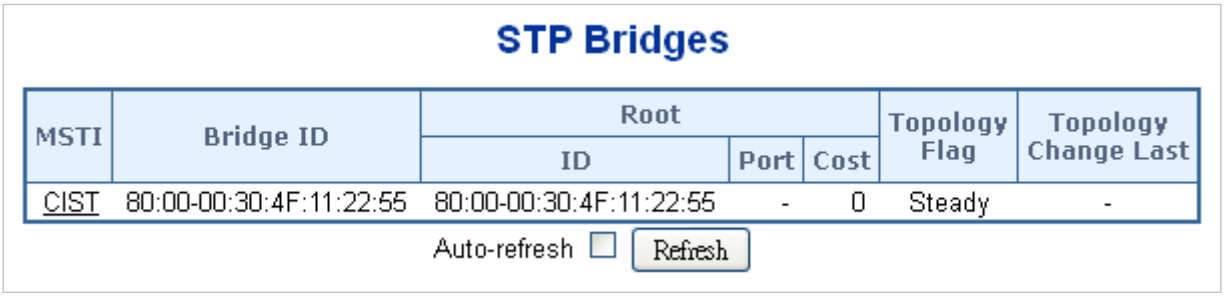
Note: The managed switch implements the rapid spanning protocol as the default spanning tree protocol. When selecting “Compatibles” mode, the system uses the RSTP (802.1w) to be compatible and work with another STP (802.1D)’s BPDU control packet.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Bridge status

The STP Bridges page provides a status overview of all STP bridge instances. The table contains a row for each STP bridge instance, and the columns display the following information:



The page includes the following fields:

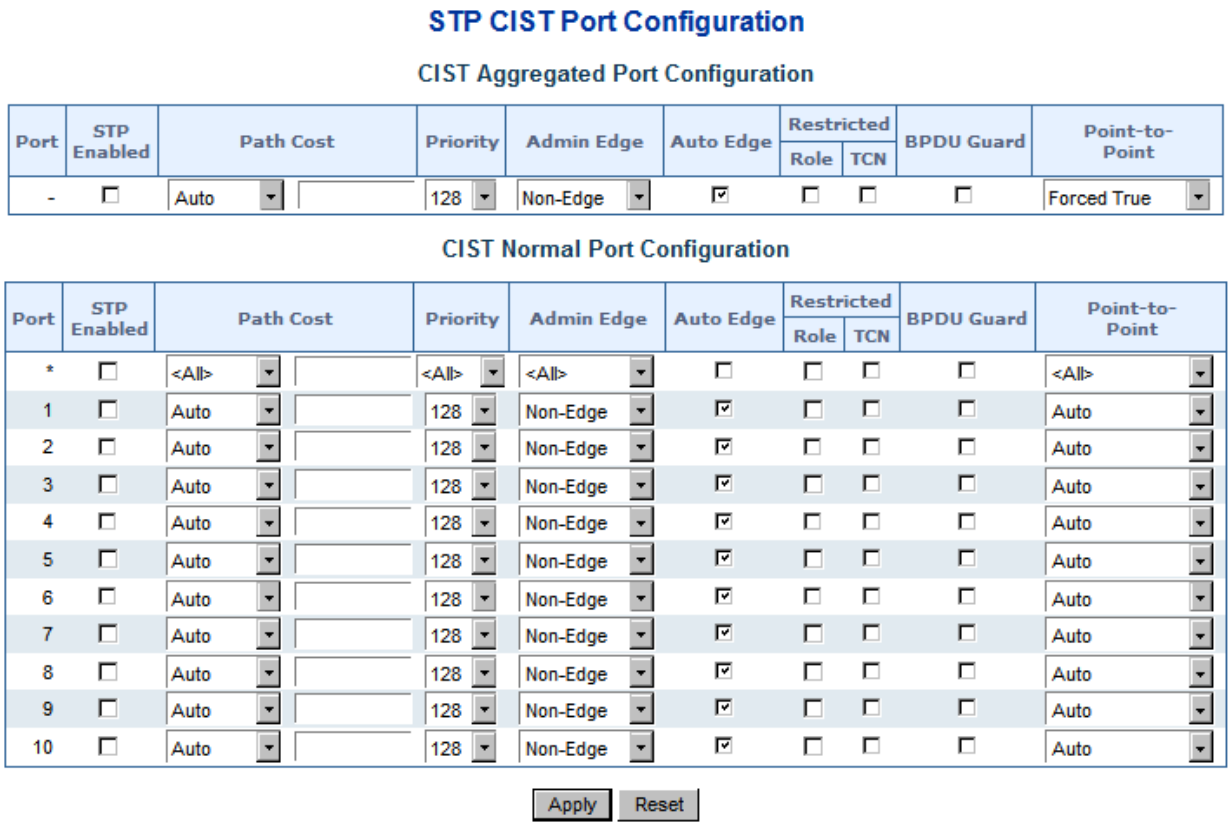
Object	Description
MSTI	The bridge instance. This is also a link to the STP detailed bridge status.
Bridge ID	The bridge ID of this bridge instance.
Root ID	The bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root Path Cost. For the root bridge this is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.
Topology Flag	The current state of the topology change flag for this bridge instance.
Topology Change Last	The time since the last topology change occurred.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

CIST port configuration

This STP CIST Port Configuration page permits the user to inspect and change the current STP CIST port configurations.



The page includes the following fields:

Object	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls if RSTP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The **Auto** setting sets 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 can be chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range of **1** to **200000000**.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Default: **128** Range: 0-240, in steps of 16
AdminEdge	Controls whether the operEdge flag should start as set or cleared (the initial operEdge state when a port is initialized).
AutoEdge	Controls if the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from BPDUs received on the port.
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 a lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network and 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 a shared medium. This can be automatically determined, or forced either true or false. Transitions to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved

values.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the following values. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Recommended STP path cost range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Recommended STP path costs

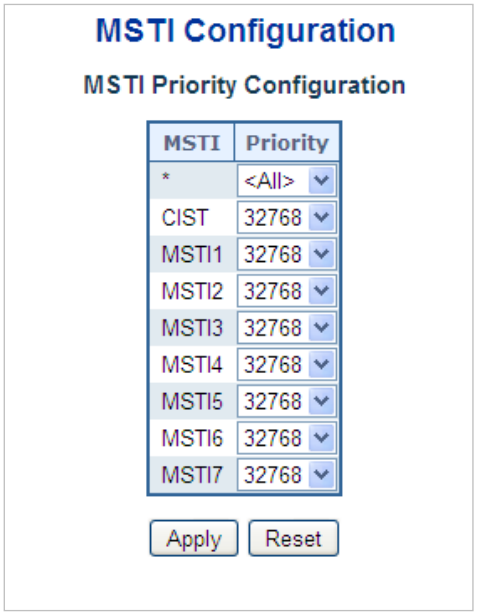
Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Default STP path costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

MSTI priorities

The MSTI Configuration page permits the user to inspect and change the current STP MSTI bridge instance priority configurations.



The page includes the following fields:

Object	Description
MSTI	The bridge instance. The CIST is the default instance, which is always active.
Priority	Controls the bridge priority. Lower numerical values have higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a bridge identifier.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

MSTI configuration

The MSTI Configuration page permits the user to inspect and change the current STP MSTI bridge instance priority configurations.

MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	00-30-4f-11-22-33
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Apply Reset

The page includes the following fields:

Configuration identification

Object	Description
Configuration Name	The name identifiying the VLAN to MSTI mapping. Bridges must share the name and revision, as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is a maximum of 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI mapping

Object	Description
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 VLAN's mapped to the MSTI. The VLANs must be separated with a comma and/or space. A VLAN can only be mapped to one MSTI. A unused MSTI should be left empty (i.e., not have any VLANs mapped to it).

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

MSTI ports configuration

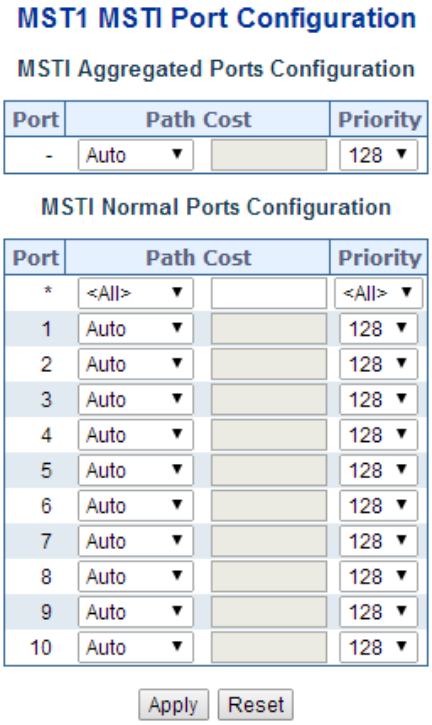
The MSTI Port Configuration page permits the user to inspect and change the current STP MSTI port configurations. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must 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.

The page includes the following fields:

MTSI port configuration

Object	Description
Select MSTI	Select the bridge instance and set more detail configuration.



The page includes the following fields:

MSTx MTSI port configuration

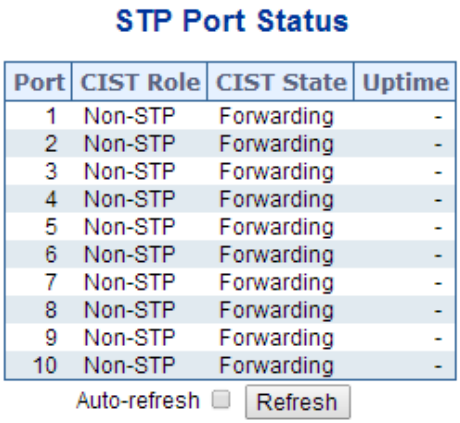
Object	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The **Auto** setting sets the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, 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 favor 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.

Buttons

- Click **Get** to set MSTx configuration.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port status

The STP Port Status page displays the STP CIST port status for physical ports in the currently selected switch.



The page includes the following fields:

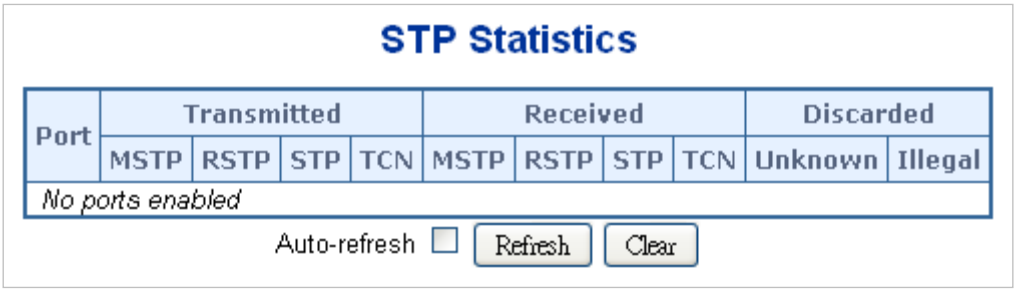
Object	Description
Port	The switch port number of the logical STP port.
CIST Role	The current STP port role of the ICST port. The port role can be one of the following values: **AlternatePort** **BackupPort** **RootPort** **DesignatedPort** **Disable**
CIST State	The current STP port state of the CIST port . The port state can be one of the following values: **Disabled** **Learning** **Forwarding**
Uptime	The time since the bridge port was last initialized.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Port statistics

The STP Statistics page displays the STP port statistics counters for physical ports in the currently selected switch.



The page includes the following fields:

Object	Description
Port	The switch port number of the logical RSTP port.
MSTP	The number of MSTP Configuration BPDU's received/transmitted on the port.
RSTP	The number of RSTP Configuration 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

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear the counters for all ports.

Multicast

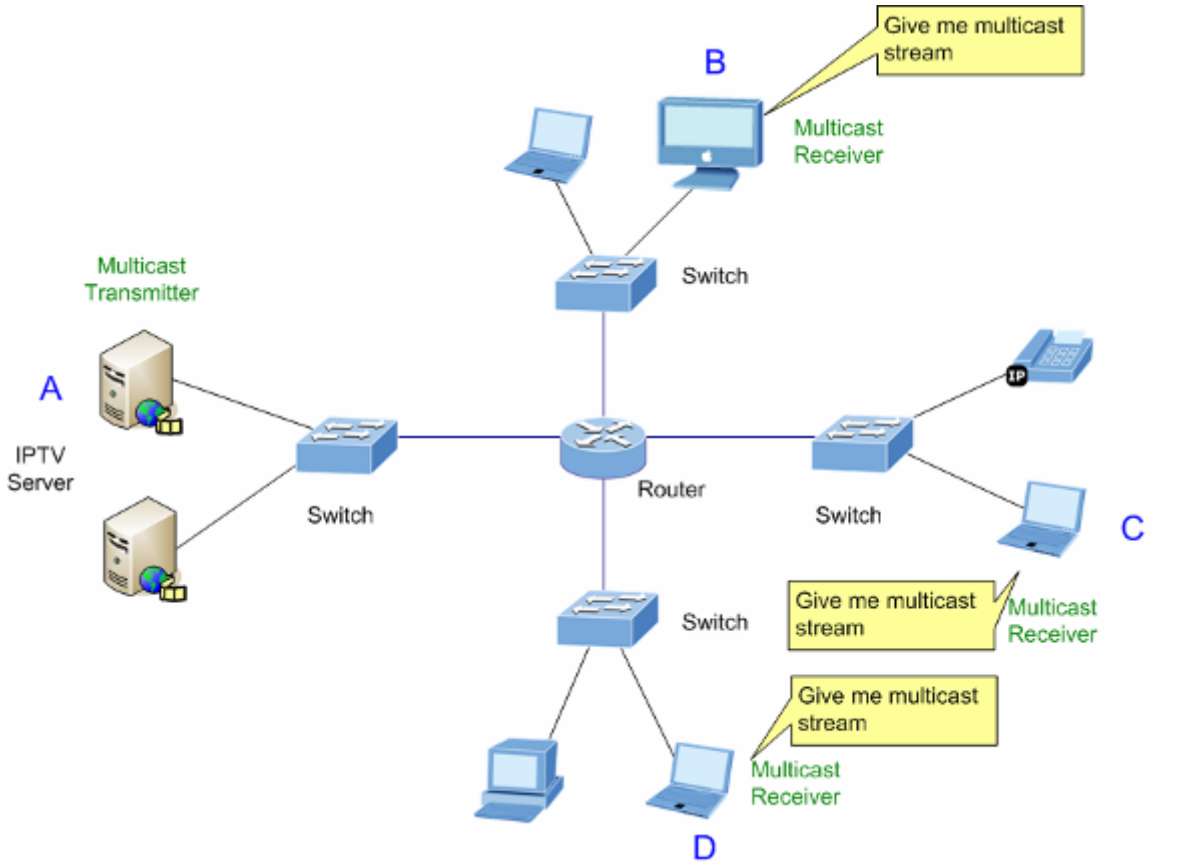
IGMP snooping

The Internet Group Management Protocol (IGMP) allows hosts and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

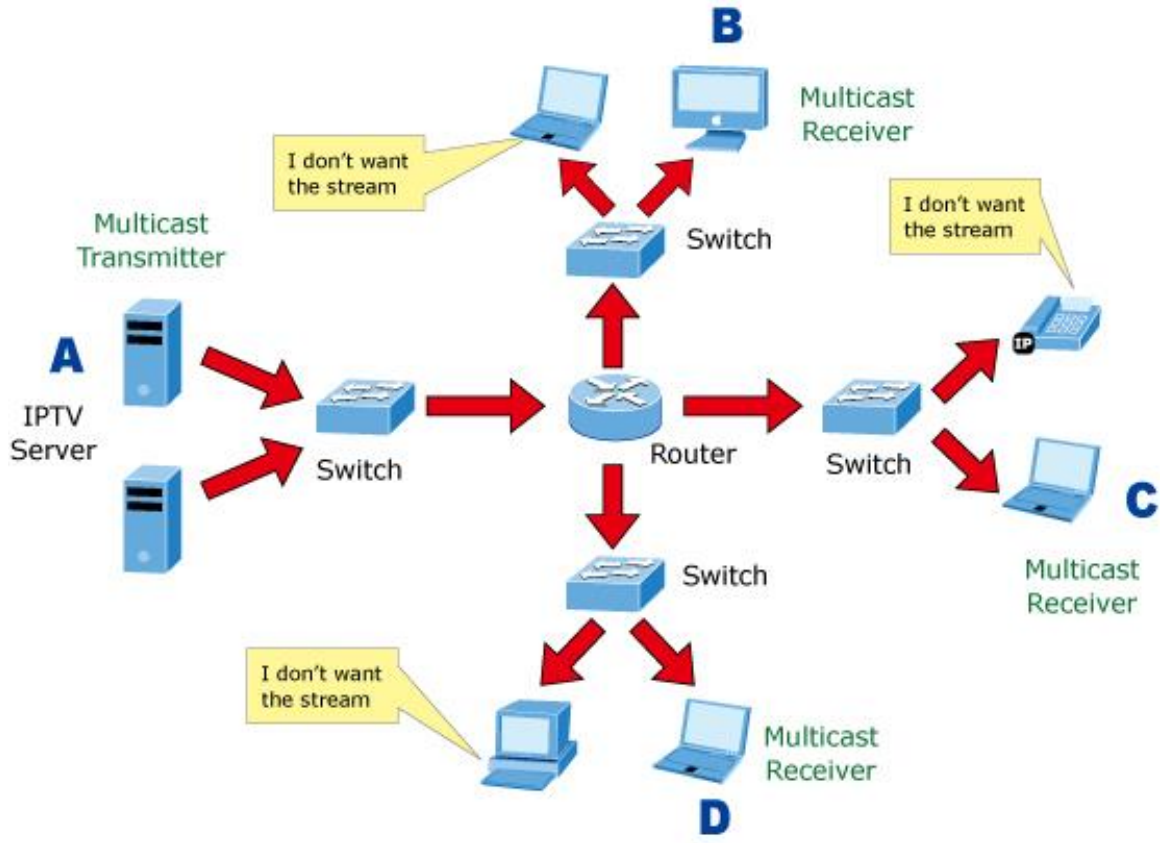
About IGMP snooping

Computers and network devices that need to receive multicast transmissions must inform nearby routers that they will become members of a multicast group. IGMP is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as ‘queried.’ This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine whether or not multicast packets should be forwarded to a given sub network. Using IGMP, the router can check to see if there is at least one member of a multicast group on a given sub network. If there are no members on a sub network, packets will not be forwarded to that sub network.

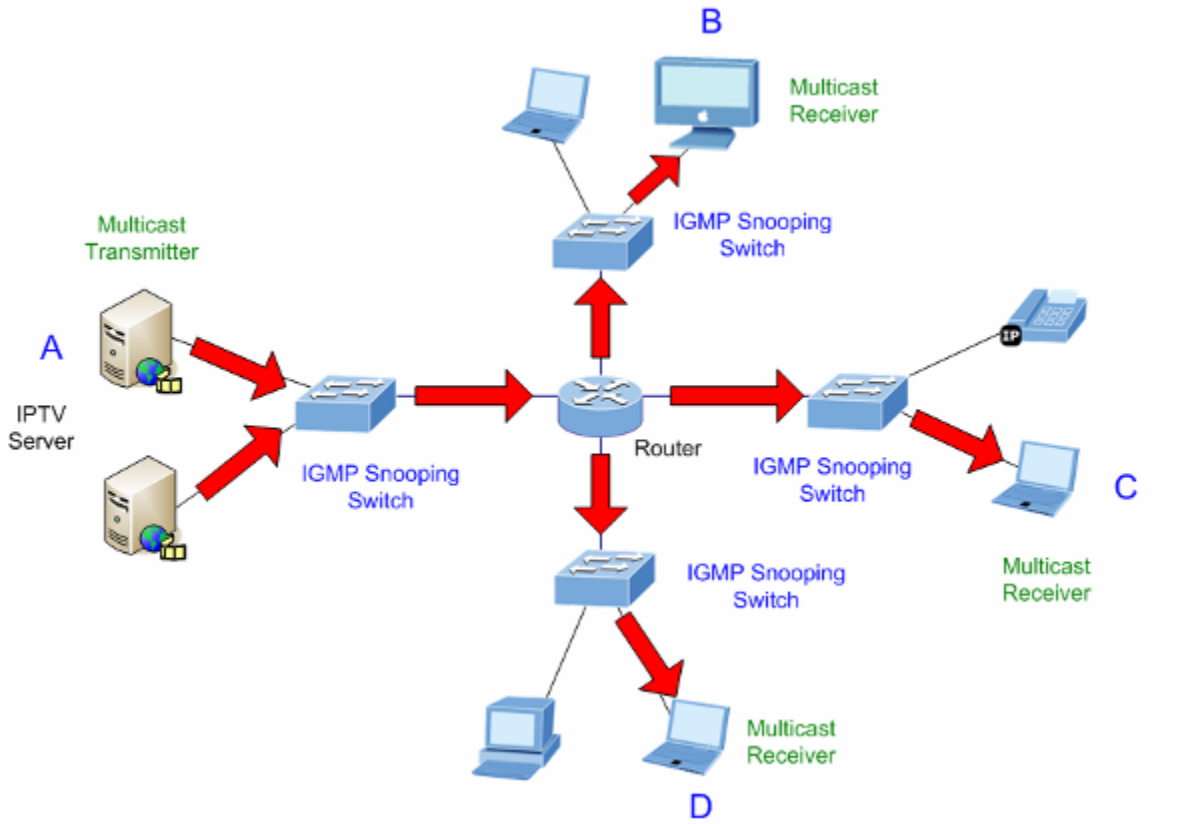
Multicast service



Multicast flooding



IGMP snooping multicast stream control

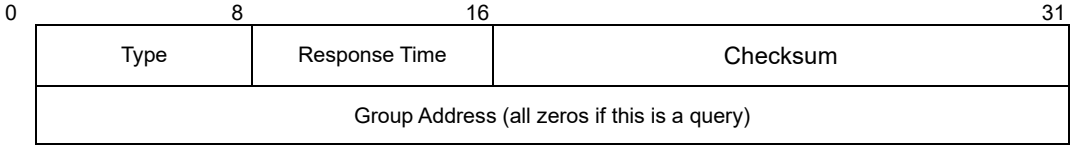


IGMP versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group. IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data. The format of an IGMP packet is shown below:

IGMP message format

Octets:



The IGMP type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	Membership Report (version 2)
0x17	Leave a Group (version 2)
0x12	Membership Report (version 1)

IGMP packets allow multicast routers to keep track of the membership of multicast groups on their respective sub networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.

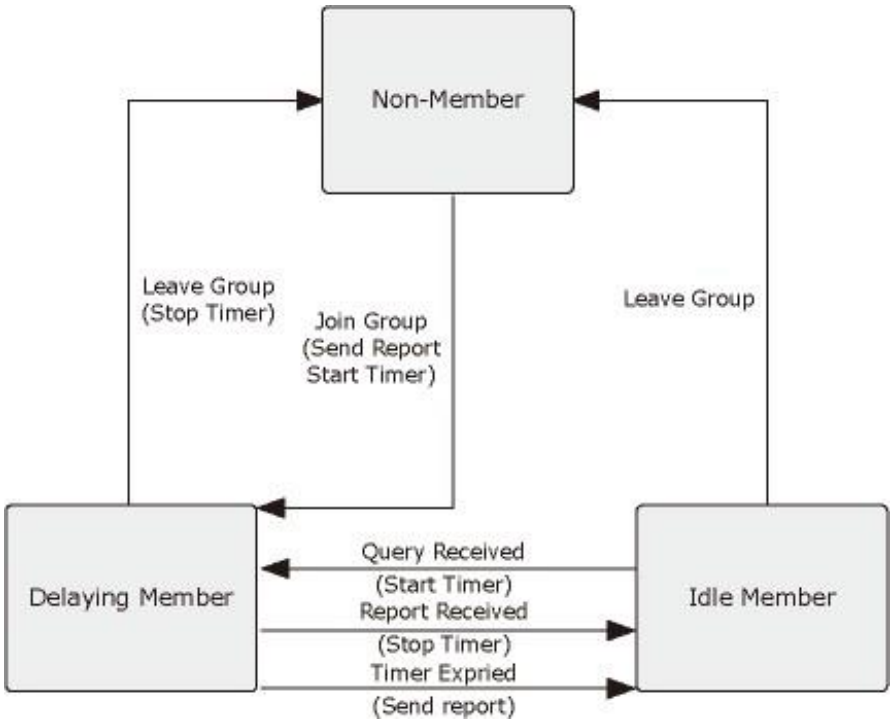
- A host sends an IGMP “report” to join a group
- A host will never send a report when it wants to leave a group (for version 1).
- A host will send a “leave” report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are as follows:



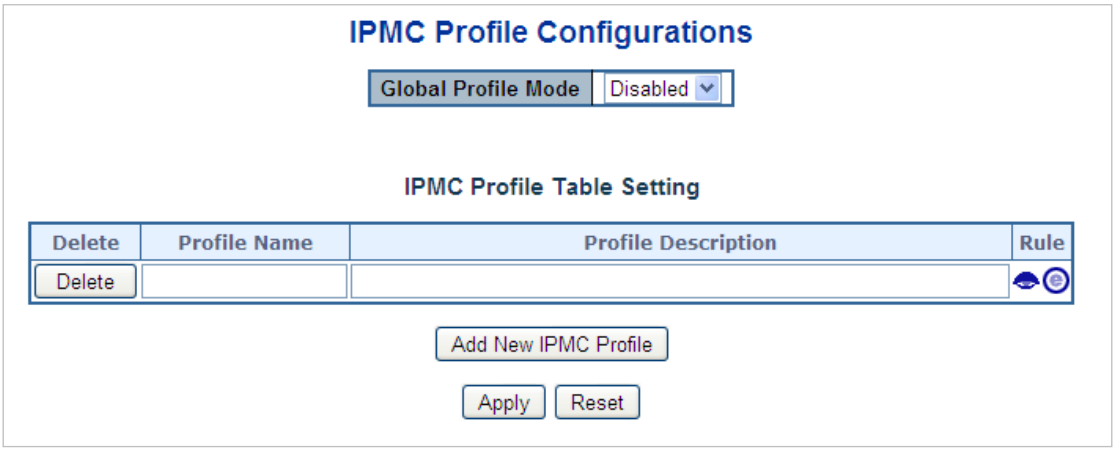
IGMP querier

A router or multicast-enabled switch can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Profile table

The IPMC Profile Configurations 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 64 Profiles with a maximum of 128 corresponding rules for each.



The page includes the following fields:

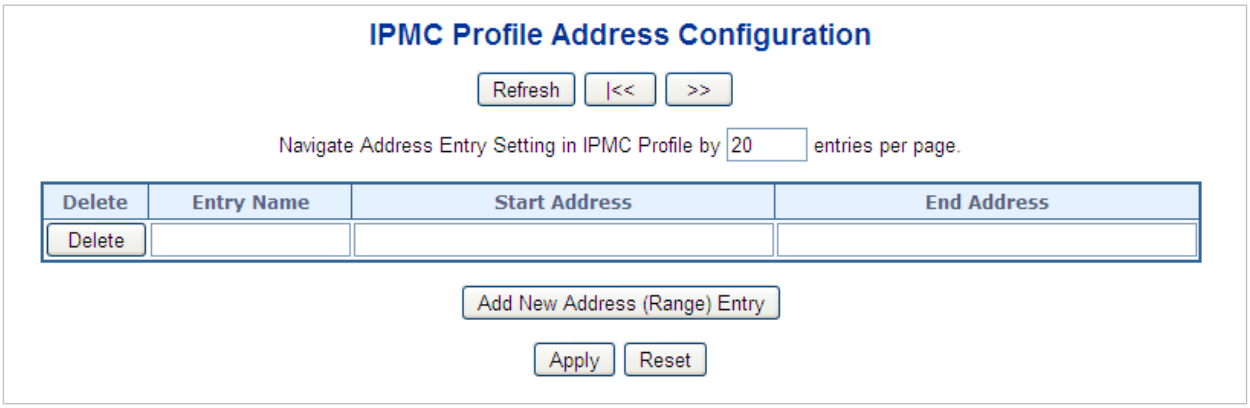
Object	Description
Global Profile Mode	Enable/Disable the Global IPMC Profile. The system starts to do filtering based on profile settings only when the global profile mode is enabled.
Delete	Check to delete the entry. The designated entry is deleted during the next save.
Profile Name	The name used for indexing the profile table. Each entry has a unique name which is composed of a maximum of 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 characters or spaces 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: : List the rules associated with the designated profile. : Adjust the rules associated with the designated profile.

Buttons

- Click **Add New IPMC Profile** to add a new IPMC profile. Specify the name and configure the new entry, and then click **Save**.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Address entry

The IPMC Profile Address Configuration page provides address range settings used in the IPMC profile. The address entry is used to specify the address range associated with the IPMC profile. It can create a maximum of 128 address entries in the system.



The page includes the following fields:

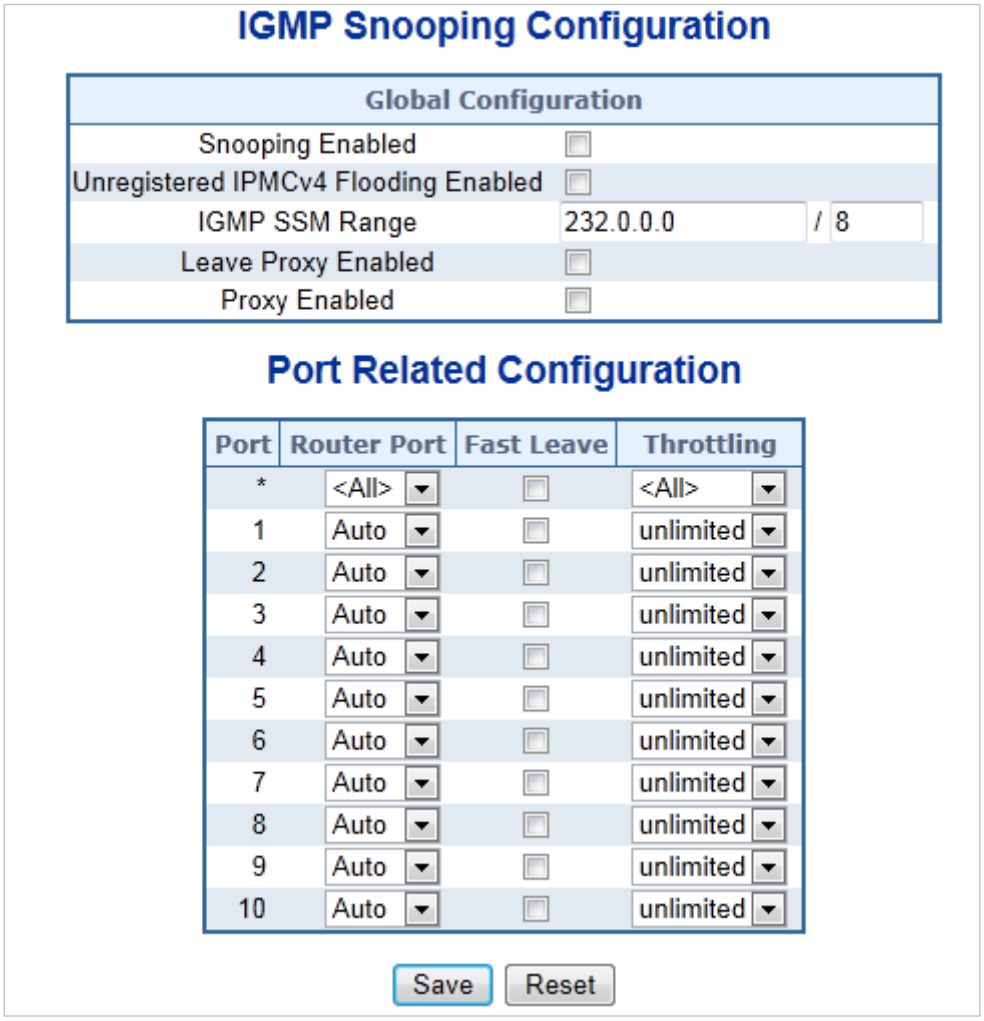
Object	Description
Delete	Click **Delete** to delete the entry. The designated entry is deleted during the next save.
Entry Name	The name used for indexing the address entry table. Each entry has a unique name with a maximum of 16 alphabetic and numeric characters. At least one alphabet must be present.
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

- Click **Add New Address (Range) Entry** to add a new address range. Specify the name and configure the addresses, and then click **Save**.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **I<<** to update the table starting from the first entry in the IPMC profile address configuration.
- Click **>>** to update the table starting with the entry after the last entry currently displayed.

IGMP snooping configuration

The IGMP Snooping Configuration page provides IGMP snooping-related configuration information.



The page includes the following fields:

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

Object	Description
Router Port	Specify which ports act as IGMP router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. The switch forwards IGMP join or leave packets to an IGMP router port. Selections are as follows: **Auto –** The managed switch automatically uses the port as IGMP router port if the port receives IGMP query packets. **Fix –** The managed switch always uses the specified port as an IGMP router port. Use this mode when connecting an IGMP multicast server or IP camera with multicast protocol to the port. **None –** The managed switch will not use the specified port as an IGMP router port and will not keep any record of an IGMP router being connected to this port. Use this mode when connecting other IGMP multicast servers directly to the non-querier managed switch, and you don't want the multicast stream to be flooded to the uplink switch through the port that connected to the IGMP querier.
Fast Leave	Enable the fast leave on the port.
Throtting	Enable to limit the number of multicast groups to which a switch port can belong. **All** means all ports wil have one specific setting.

Buttons

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

IGMP snooping VLAN configuration

The IGMP Snooping VLAN Configuration page shows up to 99 entries from the VLAN table (default is 20 entries per page). The range of entries per page can be typed into the **Start from VLAN** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the VLAN table. The first entry shown will be the one with the lowest VLAN ID found in the VLAN table.

The page includes the following fields:

Object	Description
Delete	Select this check box to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enable	Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected.
Querier Election	Enable the 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, the system uses the first available IPv4 management address. Otherwise, the 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. Selections include: **IGMP-Auto** (default selection), **Forced IGMPv1**, **Forced IGMPv2**, **Forced IGMPv3**.
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). The default interface priority value is **0**
RV	Robustness Variable. The RV permits tuning for the expected packet loss on a network. The allowed range is **1** to **255**. The default robustness variable value is **2**.
QI	Query Interval. The QI is the interval between general queries sent by the querier. The allowed range is **1** to **31744** seconds. The default query interval is 125 seconds.
QRI	Query Response Interval. This is the maximum response time used to calculate the maximum resp code inserted into the periodic general queries. The allowed range is **0** to **31744** in tenths of seconds. The 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

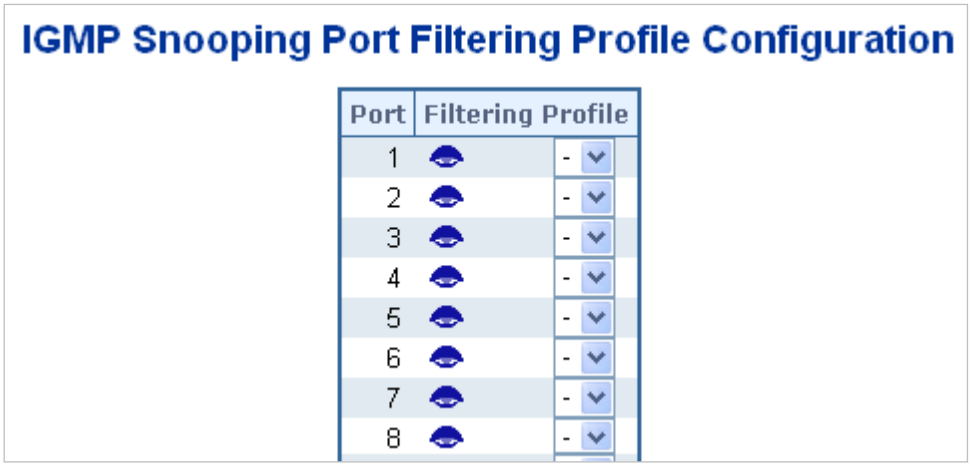
- Click **Refresh** to refresh the table starting from the **Start from VLAN** and **entries per page** input fields.
- Click **I<<** to update the table starting from the first entry in the VLAN table (i.e., the entry with the lowest VLAN ID).
- Click **>>** to updates the table, starting with the entry after the last entry currently displayed.
- Click **Add New IGMP VLAN** to add a new IGMP VLAN. Specify the VID and configure the new entry, and then click **Save**. The specific IGMP VLAN starts working after the corresponding static VLAN is also created
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

IGMP snooping port group filtering

In certain switch applications, the administrator may want to control the multicast services that are available to end users (an IP/TV service based on a specific subscription plan, for example). The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

The IGMP Snooping Port Group Filtering Configuration page permits assigning a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of, multicast addresses. However, only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.



The page includes the following fields:

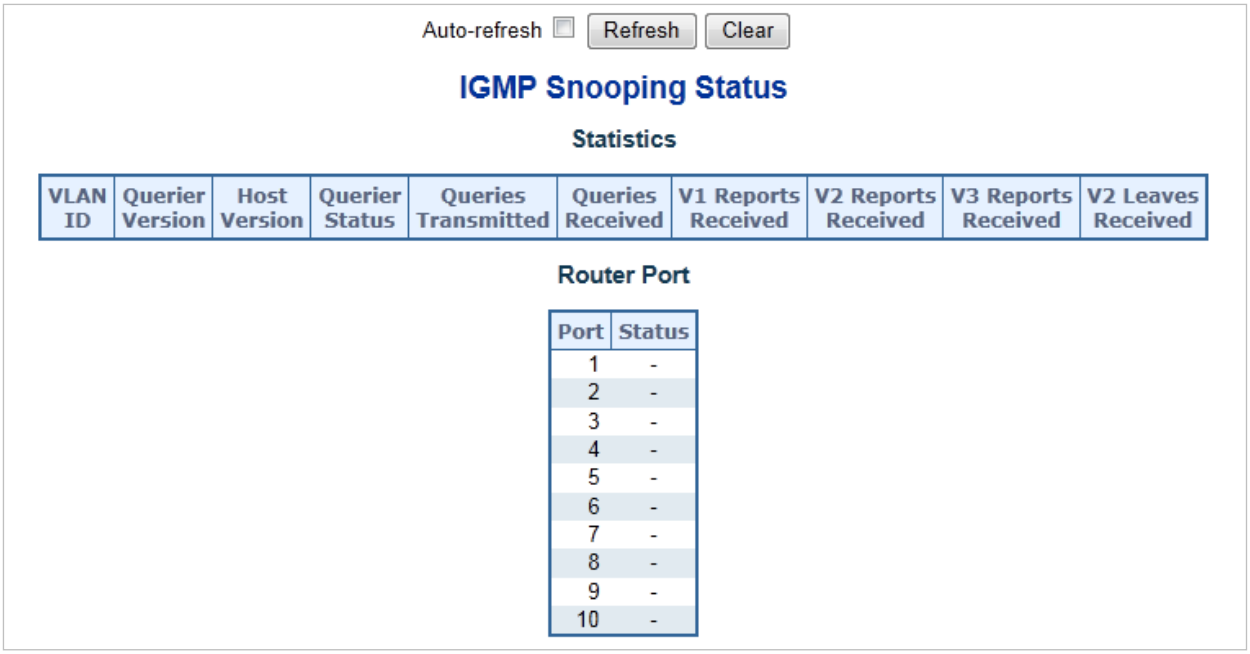
Object	Description
Port	The logical port for the settings.
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

IGMP snooping status

The IGMP Snooping Status page provides IGMP snooping status.



The page includes the following fields:

Object	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	The current working querier version.
Host Version	The current working host version.
Querier Status	Shows whether the querier status is "ACTIVE" or "IDLE".
Querier Transmitted	The number of transmitted queries.
Querier 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	Displays the ports that are acting as router ports.
Port	Switch port number.
Status	Indicates whether or not the specific port is a router port.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear all statistics counters.
- Select **Auto-refresh** to automatically refresh the page every three seconds.

IGMP group information

Entries in the IGMP group table are shown in the IGMP Snooping Group Information page. The IGMP group table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the IGMP group table (default is 20 entries per page). The range of entries per page can be typed into the **Start from VLAN** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the IGMP Group table. The **Start from VLAN** and **group Address** fields permit the user to select the starting point in the IGMP group table.

The page includes the following fields:

Object	Description
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

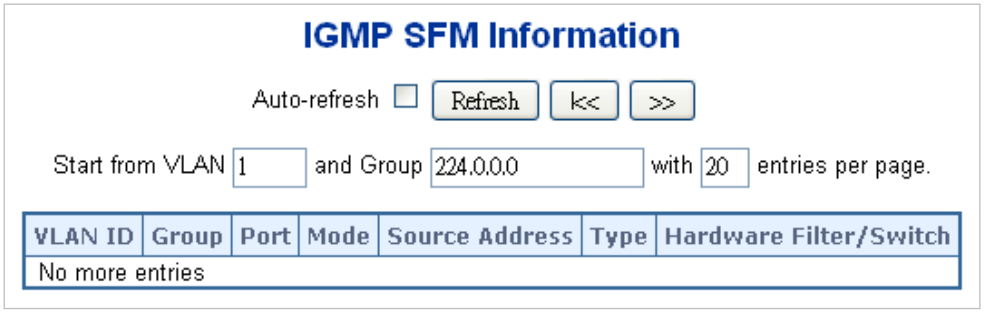
Buttons

- Select **Auto-refresh** to automatically refresh the page every three seconds.
- Click **Refresh** to refresh the table starting from the input fields.
- Click **I<<** to update the table starting from the first entry in the IGMP group table.
- Click **>>** to update the table, starting with the entry after the last entry currently shown.

IGMPv3 information

Entries in the IGMP SFM (Source-Filtered Multicast) information table are shown on the IGMP SFM Information page. The table also contains SSM (Source-Specific Multicast) information. The table is sorted first by VLAN ID, then by group, and then by port number. Different source addresses that belong to the same group are treated as a single entry.

Each page shows up to 99 entries from the IGMP SFM Information table The range of entries per page can be typed into the **Start from VLAN** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the IGMP Group table. The **Start from VLAN** and **group Address** fields permit the user to select the starting point in the IGMP information table.



The page includes the following fields:

Object	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group shown.
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.

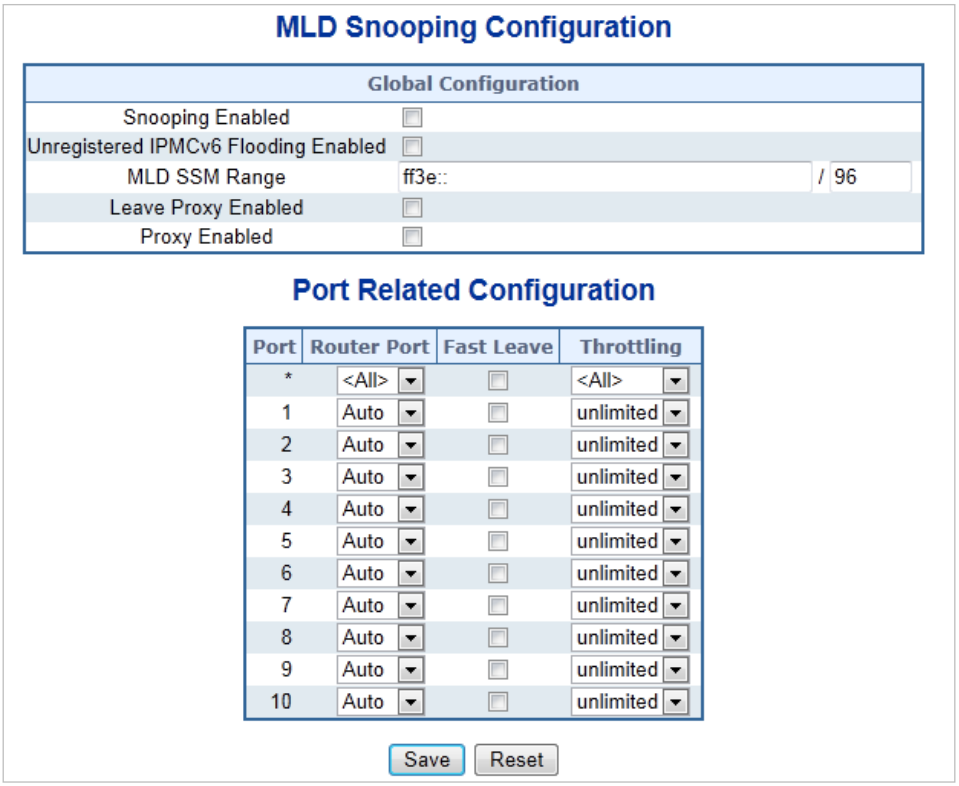
Object	Description
Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to 128.
Type	Indicates the type. It can be either **Allow** or **Deny**.
Hardware Filter/Switch	Indicates if the data plane destined to the specific group address from the source IPv4 address can be accomodated by the chip.

Buttons

- Select **Auto-refresh** to automatically refresh the page every three seconds.
- Click **Refresh** to refresh the table starting from the input fields.
- Click **I<<** to update the table starting from the first entry in the IGMP group table.
- Click **>>** to update the table, starting with the entry after the last entry currently shown.

MLD snooping configuration

The MLD Snooping Configuration page provides MLD snooping-related configuration.



The page includes the following fields:

Object	Description
Snooping Enabled	Enable 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 to run the SSM service model for the groups in the address range.
Leave Proxy Enable	Enable MLD leave proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enable	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 acts as a router port. Selections are **Auto**, **Fix**, **Fone**, and the default compatibility value is **Auto**. **All** means all ports will have one specific setting.
Fast Leave	Enable fast leave on the port.
Throtting	Enable Throttling to limit the number of multicast groups to which a switch port can belong. **All** means all ports will have one specific setting.

Buttons

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

MLD snooping VLAN configuration

Each page shows up to 99 entries from the VLAN table (default is 20 entries per page). The range of entries per page can be typed into the Start from VLAN and entries per page fields. When initially accessing the page, it shows the first 20 entries from the beginning of the VLAN table. The first entry shown will be the one with the lowest VLAN ID found in the VLAN table.

The page includes the following fields:

Object	Description
Delete	Select this check box to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enable	Enable the per-VLAN MLD snooping. Only up to 32 VLANs can be selected.
Querier Election	Enable the MLD querier election in the VLAN. Disable to act as an IGMP non-querier.
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. Selections include: **MLD-Auto** (default selection), **Forced MLDv1**, and **Forced MLDv2**.
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). The default interface priority value is **0**
RV	Robustness Variable. The RV permits tuning for the expected packet loss on a network. The allowed range is **1** to **255**. The default robustness variable value is **2**.
QI	Query Interval. The QI is the interval between general queries sent by the querier. The allowed range is **1** to **31744** seconds. The default query interval is 125 seconds.
QRI	Query Response Interval. This is the maximum response time used to calculate the maximum resp code inserted into the periodic general queries. The allowed range is **0** to **31744** in tenths of seconds. The 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 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

- Click **Refresh** to refresh the table starting from the **Start from VLAN** and **entries per page** input fields.
- Click **I<<** to update the table starting from the first entry in the VLAN table (i.e., the entry with the lowest VLAN ID).

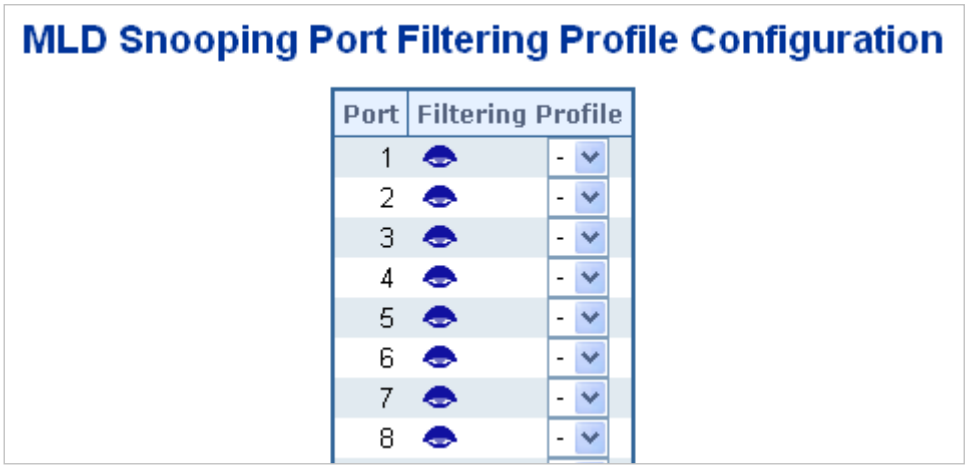
- Click **>>** to updates the table, starting with the entry after the last entry currently displayed.
- Click **Add New MLD VLAN** to add a new MLD VLAN. Specify the VID and configure the new entry, and then click **Save**. The specific MLD VLAN starts working after the corresponding static VLAN is also created.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

MLD snooping port group filtering

In certain switch applications, the administrator may want to control the multicast services available to end users (such as an IP/TV service based on a specific subscription plan, for example). The MLD filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and MLD throttling limits the number of simultaneous multicast groups a port can join.

The MLD Snooping Port Filtering Profile Configuration page permits assigning a profile to a switch port that specifies multicast groups that are permitted or denied on the port. A MLD filter profile can contain one or more, or a range of, multicast addresses. However, only one profile can be assigned to a port. When enabled, MLD join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the MLD join report is forwarded as normal. If a requested multicast group is denied, the MLD join report is dropped.

MLD throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.



The page includes the following fields:

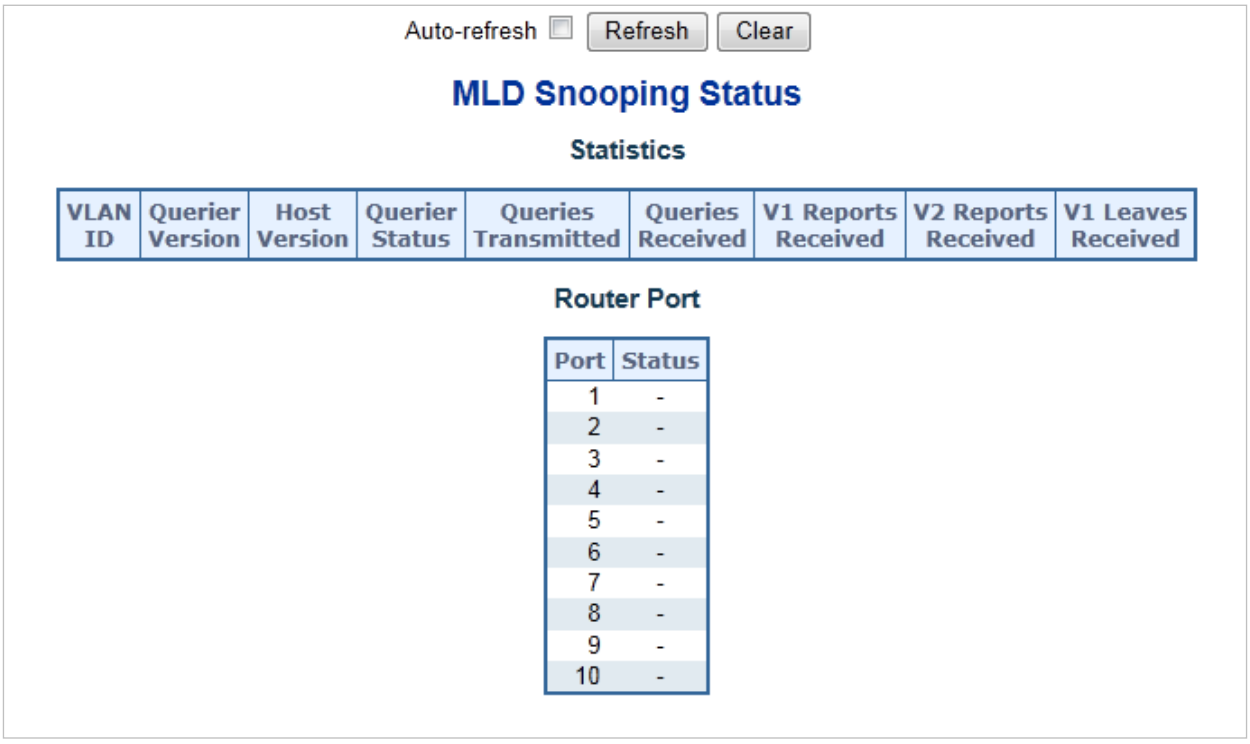
Object	Description
Port	The logical port for the settings.
Filtering Group	Select the IPMC Profile as the filtering condition for the specific port. Click the **View** button to view a summary of the designated profile.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

MLD snooping status

The MLD Snooping Status page provides MLD snooping status.



The page includes the following fields:

Object	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	The current working querier version.
Host Version	The current working host version.
Querier Status	Shows whether the querier status is "ACTIVE" or "IDLE".
Querier Transmitted	The number of transmitted queries.
Querier 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	Displays the ports that are acting 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 learned to be a router port. Both denote the specific port is configured or learned to be a router port.
Port	Switch port number.
Status	Indicates whether or not the specific port is a router port.

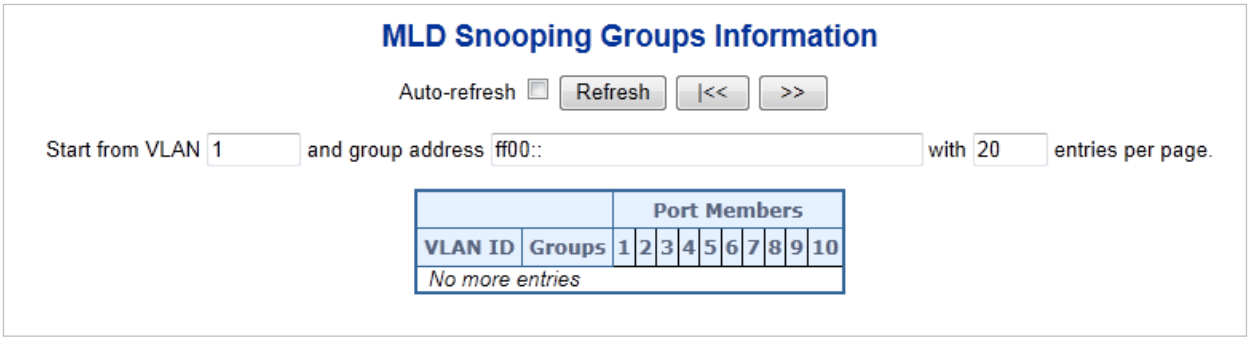
Buttons

- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear all statistics counters.
- Select **Auto-refresh** to automatically refresh the page every three seconds.

MLD group information

Entries in the MLD group table are shown in the MLD Snooping Group Information page. The MLD group table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the MLD group table (default is 20 entries per page). The range of entries per page can be typed into the **Start from VLAN** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the MLD Group table. The **Start from VLAN** and **group Address** fields permit the user to select the starting point in the MLD group table.



The page includes the following fields:

Object	Description
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

Buttons

- Select **Auto-refresh** to automatically refresh the page every three seconds.
- Click **Refresh** to refresh the table starting from the input fields.
- Click **I<<** to update the table starting from the first entry in the MLD group table.
- Click **>>** to update the table, starting with the entry after the last entry currently shown.

MLDv2 information

Entries in the MLD SFM (Source-Filtered Multicast) information table are shown on the IGMP SFM Information page. The table also contains SSM (Source-Specific Multicast) information. The table is sorted first by VLAN ID, then by group, and then by port number. Different source addresses that belong to the same group are treated as single entry.

Each page shows up to 99 entries from the MLD SFM Information table The range of entries per page can be typed into the **Start from VLAN** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the IGMP Group table. The **Start from VLAN** and **Group** fields permit the user to select the starting point in the MLD information table.

The page includes the following fields:

Object	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group shown.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per basis (VLAN ID, port number, Group Address). It can be either **Include** or **Exclude**.
Source Address	IP Address of the source. Currently, the system limits the total number of IP source addresses for filtering to 128.
Type	Indicates the type. It can be either **Allow** or **Deny**.
Hardware Filter/Switch	Indicates if the data plane destined to the specific group address from the source IPv4 address can be accomodated by the chip.

Buttons

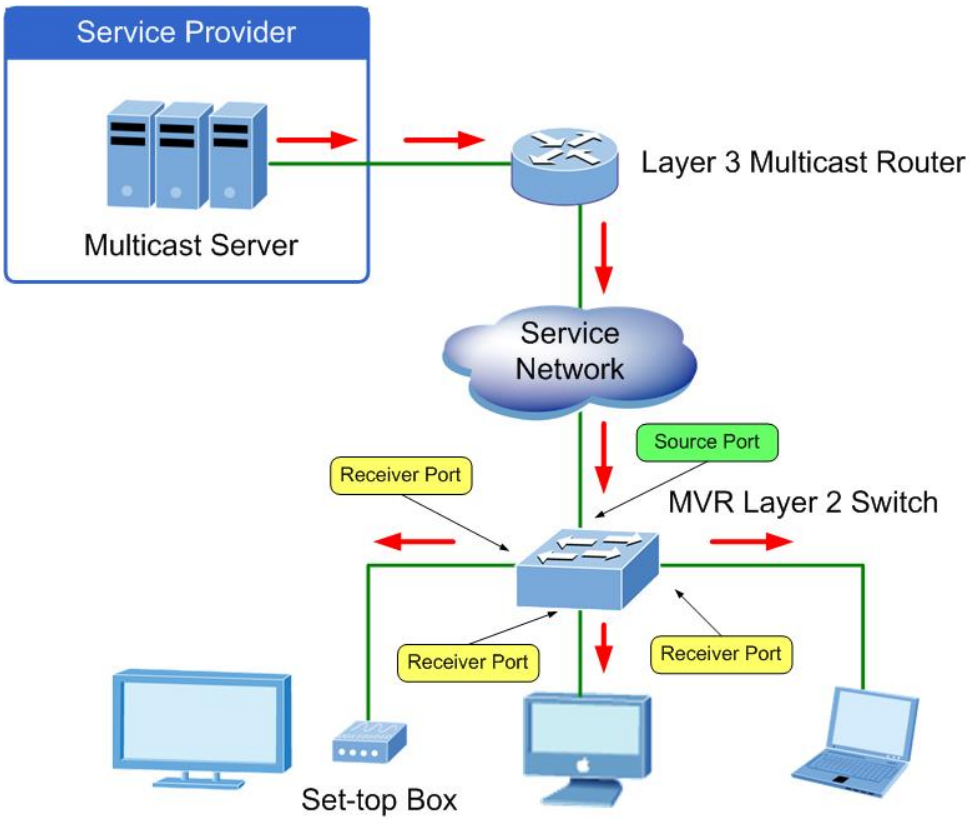
- Select **Auto-refresh** to automatically refresh the page every three seconds.
- Click **Refresh** to refresh the table starting from the input fields.
- Click **I<<** to update the table starting from the first entry in the MLD SFM information table.
- Click **>>** to update the table, starting with the entry after the last entry currently shown.

MVR (Multicast VLAN Registration)

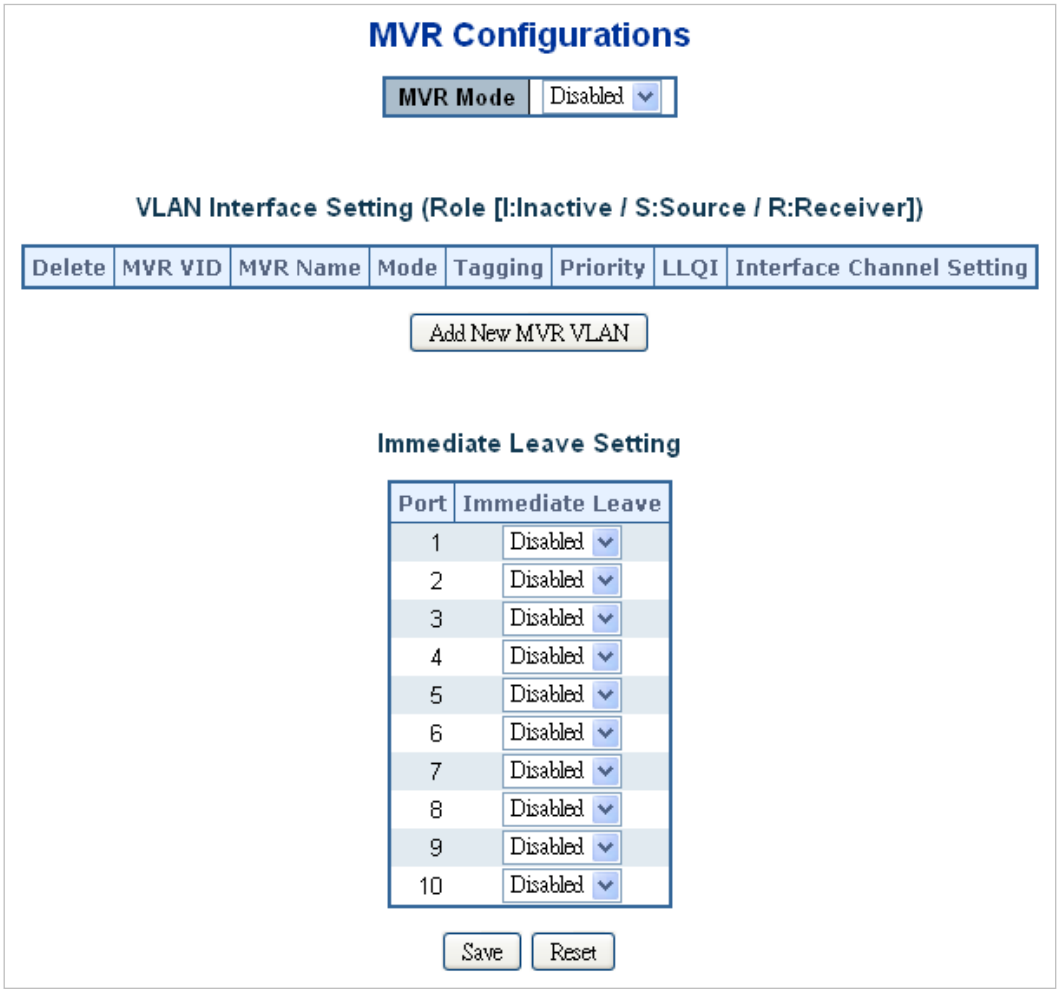
The MVR feature enables multicast traffic forwarding on the Multicast VLANs.

- In a multicast television application, a computer or a network television or a set-top box can receive a multicast stream.
- Multiple set-top boxes or computers 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 computer 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.

A maximum of eight MVR VLANs with corresponding channel settings can be created for each multicast VLAN. A maximum of 256 group addresses are available for channel settings.



The MVR Configurations page provides MVR-related configuration information.



The page includes the following fields:

Object	Description
MVR Mode	Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD snooping. We suggest enabling Unregistered Flooding control when the MVR group table is full.
Delete	Select **Delete** to delete the entry. The designated entry will be deleted during the next save.
MVR VID	Specify the Multicast VLAN ID. **Caution:** We do not recommend overlapping MVR source ports with management VLAN ports.
MVR Name	MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. The maximum length of the MVR VLAN Name string is 16 alphanumeric characters (it must contain at least one alpha character). The. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.
IGMP Address	Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, the system uses the IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the system uses the first available IPv4 management address. Otherwise, the system uses a pre-defined value. By default, this value is 192.0.2.1.
Mode	Specify the MVR mode of operation. In **Dynamic** mode (default setting), MVR allows dynamic MVR membership reports on source ports. In **Compatible** mode, MVR membership reports are forbidden on source ports.
Tagging	Specify whether the traversed IGMP/MLD control frames will be sent as **Untagged** or **Tagged** (default setting) with the MVR VID.
Priority	Specify how the traversed IGMP/MLD control frames will be sent in a prioritized manner. The default Priority is **0**.
LLQI	Define the maximun 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 five-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.
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**: The designated port does not participate in MVR operations. **Source**: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. **Receiver**: 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.

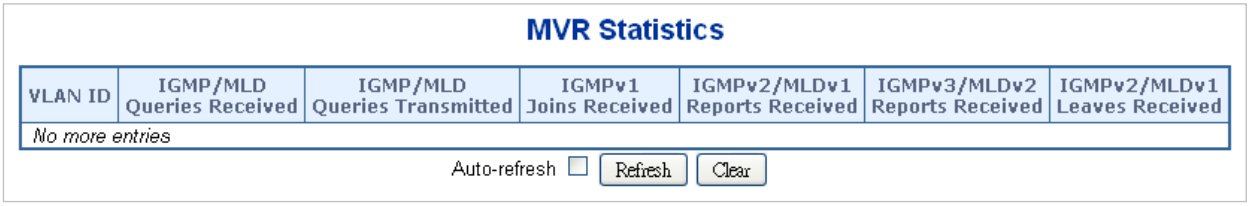
Object	Description
	Caution: We do not recommend overlapping MVR source ports with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver. The default Role is Inactive.
Immediate Leave	Enable the fast leave on the port.

Buttons

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

MVR status

The MVR Statistics page provides MVR status.



The page includes the following fields:

Object	Description
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 joins.
IGMPv2/MLDv1 Reports Received	The number of received IGMPv2 joins and MLDv1 reports, respectively.
IGMPv3/MLDv2 Reports Received	The number of received IGMPv1 joins and MLDv2 reports, respectively.
IGMPv2/MLDv1 Leaves Received	The number of received IGMPv2 leaves and MLDv1 dones, respectively.

Buttons

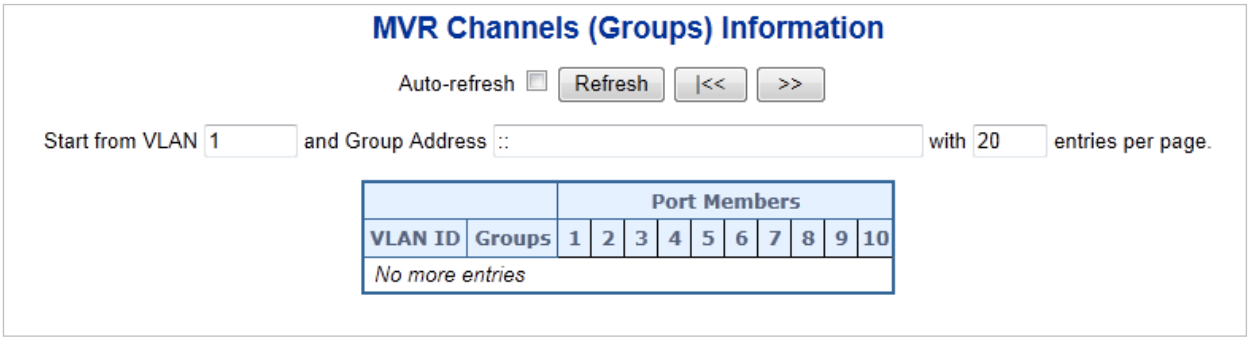
- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear all statistics counters.

- Select **Auto-refresh** to automatically refresh the page every three seconds.

MVR groups information

Entries in the MVR group table are shown in the MVR Channels (Groups) Information page. The MVR group table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the MLD group table (default is 20 entries per page). The range of entries per page can be typed into the **Start from VLAN** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the MVR Group table. The **Start from VLAN** and **Group Address** fields permit the user to select the starting point in the MVR group table.



The page includes the following fields:

Object	Description
VLAN ID	VLAN ID of the group.
Groups	Group ID of the group shown.
Port Members	Ports under this group.

Buttons

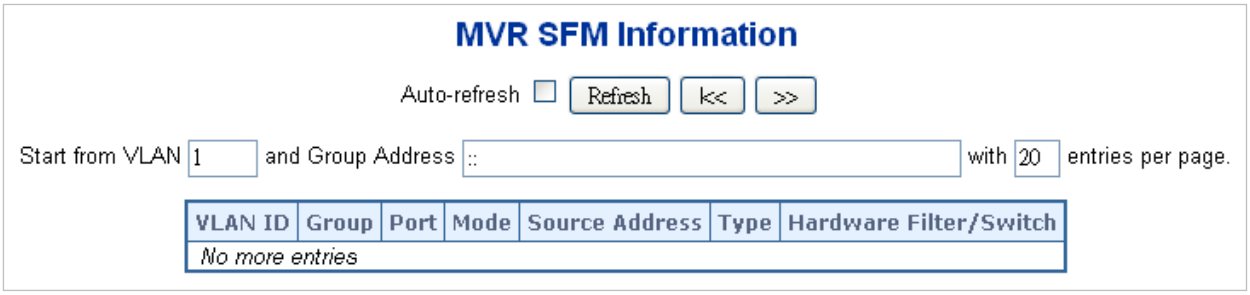
- Select **Auto-refresh** to automatically refresh the page every three seconds.
- Click **Refresh** to refresh the table starting from the input fields.
- Click **I<<** to update the table starting from the first entry in the MVR group table.
- Click **>>** to update the table, starting with the entry after the last entry currently shown.

MVR SFM information

Entries in the MVR SFM (Source-Filtered Multicast) information table are shown on the MLD SFM Information page. The table also contains SSM (Source-Specific Multicast) information. The table is sorted first by VLAN ID, then by group, and then by port number. Different source addresses that belong to the same group are treated as single entry.

Each page shows up to 99 entries from the MVR SFM information table The range of entries per page can be typed into the **Start from VLAN** and **entries per page** fields.

When initially accessing the page, it shows the first 20 entries from the beginning of the MVR SFM information table. The **Start from VLAN** and **Group Address** fields permit the user to select the starting point in the MVR SFM information table.



The page includes the following fields:

Object	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group shown.
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, the system limits the total number of IP source addresses for filtering to 128.
Type	Indicates the type. It can be either **Allow** or **Deny**.
Hardware Filter/Switch	Indicates if the data plane destined to the specific group address from the source IPv4/IPv6 address can be accomodated by the chip.

Buttons

- Select **Auto-refresh** to automatically refresh the page every three seconds.
- Click **Refresh** to refresh the table starting from the input fields.
- Click **I<<** to update the table starting from the first entry in the MVR SFM information table.
- Click **>>** to update the table, starting with the entry after the last entry currently shown.

Quality of Service (QoS)

Understanding QoS

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS permits the assignment of various grades of network service to different types of traffic such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of data and permits prioritization of certain applications across the network. You can define exactly how you want the switch to treat selected applications and types of traffic. Use QoS on the system to control a wide variety of network traffic functions by:

- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, setting higher priorities for time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Providing predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improving performance for specific types of traffic and preserving performance as the amount of traffic grows.
- Reducing the need to constantly add bandwidth to the network.
- Managing network congestion.

QoS terminology

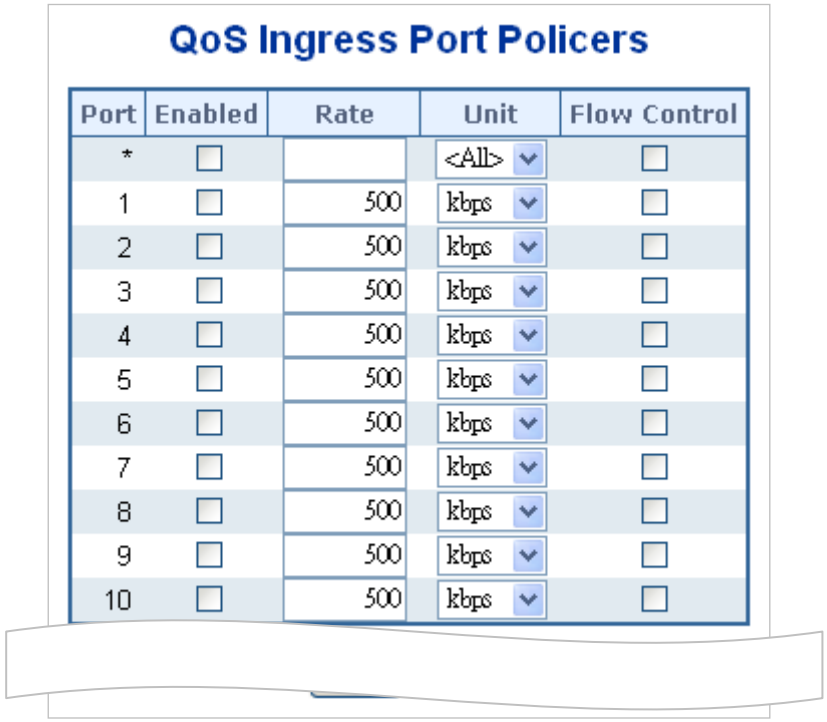
- **Classifier** – Classifies the traffic on the network. Traffic classifications are determined by protocol, application, source, destination, and so on. You can create and modify classifications. The managed switch then groups classified traffic in order to schedule them with the appropriate service level.
- **DiffServ Code Point (DSCP)** – Traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.
- **Service Level** – Defines the priority given to a set of classified traffic. You can create and modify service levels.
- **Policy** – Comprises a set of rules that are applied to a network so that a network meets the needs of the business. That is, traffic can be prioritized across a network according to its importance to that particular business type.
- **QoS Profile** – Consists of multiple sets of rules (classifier plus service level combinations). The QoS profile is assigned to a port(s).
- **Rules** – Comprises a service level and a classifier to define how the managed switch will treat certain types of traffic. Rules are associated with a QoS profile.

To implement QoS on a network, perform the following actions:

1. Define a service level to determine the priority that will be applied to traffic.
2. Apply a classifier to determine how the incoming traffic will be classified and thus treated by the managed switch.
3. Create a QoS profile that associates a service level and a classifier.
4. Apply a QoS profile to a port(s).

Port policing

The QoS Ingress Port Policers page permits configuration of the policer settings for all switch ports.



The page includes the following fields:

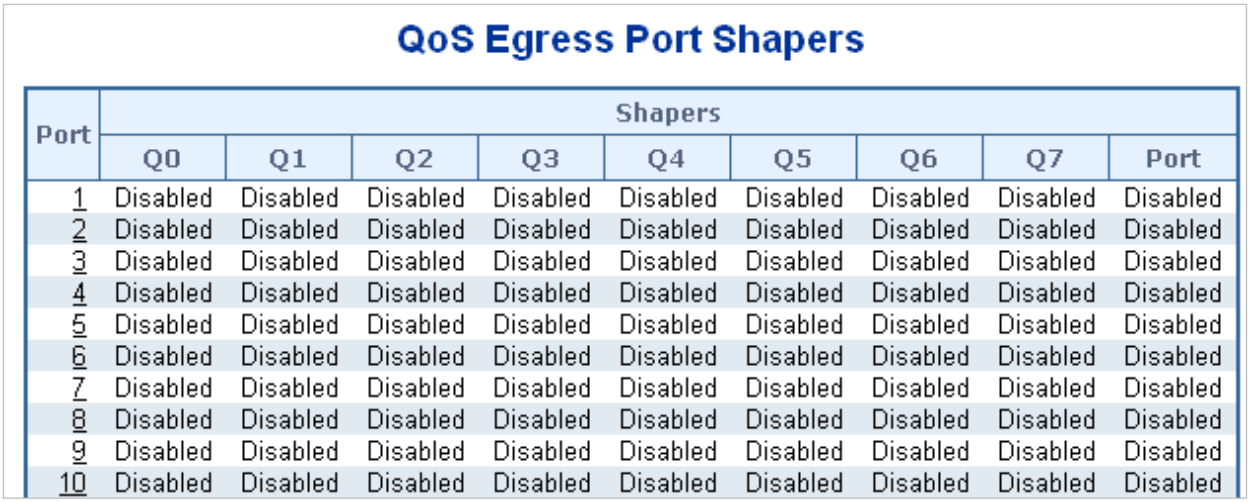
Object	Description
Port	The port number for which the configuration below applies.
Enable	Controls whether the policer is enabled on this switch port.
Rate	Controls the rate for the policer. The default value is 500. This value is restricted to **100-1000000** when the Unit is **kbps** or **fps**, and it is restricted to **1-3300** 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

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port shaping

The QoS Egress Port Shapers page provides an overview of the QoS egress port shapers for all switch ports.



QoS Egress Port Shapers

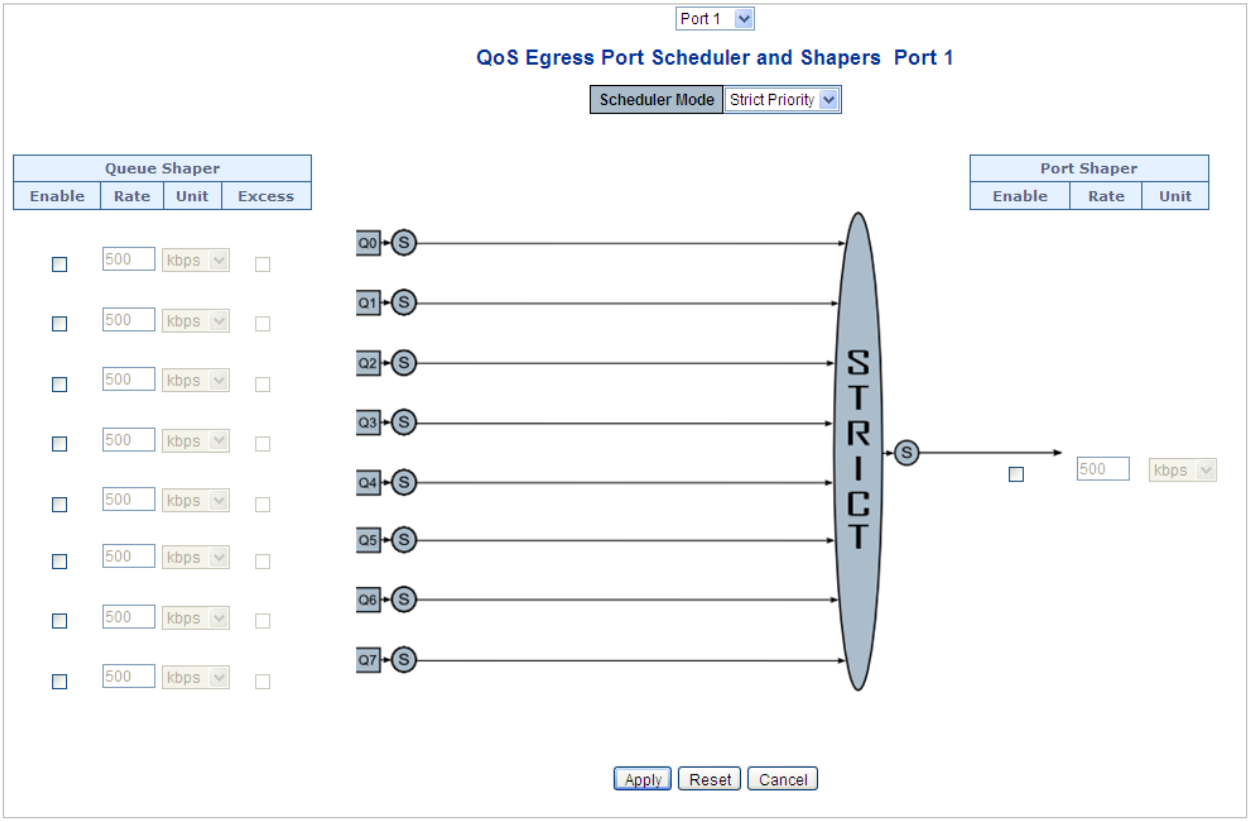
Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
4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

The page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row. Click on the port number to configure the shapers. For more details, refer to “Understanding QoS” on page 171.
Q0 ~Q7	Shows "disabled" or actual queue shaper rate (e.g., "800 Mbps").
Port	Shows "disabled" or actual port shaper rate (e.g., "800 Mbps").

QoS egress port schedule and shapers

The port scheduler and shapers for a specific port are configured on the QoS Egress Port Schedule and Shapers page.



The page includes the following fields:

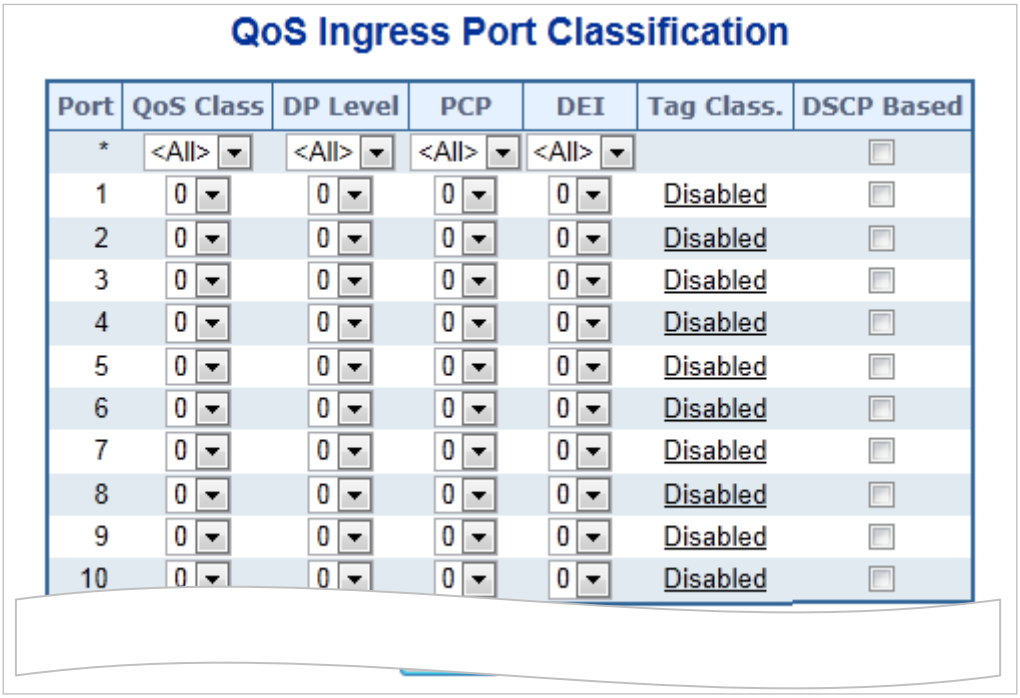
Object	Description
Scheduler Mode	Controls whether the scheduler mode is **Strict Priority** or **Weighted** on this switch port.
Queue Shaper Enable	Controls whether the queue shaper is enabled for this queue on this switch port.
Queue Shaper Rate	Controls the rate for the queue shaper. The default 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 only appears if Scheduler Mode is set to **Weighted**.
Queue Scheduler Percent	Shows the weight in percent for this queue. This parameter only appears 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

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Cancel** to undo any changes made locally and return to the previous page.

Port classification

The QoS Ingress Port Classification page permits configuration of the basic QoS ingress classification settings for all switch ports.



The page includes the following fields:

Object	Description
Port	The port number for which the configuration below applies.
QoS Class	Controls the default class of service. All frames are classified to a QoS. There is a one to one mapping between CoS, queue, and priority. A QoS class of 0 (zero) has the lowest priority. **All** means all ports will have one specific setting.
DP Level	Controls the default drop precedence level. All frames are classified to a drop precedence level. If the port is VLAN-aware and the frame is tagged, then the frame is classified to a DPL that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DPL. The classified DPL can be overruled by a QCL entry. **All** means all ports will have one specific setting.
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. **All** means all ports will have one specific setting.
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. **All** means all ports will have one specific setting.
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 to configure the mode and/or mapping.

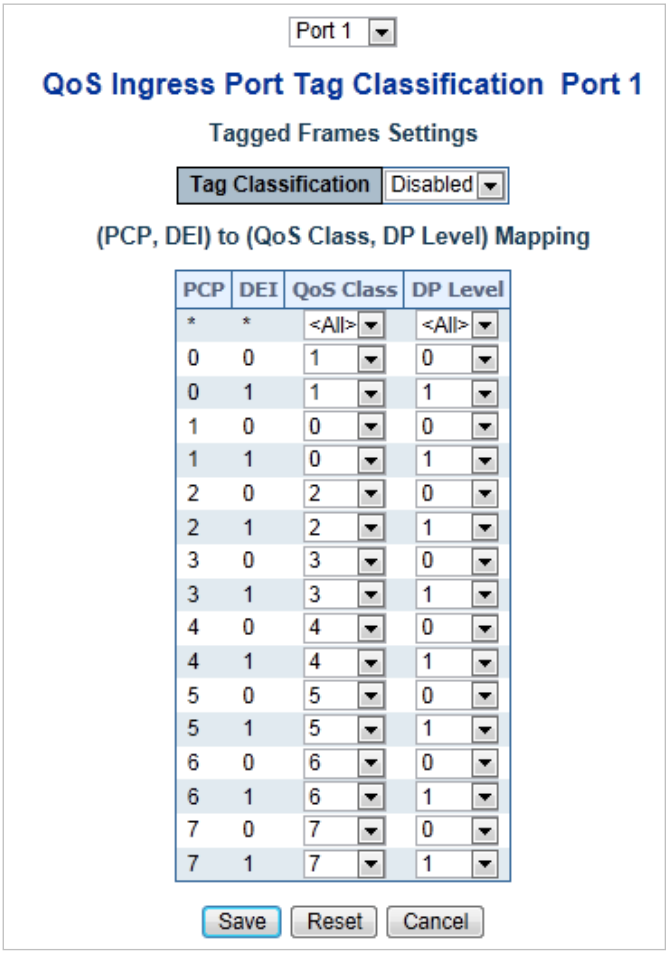
Object	Description
DSCP Based	Select **DSCP Based** to enable DSCP-based QoS ingress port classification.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

QoS ingress port tag classification

Configure the classification modes for tagged frames on this page.



The page includes the following fields:

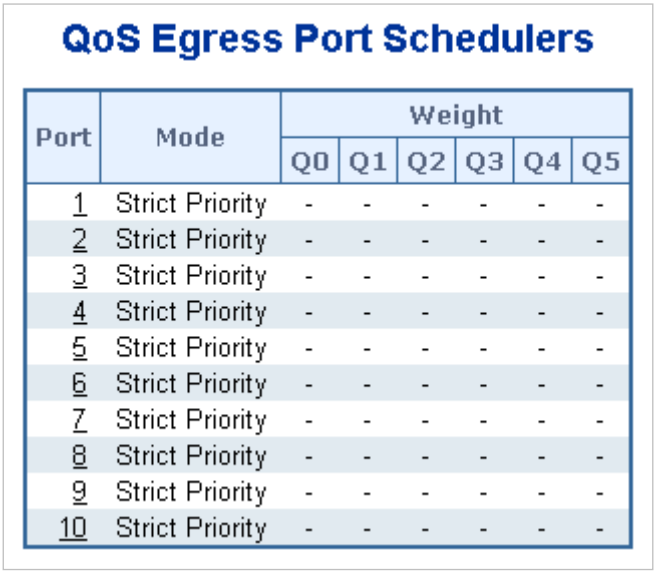
Object	Description
Tag Classification	Controls the classification mode for tagged frames on this port. **Disabled**: Use default QoS class and DP level for tagged frames. **Enabled**: Use mapped versions of PCP and DEI for tagged frames.
(PCP, DEI) to (QoS class, DP level) Mapping	The Configuration All with available values will assign to whole items. Controls the mapping of the classified (PCP, DEI) to (QoS class, DP level) values when Tag Classification is set to **Enabled**.

Buttons

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

Port scheduler

The QoS Egress Port Schedulers page provides an overview of the QoS egress port schedulers for all switch ports.



QoS Egress Port Schedulers

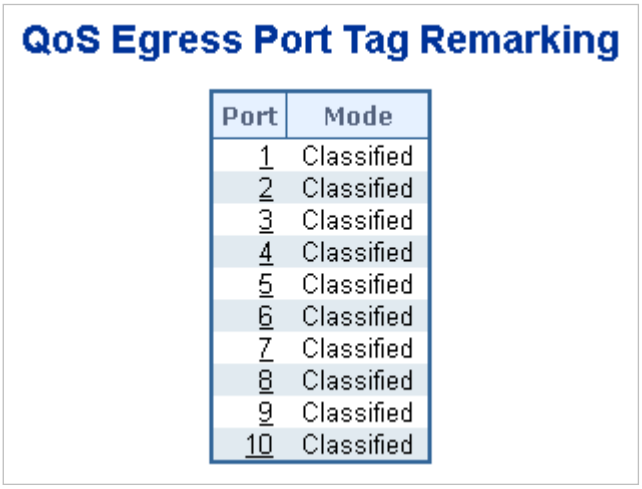
Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-

The page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row. Click on the port number to configure the schedulers. For more details, refer to “Understanding QoS” on page 171.
Mode	Shows the scheduling mode for this port.
Q0 ~ Q5	Shows the weight for this queue and port.

Port tag remarking

The QoS Egress Port Tag Remarking page provides an overview of QoS egress port tag remarking for all switch ports.



The page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row. Click on the port number to configure tag remarking. For further details, refer to “QoS egress port tag remarking” below.
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.

QoS egress port tag remarking

The QoS Egress Port Tag Remarking page can also provide an overview of QoS egress port tag remarking for a specific port.

The page includes the following fields:

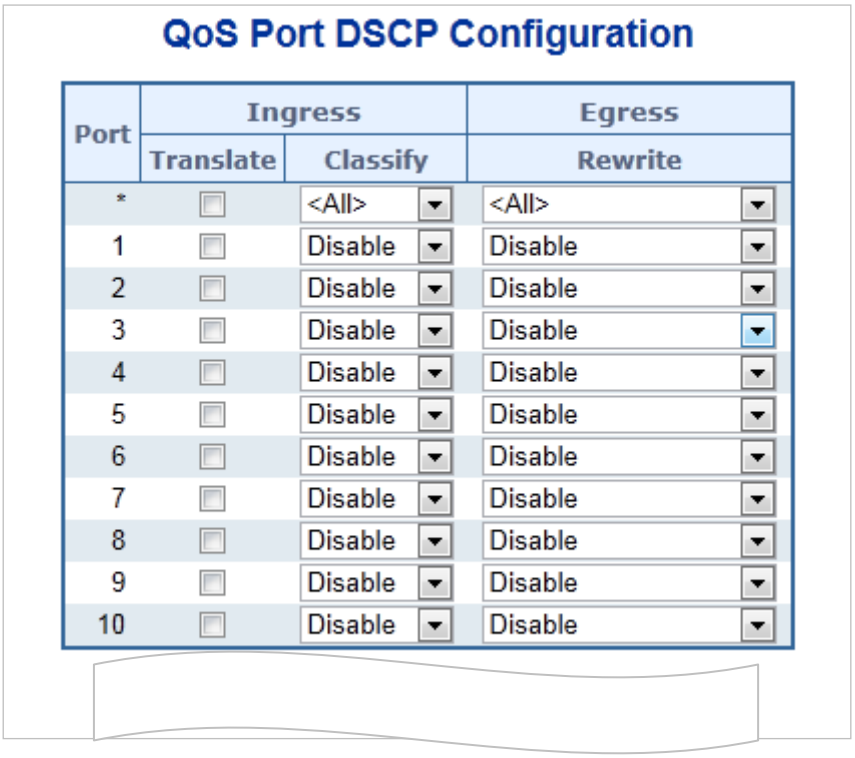
Object	Description
Mode	Controls the tag remarking mode for this port. **Classified**: Use classified PCP/DEI values. **Default**: Use default PCP/DEI values. **Mapped**: Use mapped versions of QoS class and DP level.
PCP/DEI Configuration	Controls the default PCP and DEI values used when the mode is set to **Default**.
(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

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Cancel** to return to the previous page.

Port DSCP

The QoS Port DSCP Configuration page permits configuration of the basic QoS port DSCP settings for all switch ports.



The page includes the following fields:

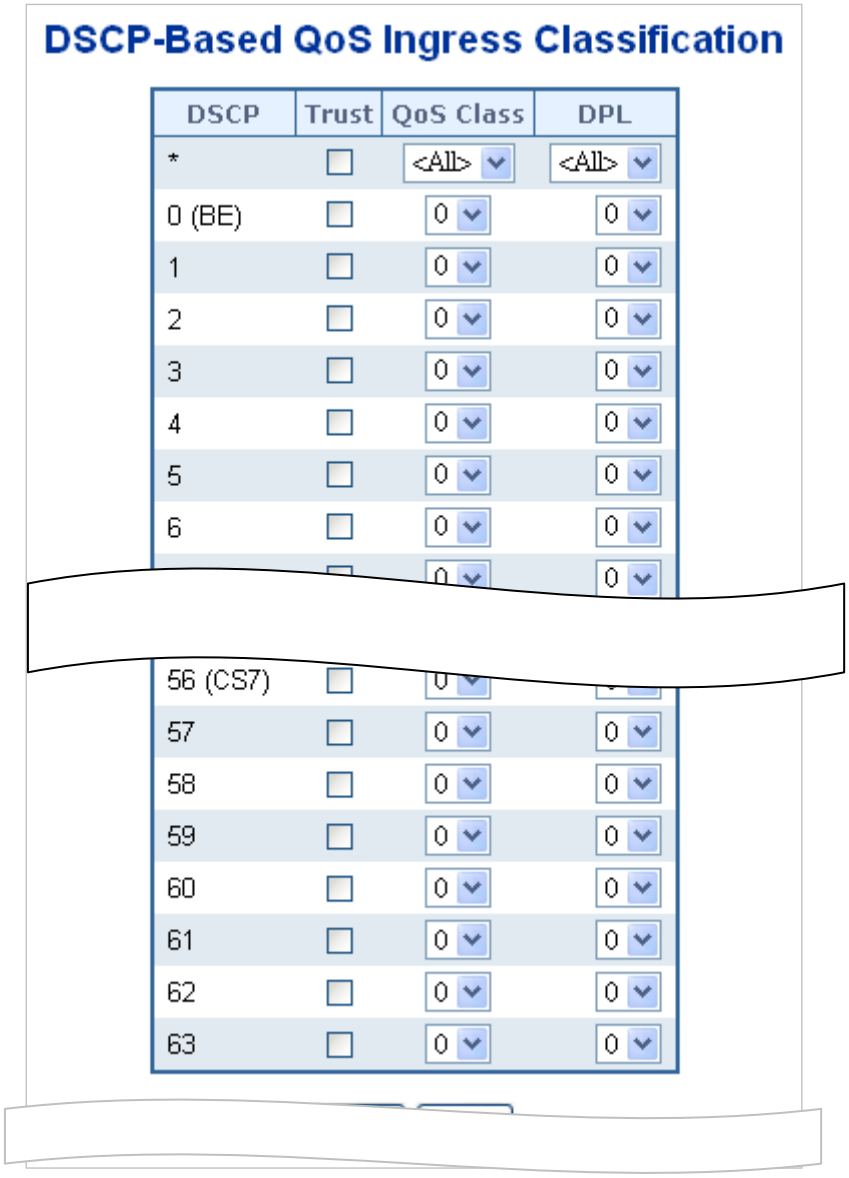
Object	Description
Port	The Port column shows the list of ports for which DSCP ingress and egress settings can be configured.
Ingress	Change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: **Translate** **Classify**
Translate	Select the **Translate** check box to enable the Ingress translation.
Classify	Selections are as follows: **Disable**: No Ingress DSCP Classification. **DSCP=0**: Classify if incoming (or translated if enabled) DSCP is 0. **Selected**: Classify only the selected DSCP for which classification is enabled as specified in the DSCP Translation window for the specific DSCP. **All**: Classify all DSCP.
Egress	Selections for Rewrite are as follows: **Disable**: No egress rewrite. **Enable**: Rewrite enabled without remapping. **Remap DP Unaware**: DSCP from the analyzer is remapped and the frame is remarked with the remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. **Remap DP Aware**: DSCP from the analyzer is remapped and the frame is remarked with the remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

DSCP-based QoS

The QoS DSCP-Based QoS Ingress Classification page permits configuration of the basic QoS DSCP-based QoS ingress classification settings for all switches.



The page includes the following fields:

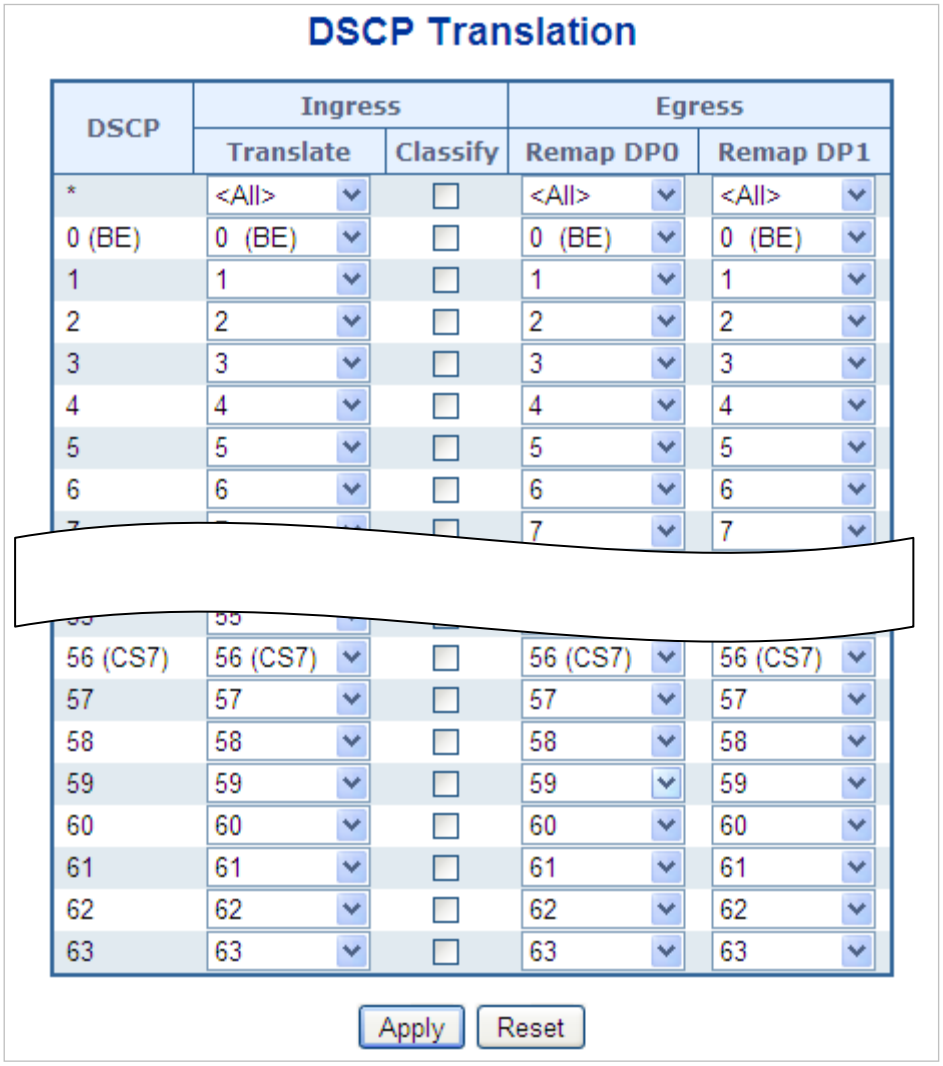
Object	Description
DSCP	Maximum number of supported DSCP values is 64.
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS Class	QoS Class values can be between **0**-**7**.
DPL	Drop Precedence Level (**0**-**1**)

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

DSCP translation

The DSCP Translation page permits configuration of the basic QoS DSCP translation settings for all switches. DSCP translation can be done in Ingress or Egress.



The page includes the following fields:

Object	Description
DSCP	The maximum number of supported DSCP values is 64 and valid DSCP values range from 0 to 63.
Ingress	The Ingress side of DSCP can be first translated to new DSCP before using the DSCP for the QoS class and DPL map. There are two configuration parameters for DSCP Translation: **Translate** **Classify**
Translate	DSCP at the Ingress side can be translated to any of 0-63 DSCP values.
Classify	Click **Classify** to enable classification at the Ingress side.

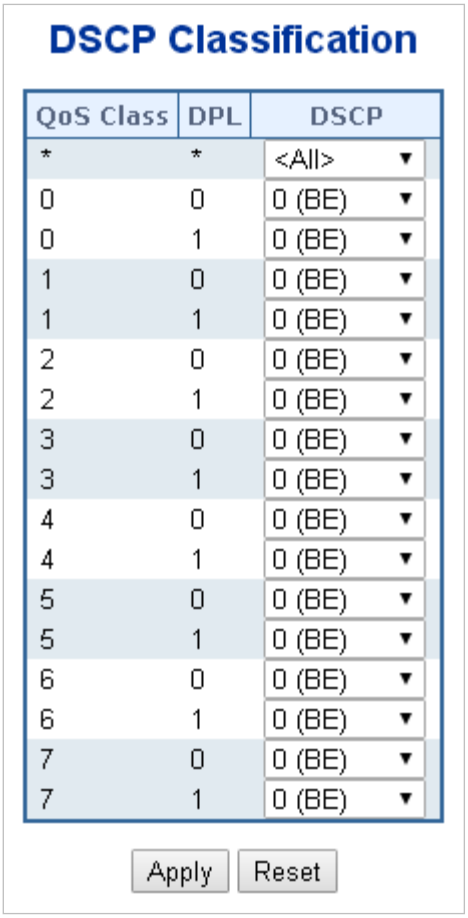
Object	Description
Egress	There are the following configurable parameters for Egress side – **Remap DP0** Controls the remapping for frames with DP level 0. **Remap DP1** Controls the remapping for frames with DP level 1.
Remap DP0	The Configuration All with available values will assign to whole DSCP values. Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.
Remap DP1	The Configuration All with available values will assign to whole DSCP values. Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

DSCP classification

The DSCP Classification page permits mapping a DSCP value to a QoS Class and DPL value.



The page includes the following fields:

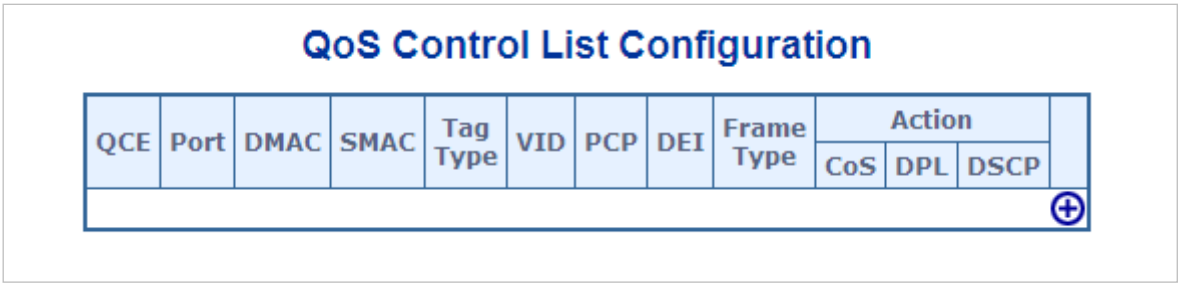
Object	Description
QoS Class	Available QoS Class values range from 0 to 7. QoS Class (0-7) can be mapped to followed parameters.
DPL	Actual Drop Precedence Level.
DSCP	Select DSCP value (0-63) from DSCP menu to map DSCP to corresponding QoS Class and DPL value

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

QoS control list

The QoS Control List Configuration 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.



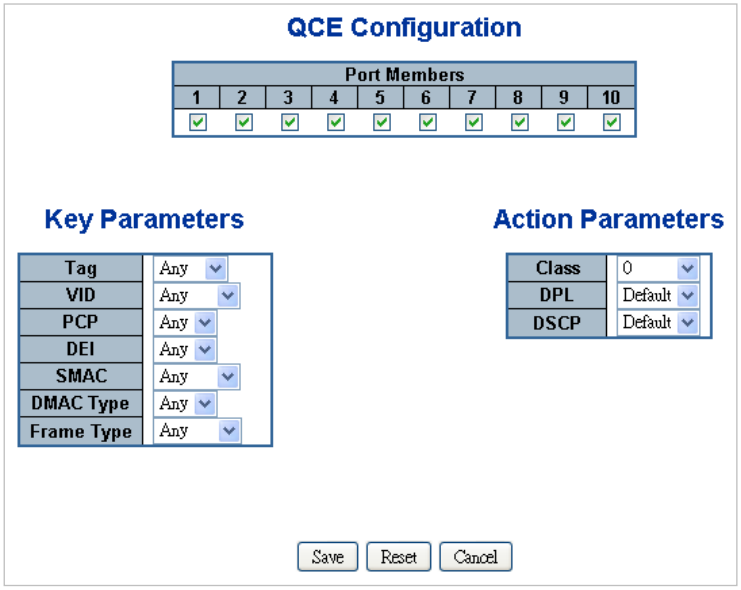
The page includes the following fields:

Object	Description
QCE#	Indicates the index of QCE.
Port	Indicates the list of ports configured with the QCE.
DMAC	Specify the type of Destination MAC addresses for incoming frames. Selections include: **Any**: All types of Destination MAC addresses are allowed. Default value. **Unicast**: Only Unicast MAC addresses are allowed. **Multicast**: Only Multicast MAC addresses are allowed. **Broadcast**: Only Broadcast MAC addresses are allowed.
SMAC	Displays the OUI field of Source MAC address (i.e., the first three octets (in bytes) of the MAC address).
Tag Type	Indicates tag type. Selections include: **Any**: Match tagged and untagged frames. Default value. **Untagged**: Match untagged frames.

Object	Description
	Tagged: Match tagged frames.
VID	Indicates VLAN ID (either a specific VID or range of VIDs). VID can be in the range of **1-4095** or **Any**.
PCP	Priority Code Point: Valid PCP values are specific (0, 1, 2, 3, 4, 5, 6, 7), a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7), or **Any**.
DEI	Drop Eligible Indicator: Selections include **0**, **1**, or **Any**.
Frame Type	Indicates the type of frame to look for incoming frames. Selections include: **Any**: The QCE will match all frame types. **Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. **LLC**: Only (LLC) frames are allowed. **SNAP**: Only (SNAP) frames are allowed. **IPv4**: The QCE only matches IPV4 frames. **IPv6**: The QCE only matches IPV6 frames.
Action	Indicates the classification action taken on the ingress frame if the parameters configured match with the frame's content. Action fields include: **Class**: Classified QoS class. **DPL**: Classified Drop Precedence Level. **DSCP**: Classified DSCP value.
Modification Buttons	Modify each QCE in the table using the following buttons: : Inserts a new QCE before the current row. : Edits the QCE. : Moves the QCE up the list. : Moves the QCE down the list. : Deletes the QCE. : The lowest plus sign adds a new entry at the bottom of the list of QCL.

QoS control entry configuration

The QCE Configuration page appears as follows:



The page includes the following fields:

Object	Description
Port Members	Select the **Port Members** check boxes to make any port a member of the QCL entry. All ports are selected by default.
Key Parameters	Key configuration selections are as follows: **DMAC Type** – Destination MAC type: possible values are unicast (**UC**), multicast (**MC**), broadcast (**BC**) or **Any**. **SMAC** – Source MAC address: 24 MS bits (**OUI**) or **Any**. **Tag** – Value of Tag field can be **Any**, **Untag**, or **Tag**. **VID** – Valid value of VLAN ID can be any value in the range 1-4095 or **Any**. The user can enter either a specific value or a range of VIDs **PCP** – Priority Code Point: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or **Any**. **DEI** – Drop Eligible Indicator: Selections include **0**, **1**, or **Any**. **Frame Type** – Frame Type can have any of the following values: **Any**, **Ethernet**, **LLC**, **SNAP**, **IPv4**, or **IPv6.** **Note**: These frame types are described below.
Any	Allow all types of frames.
EtherType	**Ethernet Type** –Ethernet types can have values of **0x600-0xFFFF** or **Any**. Excluding 0x800(IPv4) and 0x86DD(IPv6), the default value is **Any**.
LLC	**SSAP Address** – SSAP (Source Service Access Point) selections are **0x00** to **0xFF** or **Any** (default value). **DSAP Address** – DSAP (Destination Service Access Point) selections are **0x00** to **0xFF** or **Any** (default value). **Control Address** – Control Address selections are **0x00** to **0xFF** or **Any** (default value).
SNAP	**PID** – PID(a.k.a., Ethernet type) elections are **0x00** to **0xFFFF** or **Any** (default value).
IPv4	**Protocol** – IP protocol number: (**0-255**, **TCP** or **UDP**) or **Any**. **Source IP** – Specific Source IP address in value/mask format or **Any**. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. **DSCP** – Diffserv Code Point value (DSCP): It can be a specific value, range of values, or **Any**. DSCP values are in the range of 0-63 including BE, CS1-CS7, EF or AF11-AF43. **IP Fragment** – IPv4 frame fragmented option: yes, no, any. **Sport** – Source TCP/UDP port: (0-65535) or **Any**, specific or port range applicable for IP protocol UDP/TCP. **Dport** – Destination TCP/UDP port: (0-65535) or **Any**, specific or port range applicable for IP protocol UDP/TCP.
IPv6	**Protocol** – IP protocol number: (0-255, TCP or UDP) or **Any**. **Source IP** – IPv6 source address: (a.b.c.d) or **Any**, 32 LS bits. **DSCP** – Diffserv Code Point value (DSCP): It can be a specific value, range of values, or **Any**. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. **Sport** – Source TCP/UDP port:(0-65535) or **Any**, specific or port range applicable for IP protocol UDP/TCP.

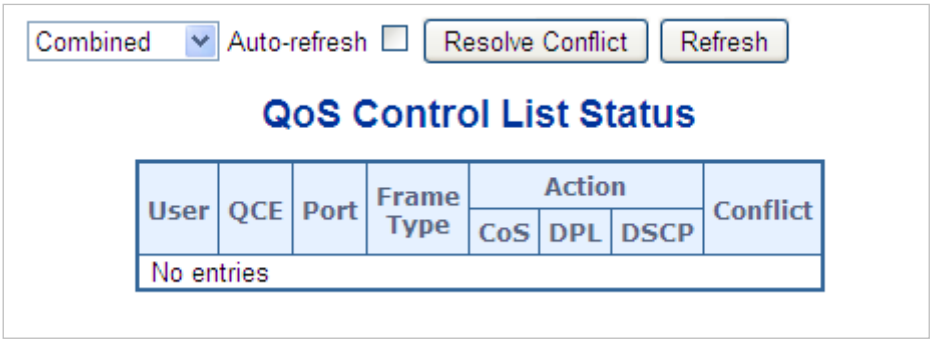
Object	Description
	Dport – Destination TCP/UDP port:(0-65535) or **Any**, specific or port range applicable for IP protocol UDP/TCP.
Action Parameters	**Class** – QoS class: (0-7) or **Default**. **DPL** – Drop Precedence Level selections include (**0-3**) or **Default**. **DSCP** – DSCP selections include (**0-63**, **BE**, **CS1-CS7**, **EF** or **AF11-AF43**) or **Default**. **Default** indicates that the default classified value is not modified by this QCE.

Buttons

- Click **Save** to save changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Cancel** to return to the previous page without saving the configuration change.

QCL status

The QoS Control List Status page shows the QCL status by different QCL users. Each row describes the QCE that is defined. A conflict occurs if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.



The page includes the following fields:

Object	Description
User	Indicates the QCL user.
QCE#	Indicates the index of QCE.
Port	Indicates the list of ports configured with the QCE.
Frame Type	Indicates the type of frame to look for incoming frames. Possible frame types are: **Any**: The QCE will match all frame types. **Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. **LLC**: Only (LLC) frames are allowed. **SNAP**: Only (SNAP) frames are allowed. **IPv4**: The QCE will match only IPV4 frames.

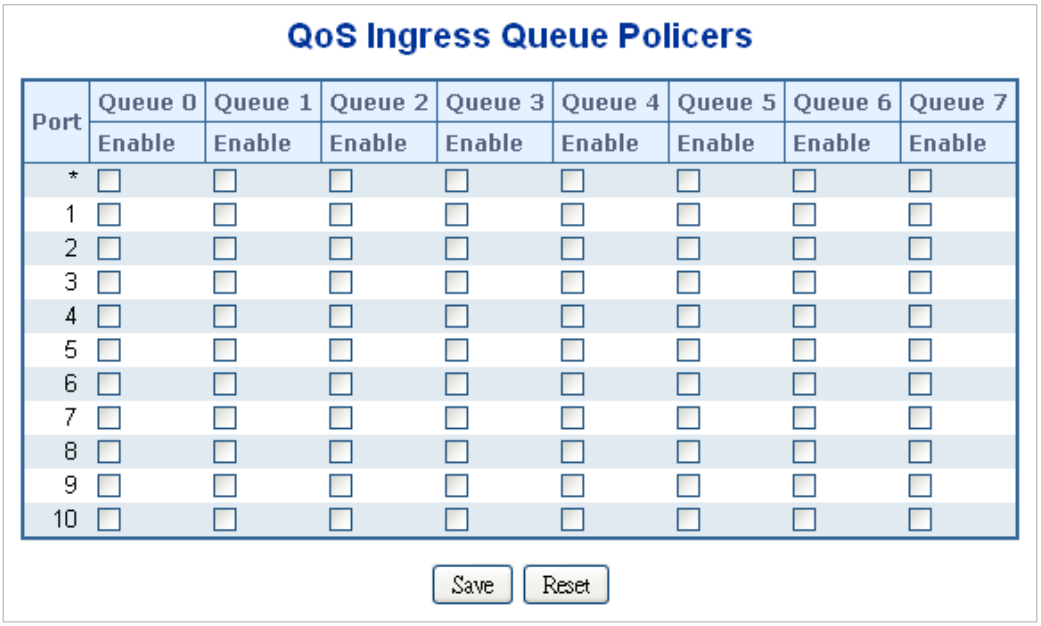
Object	Description
	IPv6: The QCE will match only IPV6 frames.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Action fields are as follows: **Class**: Classified QoS class. If a frame matches the QCE it will be put in the queue. **DPL**: Drop Precedence Level. If a frame matches the QCE then the DP level will be set to the value shown under the DPL column. **DSCP**: If a frame matches the QCE then DSCP will be classified with the value shown under DSCP column.
Conflict	Displays the conflict status of QCL entries when hardware resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in which case it shows conflict status as **Yes**, otherwise it is always **No**. Conflict can be resolved by releasing the hardware resources required to add the QCL entry by clicking the **Resolve Conflict** button.

Buttons

- Select the QCL status from the **Combined** drop-down list.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Resolve Conflict** to release the resources required to add the QCL entry when the conflict status for any QCL entry is **Yes**.
- Click **Refresh** to refresh the page.

Queue policing

Configure the queue policer settings for all switch ports in the QoS Ingress Queue Policers page.



The page includes the following fields:

Object	Description
Port	The port number for which the configuration below applies.
Enable (E)	Enable or disable the queue policer for this switch port.
Rate	Controls the rate for the queue policer. This value is restricted to 25-13128147 when "Unit" is kbps, and 1-13128 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if at least one of the queue policers are enabled.
Unit	Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if at least one of the queue policers are enabled.

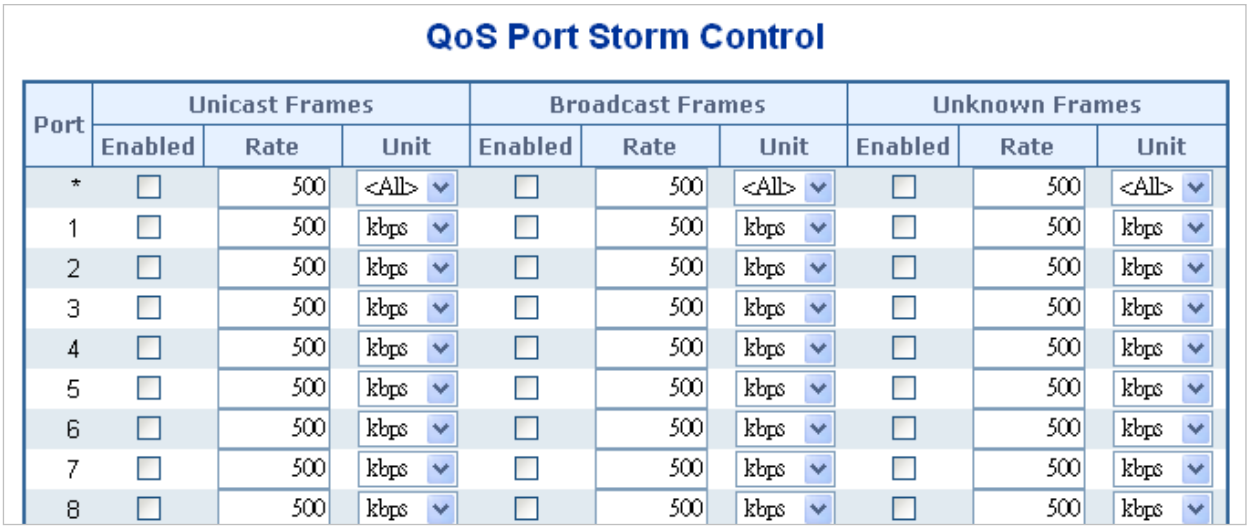
Buttons

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

Storm control configuration

Storm control for the switch is configured on the QoS Port Storm Control page. There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames (i.e., frames with a (VLAN ID, DMAC) pair not present on the MAC Address table).

The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.



The page includes the following fields:

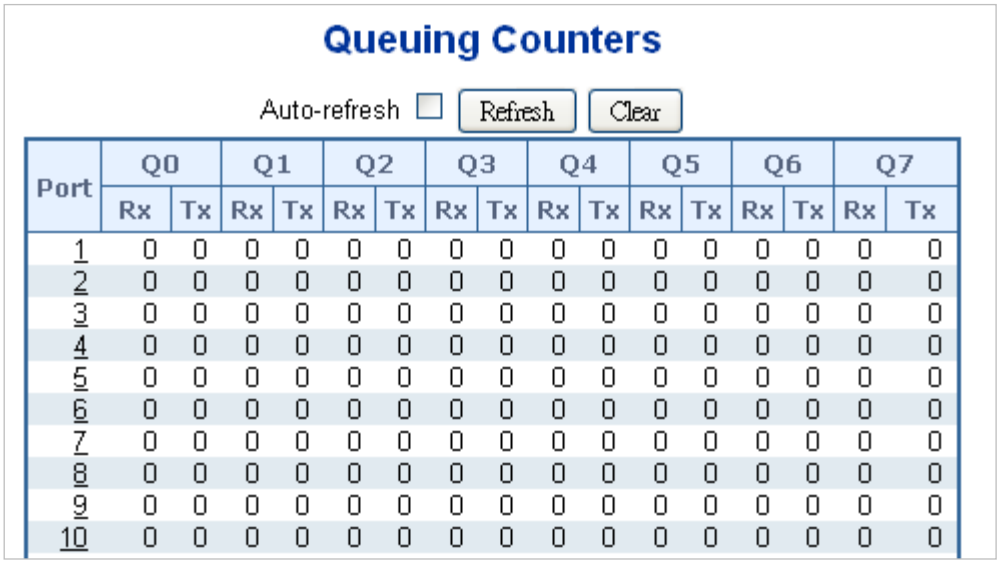
Object	Description
Port	The port number for which the configuration below applies.
Enable	Enable storm control on this switch port.
Rate	Controls the rate for the storm control. The default value is **500**. This value is restricted to **100-1000000** when the Unit is **kbps** or **fps**, and it is restricted 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

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

QoS statistics

The Queuing Counters page provides statistics for the different queues for all switch ports.



The page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row.
Q0 ~ Q7	There are eight QoS queues per port. Q0 is the lowest priority queue.
Rx/Tx	The number of received and transmitted packets per queue.

Buttons

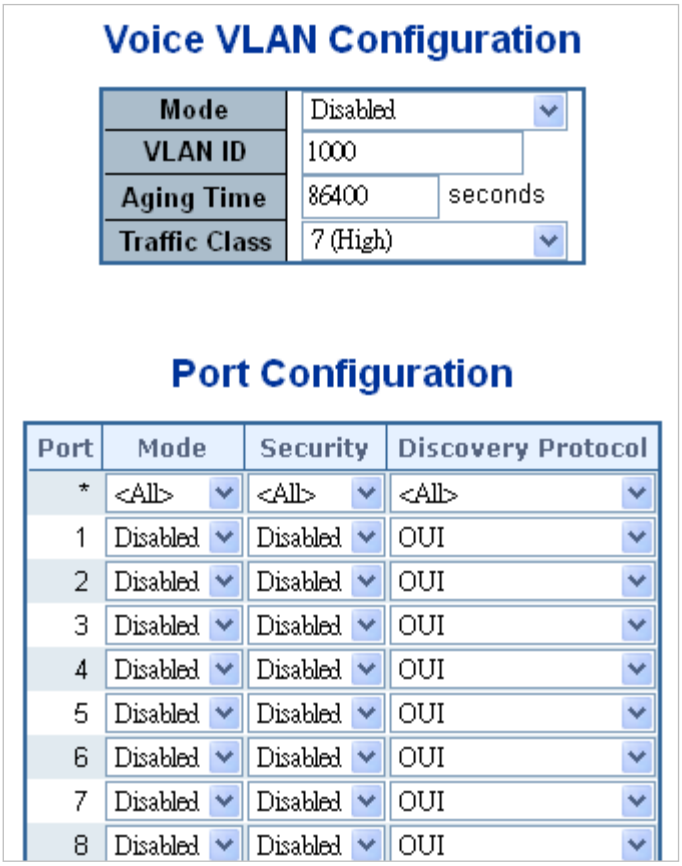
- Click **Refresh** to refresh the page.

- Click **Clear** to clear the counters for all ports.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.

Voice VLAN configuration

The Voice VLAN Configuration page contains the Voice VLAN feature. This enables voice traffic forwarding on the Voice VLAN, permitting the switch to classify and schedule network traffic. We recommended that there be two VLANs on a port – one for voice and 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.



The page includes the following fields:

Object	Description
Mode	Indicates the Voice VLAN mode operation. The MSTP feature must be disabled before enabling Voice VLAN. This helps avoid an ingress filter conflict. Selections include: **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. A configuration conflict occurs if the value equals management VID, MVR VID, PVID, etc.

Object	Description
	The permitted range is **1** to **4095**.
Aging Time	Indicates the Voice VLAN secure learning age time. The permitted range is **10** to **10000000** seconds. It is used when the security mode or auto detect mode is enabled. In other cases, it is based on hardware age time. The actual age time is situated in the [age_time; 2 * age_time] interval.
Traffic Class	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN applies to this class.
Mode	Indicates the Voice VLAN port mode. Selections include: **Disabled**: Disjoin from Voice VLAN. **Auto**: Enable auto detect mode. It detects if there is a 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-telephone MAC address in Voice VLAN are blocked 10 seconds. Selections include: **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 only works when auto detect mode is enabled. Enable the LLDP feature before configuring the discovery protocol to **LLDP** or **Both**. Changing the discovery protocol to **OUI** or **LLDP** restarts the auto detect process. Selections include: **OUI**: Detect telephony device by OUI address. **LLDP**: Detect telephony device by LLDP. **Both**: Both OUI and LLDP.

Voice VLAN OUI table

Configure Voice VLAN OUI table on the Voice VLAN OUI Table page. The maximum entry number is 16. Modifying the OUI table restarts auto detection of the OUI process.

The page includes the following fields:

Object	Description
Delete	Select the check boxes to delete the entry. Entries are deleted during the next save.
Telephony OUI	An telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be six characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
Description	The description of the OUI address. Normally, it describes the vendor telephony device it belongs to. The allowed string length is 0 to 32.

Buttons

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

Access Control Lists (ACL)

ACL is an acronym for Access Control List. It is the list table of ACEs containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine if there are specific traffic object access rights.

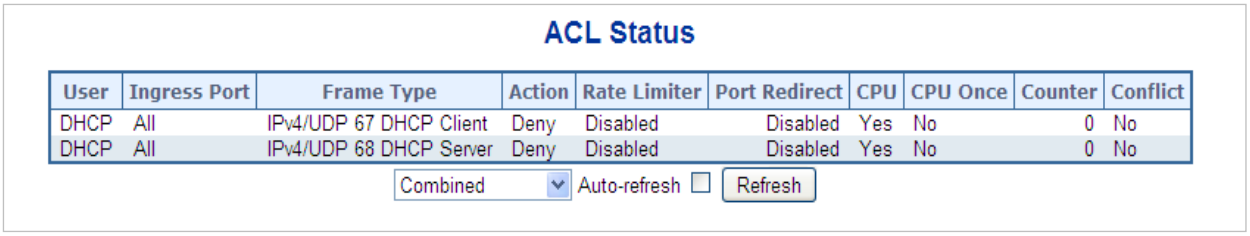
ACL implementations can be quite complex (as when the ACEs are prioritized for various situations). In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACLs can generally be configured to control inbound traffic and, in this context, they are similar to firewalls.

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual applications.

ACL status

The Voice VLAN OUI Table page shows the ACL status by different ACL users. Each row describes the ACE that is defined. A conflict occurs if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.



The page includes the following fields:

Object	Description
User	Indicates the ACL user.
Ingress Port	Indicates the ingress port of the ACE. Values include: **All**: The ACE matches all ingress ports. **Port**: The ACE matches a specific ingress port.
Frame Type	Indicates the frame type of the ACE. Values are: **Any**: The ACE matches any frame type. **EType**: The ACE matches Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. **ARP**: The ACE matches ARP/RARP frames. **IPv4**: The ACE matches all IPv4 frames. **IPv4/ICMP**: The ACE matches IPv4 frames with ICMP protocol. **IPv4/UDP**: The ACE matches IPv4 frames with UDP protocol. **IPv4/TCP**: The ACE matches IPv4 frames with TCP protocol. **IPv4/Other**: The ACE matches IPv4 frames, which are not ICMP/UDP/TCP. **IPv6**: The ACE matches 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 shown, 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 shown, the port redirect operation is disabled.
Mirror	Specify the mirror operation of this port. The allowed values are: **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is **Disabled**.
CPU	Forward packet that matched the specific ACE to CPU.
CPU Once	Forward first packet that matched the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Conflict	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

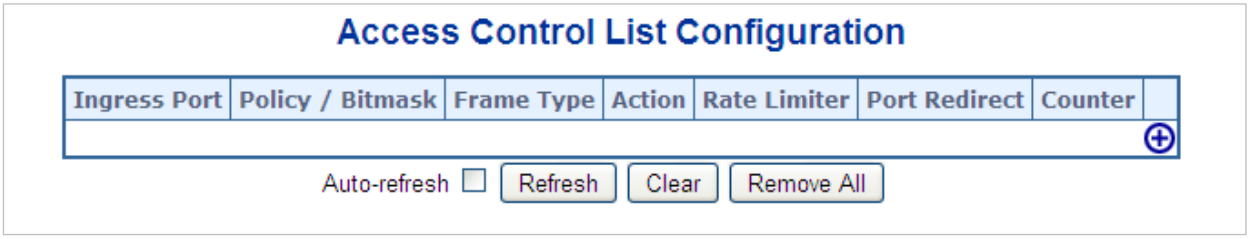
Buttons

- Select the ACL status from the **Combined** drop-down list.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page.

ACL configuration

The Access Control List Configuration 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 256 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.



The page includes the following fields:

Object	Description
Ingress Port	Indicates the ingress port of the ACE. Possible values are: **All**: The ACE matches all ingress port. **Port**: The ACE matches 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 matches any frame type. **EType**: The ACE matches Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. **ARP**: The ACE matches ARP/RARP frames. **IPv4**: The ACE matches all IPv4 frames. **IPv4/ICMP**: The ACE matches IPv4 frames with ICMP protocol. **IPv4/UDP**: The ACE matches IPv4 frames with UDP protocol. **IPv4/TCP**: The ACE matches IPv4 frames with TCP protocol. **IPv4/Other**: The ACE matches IPv4 frames, which are not ICMP/UDP/TCP. **IPv6**: The ACE matches 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 shown, the rate limiter operation is disabled.

Object	Description
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 shown, the port redirect operation is disabled.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Modification Buttons	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

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page.
- Click **Clear** to clear the counters.
- Click **Remove All** to remove all ACEs.

ACL ports configuration

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

ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*		<All>	<All>	<All>	<All>	<All>	<All>	<All>	*
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	276
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	490
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0

The page includes the following fields:

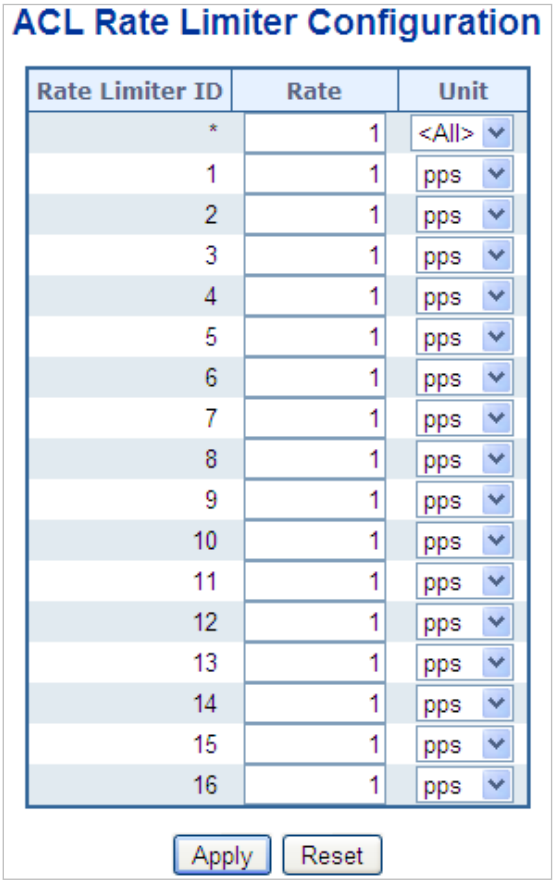
Object	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are **0** through **255**. The default value is 0.
Action	Select whether forwarding is permitted (**Permit**) or denied (**Deny**). The default value is **Permit**. **All** means all ports will have one specific setting.
Rate Limiter ID	Select which rate limiter to apply on this port. Selections include **Disabled** (default value) or the values **1** through **16**. **All** means all ports will have one specific setting.
Port Redirect	Select which port frames are redirected on. Selections include **Disabled** (default value)or a specific port number and it can't be set when action is permitted. **All** means all ports will have one specific setting.
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**. **All** means all ports will have one specific setting.
Logging	Specify the logging operation of this port. Selections include: **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**. **Note**: The System Log memory size and logging rate are limited. **All** means all ports will have one specific setting.
Shutdown	Specify the port shut down operation of this port. Selections include: **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**. **All** means all ports will have one specific setting.
State	Specify the port state of this port. Selections include: **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**. **All** means all ports will have one specific setting.
Counter	Counts the number of frames that match this ACE.

Buttons

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

ACL rate limiter configuration

Configure the rate limiter for the ACL of the managed switch on the ACL Rate Limiter Configuration page.



The page includes the following fields:

Object	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate (pps)	The allowed values are: **0-3276700** in pps or **0, 100, 200, 300, ..., 1000000** in kbps.
Unit	Specify the rate unit. The allowed values are: **pps**: packets per second. **kbps**: Kbits per second. **All** means all ports will have one specific setting.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Authentication

This section describes user access and management control for the managed switch, including user access and management control. The following main topics are covered:

- IEEE 802.1X port-based network access control
- MAC-based authentication
- User authentication

Overview of 802.1X (port-based) authentication

In 802.1X, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch 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 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 authenticator (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.

Overview of MAC-based authentication

Unlike 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 static entries into the MAC table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, therefore MAC-based authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g., through a third party switch or a hub) and still require individual authentication, and 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 that can be used by anyone, and only the MD5-Challenge method is supported.

The 802.1X and MAC-based authentication configuration consists of two sections, a system- and a port-wide.

Overview of user authentication

The managed switch may be configured to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and web browser. The managed switch provides secure network management access using the following options:

- Remote Authentication Dial-in User Service (RADIUS)
- Terminal Access Controller Access Control System Plus (TACACS+)
- Local user name and privilege level control

RADIUS and TACACS+ are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An authentication server contains a database of multiple user name / password pairs with associated privilege levels for each user that requires management access to the managed switch.

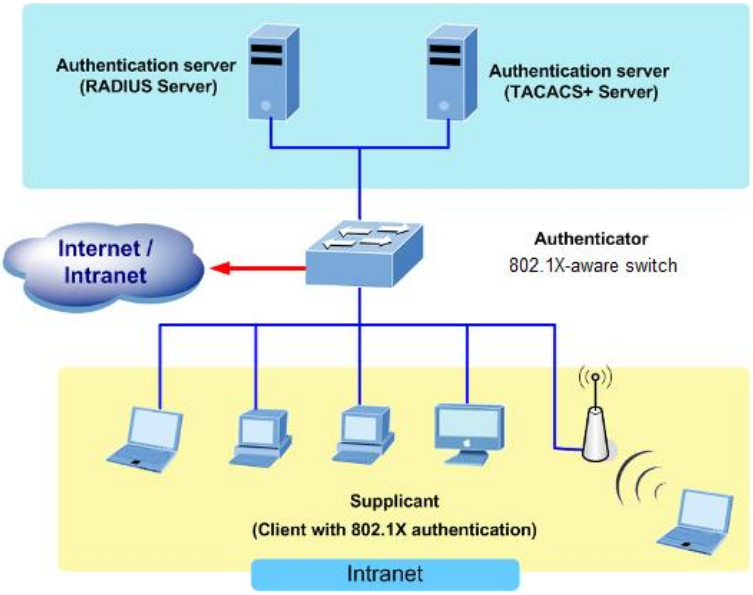
Understanding IEEE 802.1X port-based authentication

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making any services offered by the switch or the LAN available.

Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

Device roles

With 802.1X port-based authentication, the devices in the network have specific roles as shown below.



- **Client** – The device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft operating systems (the client is the supplicant in the IEEE 802.1X specification).
- **Authentication server** – Performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch if the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server, which is available in the Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- **Switch (802.1X device)** – Controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame which is then encapsulated for Ethernet and sent to the client.

Authentication initiation and message exchange

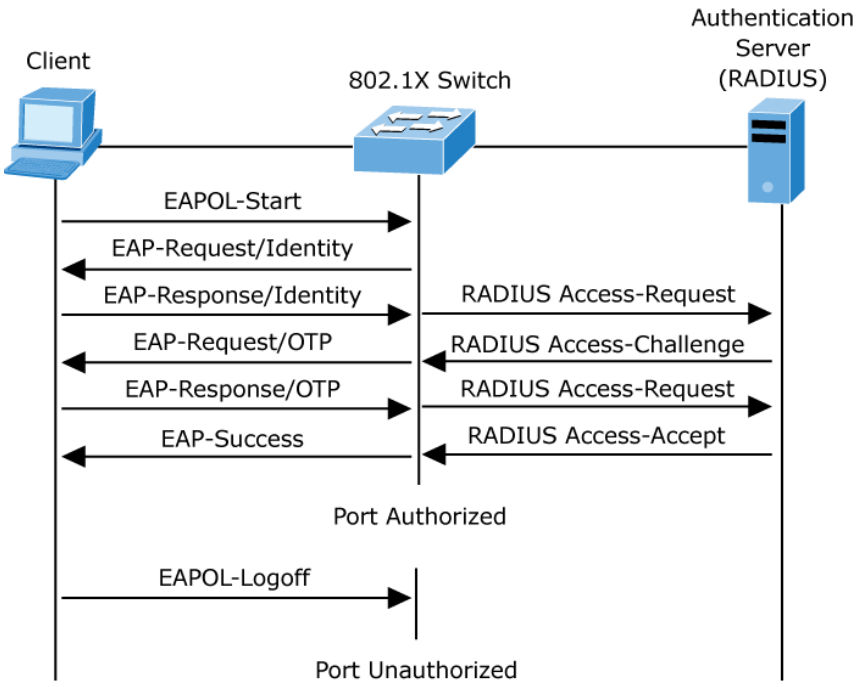
The switch or the client can initiate authentication. If you enable authentication on a port by using the dot1x port-control auto interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if the client does not receive an EAP-request/identity frame from the switch during bootup, the client can initiate authentication by sending an EAPOL-start frame which prompts the switch to request the client's identity.

Note: If 802.1X is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. The diagram below shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.



Ports in authorized and unauthorized states

The switch port state determines if the client is granted access to the network. The port starts in the unauthorized state. While in this state, the port disallows all ingress and

egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1X-enabled client connects to a port that is not running the 802.1X protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state

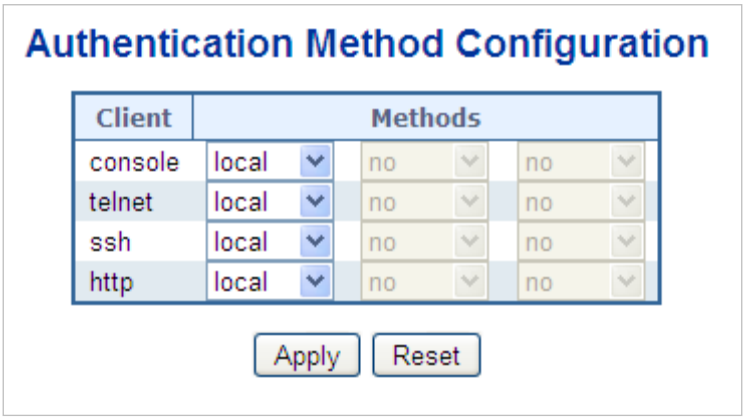
If the client is successfully authenticated (receives an accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message that causes the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

Authentication configuration

The Authentication Method Configuration page allows you to configure how a user is authenticated when logging into the switch via one of the management client interfaces.



The page includes the following fields:

Object	Description
Client	The management client for which the configuration below applies.
Authentication Method	Authentication method can be set to one of the following values: **None**: Authentication is disabled and login is not possible. **Local**: Use the local user database on the switch for authentication. **RADIUS**: Use a remote RADIUS server for authentication. **TACACS+**: Use a remote TACACS+ server 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, we recommend configuring secondary authentication as **local**. This permits the management client to log in via the local user database if none of the configured authentication servers are valid.
Fallback	Enable fallback to local authentication by selecting this check 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 something other than 'none or 'local'.

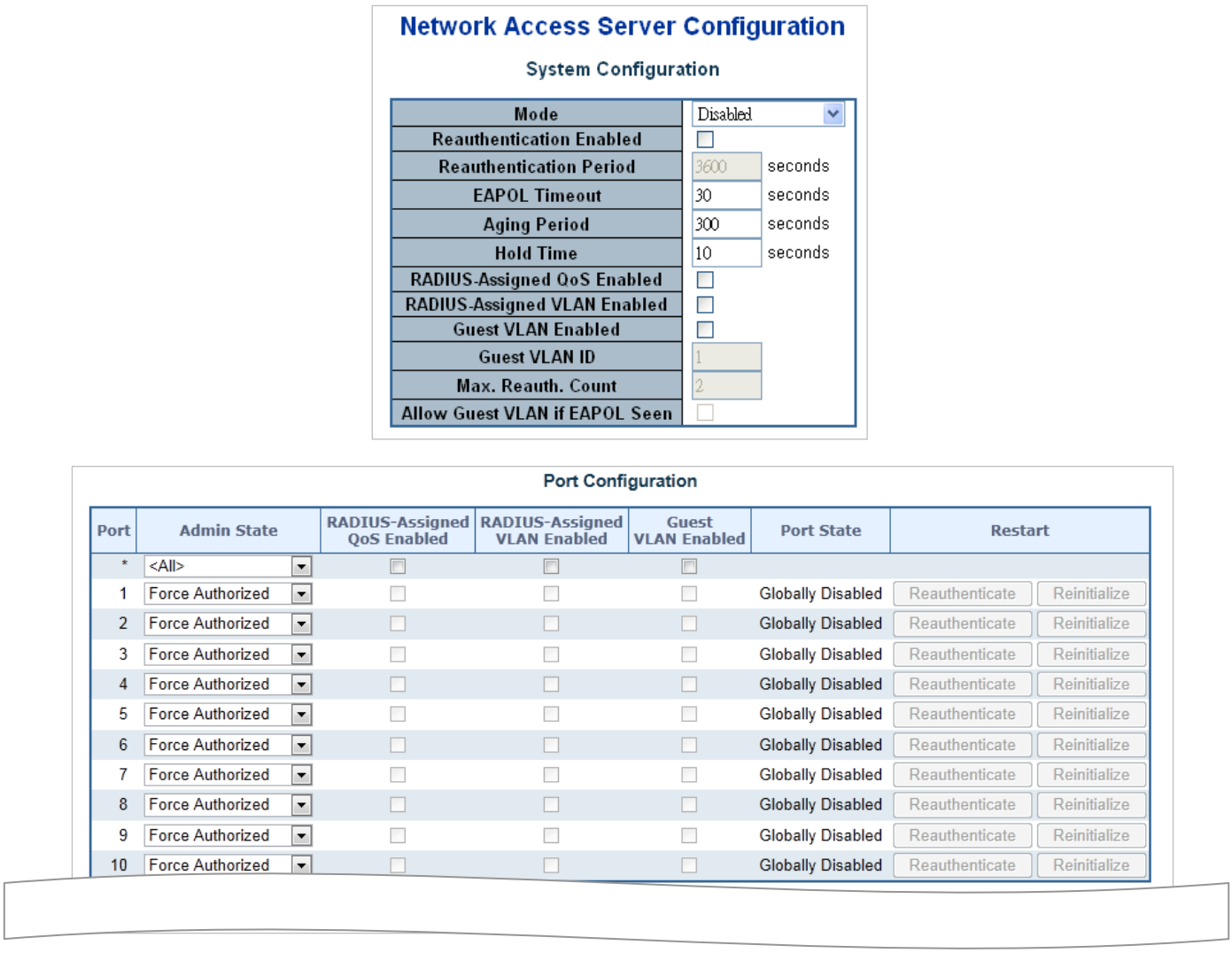
Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Network access server configuration

Configure the IEEE 802.1X and MAC-based authentication system and port settings on the Network Access Server Configuration page. 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, or the back end servers, determine if the user is allowed access to the network. These back end (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.

MAC-based authentication permits 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 the system. The switch uses the MAC address to authenticate against the back end 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.



Network Access Server Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	
RADIUS-Assigned VLAN Enabled	
Guest VLAN Enabled	
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<All>						
1	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized				Globally Disabled	Reauthenticate	Reinitialize

The page includes the following fields:

System configuration

Object	Description
Mode	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
Reauthentication Enabled	If selected, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the reauthentication period. Reauthentication 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, reauthentication 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.
Reauthentication Period	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the **Reauthentication Enabled** check box is selected. 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 on MAC-based ports.

Object	Description
Aging Period	This setting applies to the following modes (modes using 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 reauthentication is enabled and the port is in a 802.1X-based mode, this is not so criticial, since supplicants that are no longer attached to the port are removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect if the client is still attached, 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 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. The **RADIUS-Assigned QoS Enabled** check box provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When selected, the individual ports' ditto setting determines whether RADIUS-assigned QoS Class is enabled for that port. When deselected, RADIUS-server assigned QoS Class is disabled for 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. The **RADIUS-Assigned VLAN Enabled** check box provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When selected, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled for that port. When deselected, RADIUS-server assigned VLAN is disabled for all ports.

Object	Description
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** check box provides a quick way to globally enable/disable Guest VLAN functionality. When selected, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When deselected, the ability to move to the Guest VLAN is disabled for 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 to 4095.
Max. Reauth. Count	The number of times that 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 to 255.
Allow Guest VLAN if EAPOL Seen	The switch remembers if an EAPOL frame has been received on the port for the lifetime 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 (default setting), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the lifetime of the port. If enabled (selected), the switch considers entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.

Port configuration

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

Object	Description
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 sends one EAPOL success frame when the port link comes up, and any client on the port will be permitted network access without authentication. **Force Unauthorized** In this mode, the switch sends 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**

Object	Description
	In the 802.1X, 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 authenticator (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 back end 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). In this case, 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 back end 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 back end 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, the whole port is opened for network traffic after a supplicant is successfully authenticated on a port. This allows other clients connected to the port (through a hub, for example) 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. After 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 after successful authentication. **Multi 802.1X**

Object	Description
	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 authentication** 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 in the format "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, therefore MAC-based authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g., through a third party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. 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 (selected) for 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, it is invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class immediately reverts to the original QoS Class (which may be changed by the administrator in the meantime without affecting the RADIUS-assigned).

Object	Description
	This option is only available for single-client modes (i.e., Port-based 802.1X and 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 eight octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the required QoS Class in the range [0; 3].
RADIUS-Assigned VLAN Enabled	When RADIUS-Assigned VLAN is both globally enabled and enabled (selected) 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 immediately reverts 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 and Single 802.1X). For troubleshooting 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 fulfill 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 (selected) 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, and Multi 802.1X) For troubleshooting 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:**

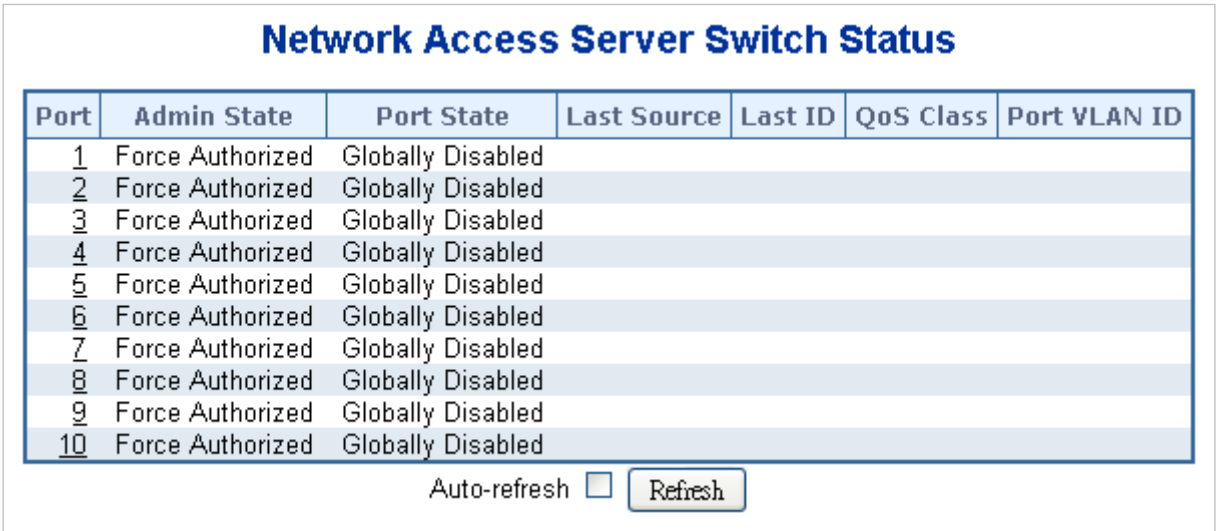
Object	Description
	When a Guest VLAN enabled port link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meantime, the switch considers entering the Guest VLAN. 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 is 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 is 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** check box is deselected.
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. **Reauthenticate**: Schedules a reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication is attempted immediately. The button only has an 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 reauthentication immediately. The clients transfer to the unauthorized state while the reauthentication is in progress.

Buttons

- Click **Refresh** to refresh the page.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Network access overview

The Network Access Overview page provides an overview of the current NAS port states for the selected switch.



The page includes the following fields:

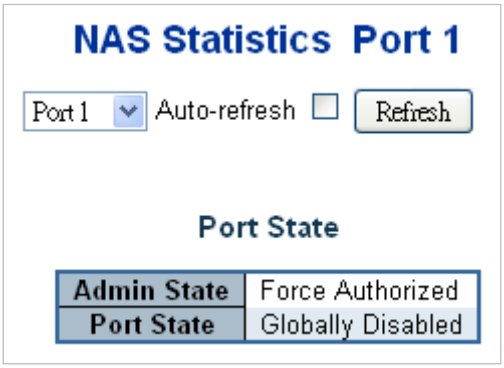
Object	Description
Port	The switch port number. Click to navigate to detailed NAS statistics.
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the 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 the most 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

- Click **Refresh** to refresh the page immediately.
- Click **Auto-refresh** to to refresh the page automatically. Automatic refresh occurs every three seconds.

Network access statistics

The Network Access Statistics page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it only shows selected back end server (RADIUS Authentication Server) statistics. Use the port drop-down menu to select the port details to be displayed.



The page includes the following fields:

Port state

Object	Description
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. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Port counters

Object	Description			
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**			
	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.
Back end Server Counters	These back end (RADIUS) frame counters are available for the following administrative states: **Port-based 802.1X** **Single 802.1X** **Multi 802.1X** **MAC-based Auth**.			

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 back end server following the first response from the supplicant. Indicates that the back end server has communication with the switch. **MAC-based**: Counts all Access Challenges received from the back end 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 back end 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 back end 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 back end 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 back end server. Indicates the switch attempted communication with the back end server. Possible retransmissions are not counted.

		MAC-based: Counts all the back end server packets sent from the switch towards the back end 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**.	

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

Object	Description
Selected Counters	The Selected Counters table is visible when the port is 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 address

Object	Description
Identity	Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and back end 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 back end 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 back end 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).

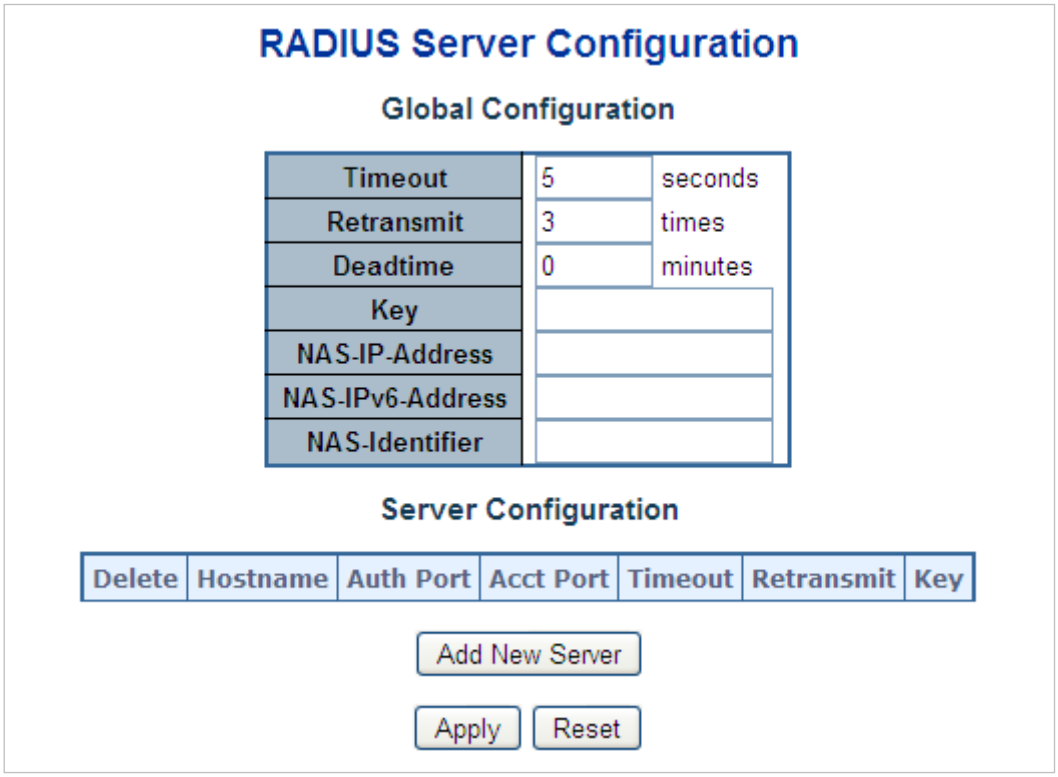
Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear the counters for the selected port. This button is available in the following modes:
  - Force Authorized
  - Force Unauthorized
  - Port-based 802.1X
  - Single 802.1X
- Click **Clear All** to clear both the port counters and all of the attached client's counters. Performing this action will not clear "Last Client." This button is available in the following modes:
  - Multi 802.1X
  - MAC-based Auth.X
- Click **Clear This** to clear only the currently selected client's counter. This button is available in the following modes:
  - Multi 802.1X

- MAC-based Auth.X

RADIUS

Configure the RADIUS servers on the RADIUS Server Configuration page.



The page includes the following fields:

Global configuration

These settings are common for all of the RADIUS Servers.

Object	Description
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.
Dead Time	The Dead Time, which can be set to a number between 0 and 3600 seconds, 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 Dead Time 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	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	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	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:

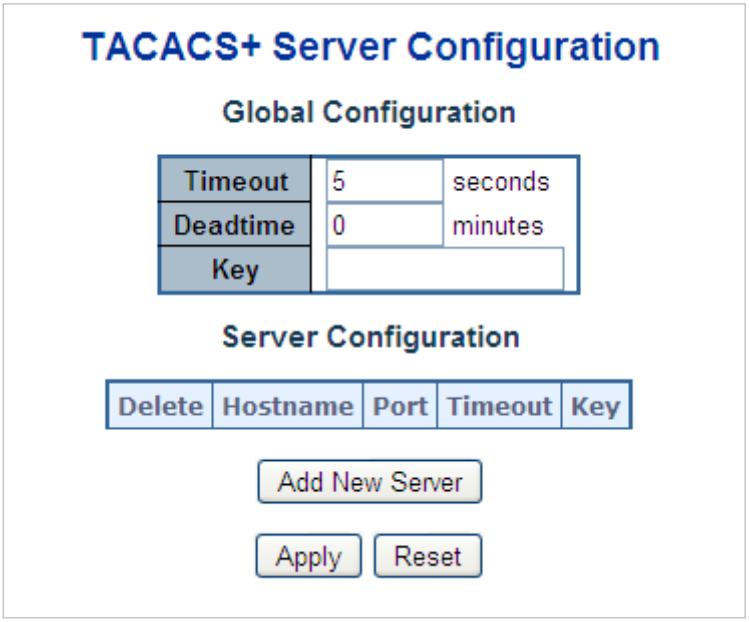
Object	Description
Delete	To delete a RADIUS server entry, check this box. The entry will be deleted during the next save.
Hostname	The IP address or hostname of the RADIUS server.
Auth Port	The UDP port to use on the RADIUS server for authentication.
Acct Port	The UDP port to use on the RADIUS server 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.

Buttons

- Click **Add New Server** 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 five servers are supported.
- Click **Delete** to undo the addition of the new server.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

TACACS+

The TACACS+ Server Configuration page permits configuration of the TACACS+ Servers.



The page includes the following fields:

Global configuration

These settings are common for all of the TACACS+ Servers.

Object	Description
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.
Dead Time	The Dead Time, which can be set to a number between 0 and 3600 seconds, 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 Dead Time 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.

Server configuration

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

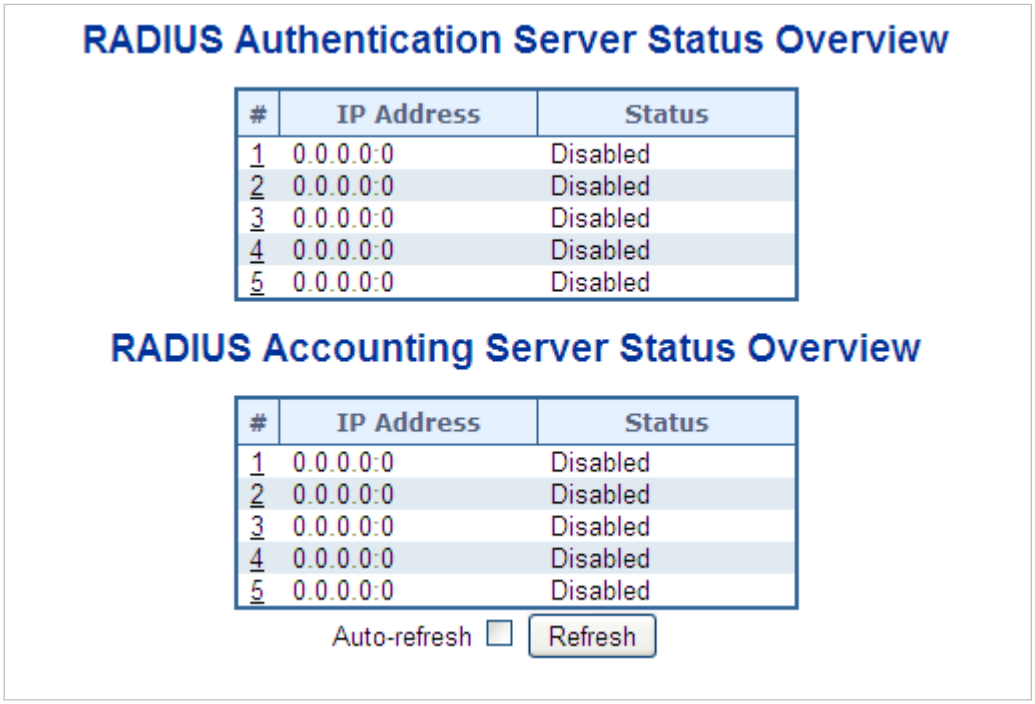
Object	Description
Delete	To delete a TACACS+ server entry, select this check box. The entry will be deleted during the next save.
Hostname	The IP address or hostname of the TACACS+ server.
Port	The TCP port to use on the TACACS+server for authentication.
Timeout	This optional setting overrides the global 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.

Buttons

- Click **Add New Server** to add a new TACACS+server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to five servers are supported.
- Click **Delete** to undo the addition of the new server.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

RADIUS overview

The RADIUS Authentication/Accounting Server Overview page provides an overview of the status of the RADIUS servers configurable on the authentication configuration page.



The page includes the following fields:

RADIUS authentication/accounting server status overview

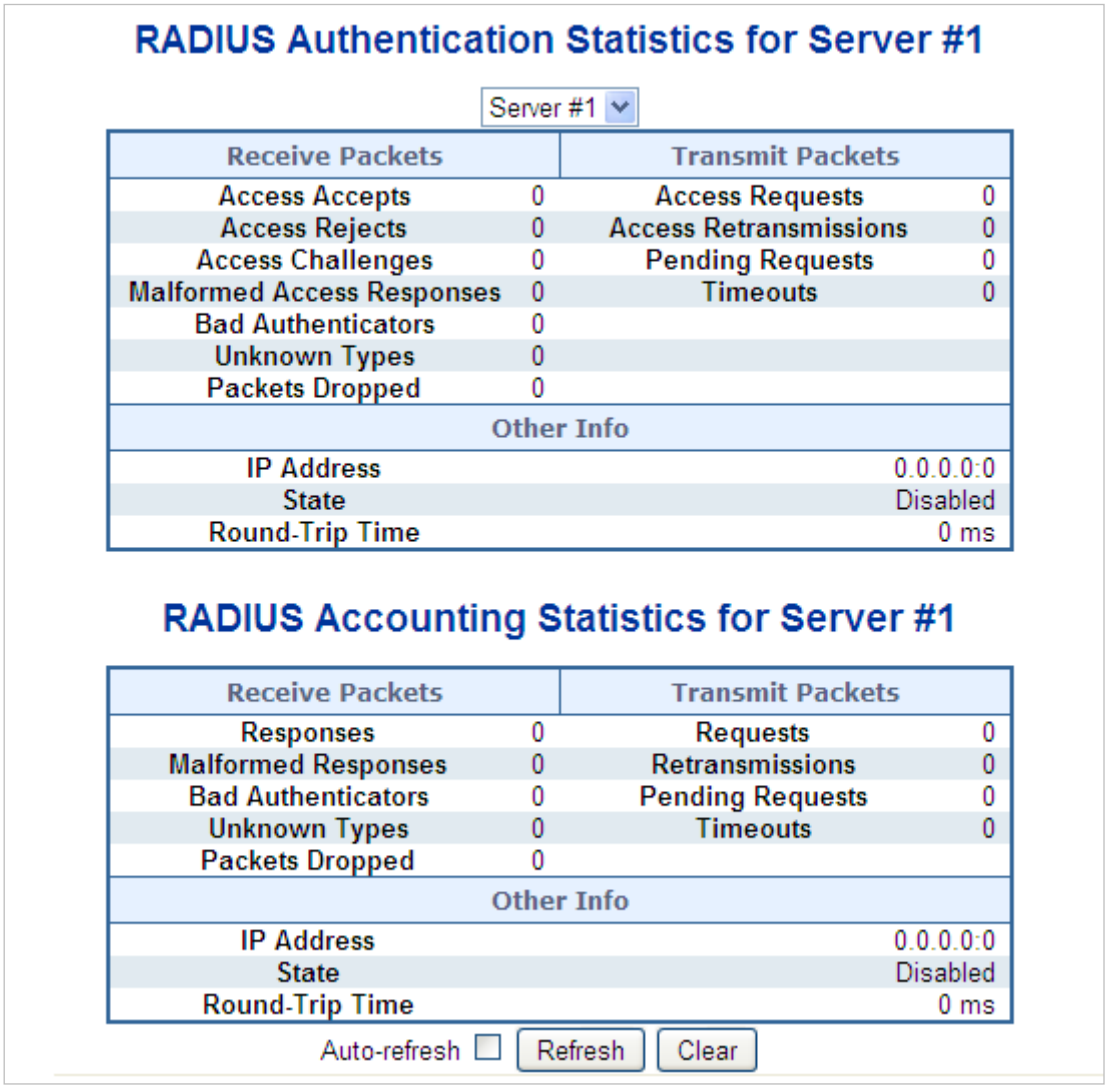
Object	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
Status	The current state of the server. This field takes one of the following values: **Disabled**: 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 or accounting attempts. **Dead (X seconds left)**: Access or 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

- Click **Refresh** to refresh the page immediately.
- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.

RADIUS details

The RADIUS Authentication Statistics for Server overview page provides detailed statistics for a particular RADIUS server.



The page includes the following fields:

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 back end servers to show details for each.

Object	Description			
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 from the server on the authentication port and dropped for some other reason.
	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 has yet to be round-trip communication with the server.

RADIUS accounting statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server check box to switch between the back end servers to show details for each.

<table>
<tr><th>Object</th><th>Description</th></tr>
<tr><td>Packet Counters</td><td>RADIUS accounting server packet counter. There are five receive and four transmit counters.
<table>
<tr><th>Direction</th><th>Name</th><th>RFC4670 Name</th><th>Description</th></tr>
<tr><td>Rx</td><td>Responses</td><td>radiusAccClientExtResponses</td><td>The number of RADIUS packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td>Malformed Responses</td><td>radiusAccClientExtMalformedResponses</td><td>The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or or unknown types are not included as malformed access responses.</td></tr>
<tr><td>Rx</td><td>Bad Authenticators</td><td>radiusAcctClientExtBadAuthenticators</td><td>The number of RADIUS packets containing invalid authenticators received from the server.</td></tr>
<tr><td>Rx</td><td>Unknown Types</td><td>radiusAccClientExtUnknownTypes</td><td>The number of RADIUS packets of unknown types that were received from the server on the accounting port.</td></tr>
<tr><td>Rx</td><td>Packets Dropped</td><td>radiusAccClientExtPacketsDropped</td><td>The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.</td></tr>
<tr><td>Tx</td><td>Requests</td><td>radiusAccClientExtRequests</td><td>The number of RADIUS packets sent to the server. This does not include retransmissions.</td></tr>
<tr><td>Tx</td><td>Retransmissions</td><td>radiusAccClientExtRetransmissions</td><td>The number of RADIUS packets retransmitted to the RADIUS accounting server.</td></tr>
<tr><td>Tx</td><td>Pending Requests</td><td>radiusAccClientExtPendingRequests</td><td>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.</td></tr>
</table></td></tr>
</table>

	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 has yet to be round-trip communication with the server.

Buttons

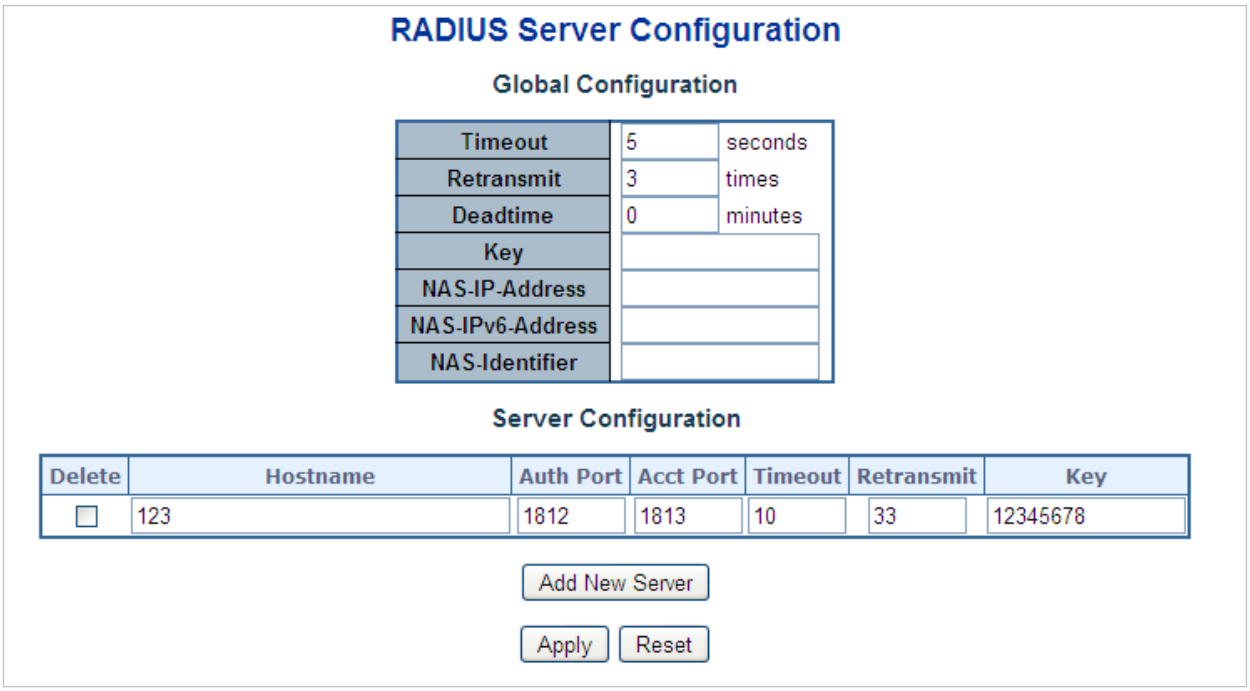
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

- Click **Clear** to clear the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

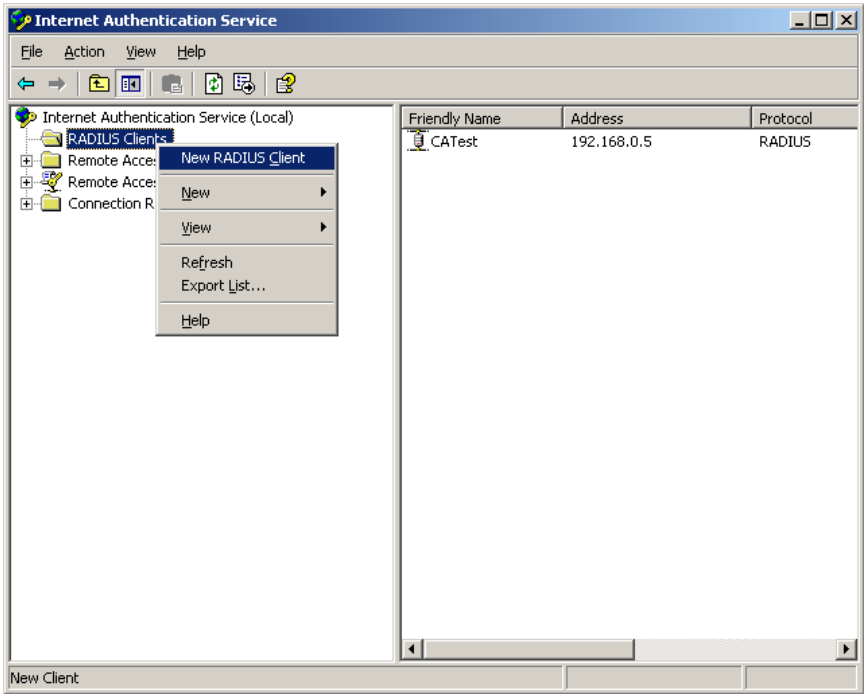
Windows platform RADIUS server configuration

Set up the RADIUS server and assign the client IP address to the managed switch (in this case, the field in the default IP address of the managed switch with 192.168.0.100). Ensure that the shared secret key is as same as the one you had set at the managed switch's 802.1x system configuration (12345678 in this case).

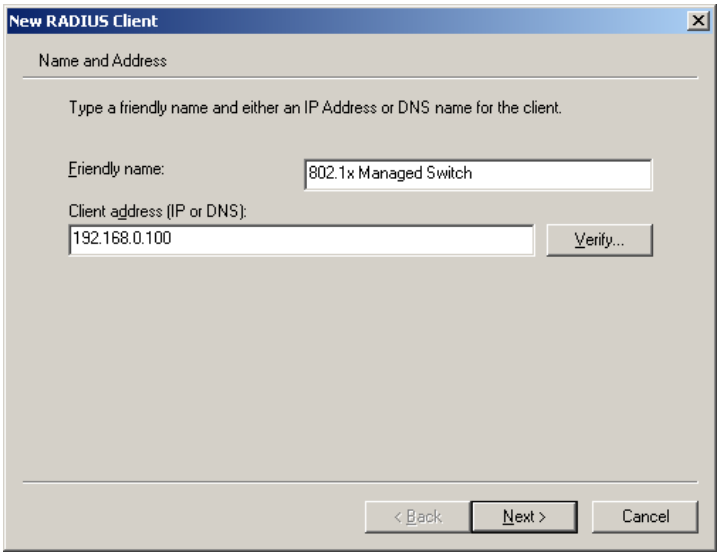
1. Configure the IP Address of remote RADIUS server and secret key.



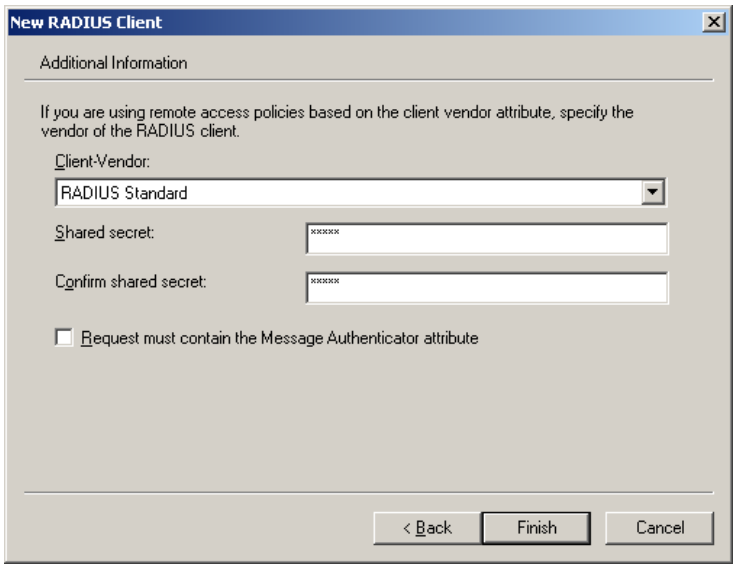
2. Click **New RADIUS Client** on the Windows 2003 server.



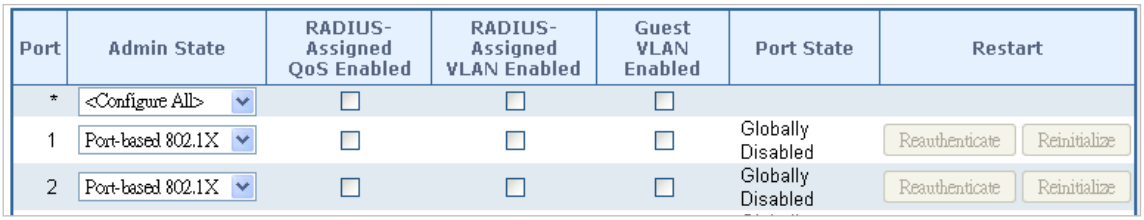
3. Assign the client IP address to the managed switch.



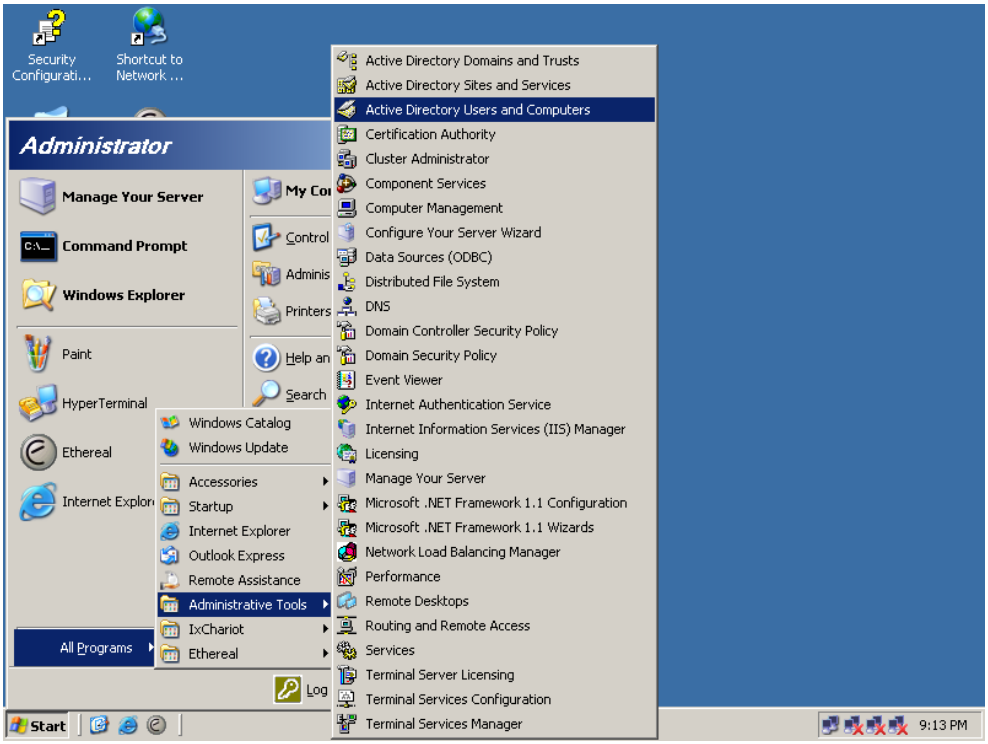
4. The shared secret key should be as same as the key configured on the managed switch.



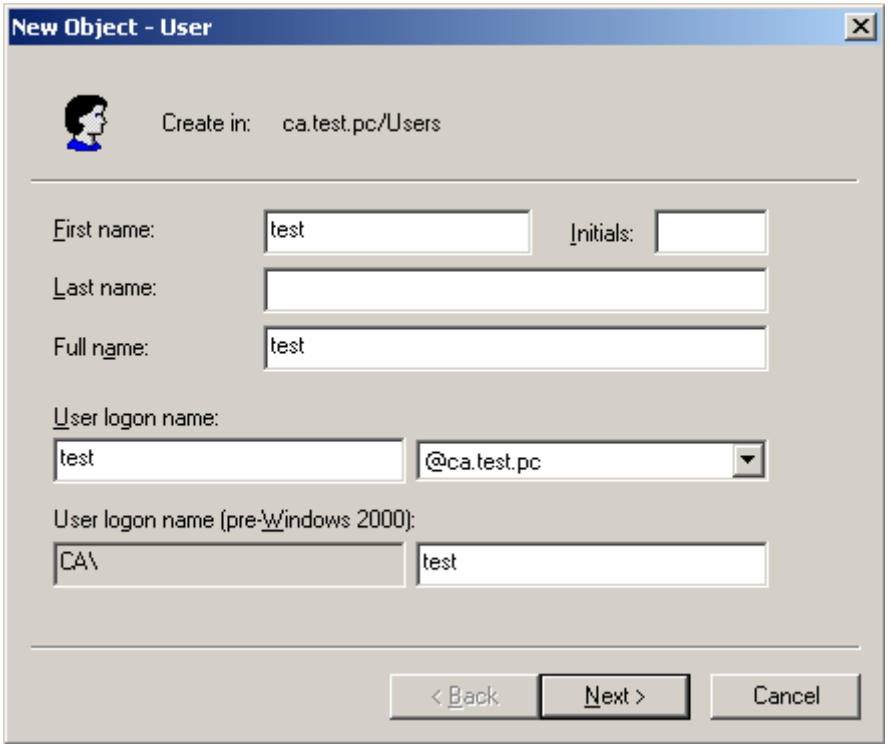
5. Configure ports attribute of 802.1X, the same as “802.1X Port Configuration.”

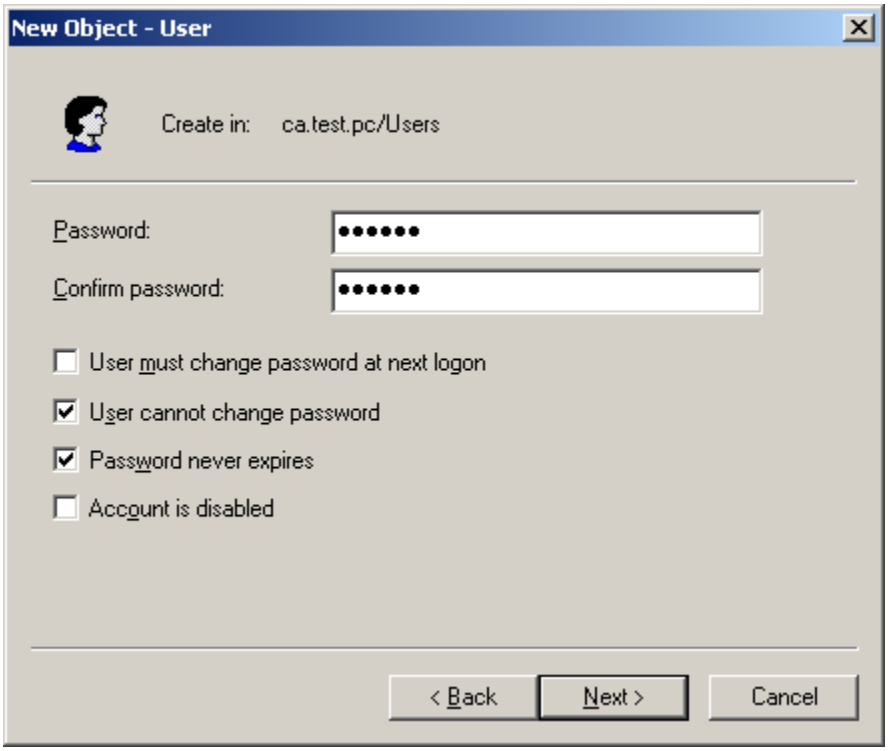


6. Create user data. The establishment of the user data needs to be created on the Radius Server PC. For example, select **Active Directory Users and Computers** and create legal user data (Windows Server 2003).



7. Right-click a user that you created and then type in properties and configure settings.





Note: Set the Port Authenticate Status to “Force Authorized” if the port is connected to the RADIUS server or the port is an uplink port that is connected to another switch. Otherwise, the switch might not be able to access the RADIUS server after the 802.1X starts to work.

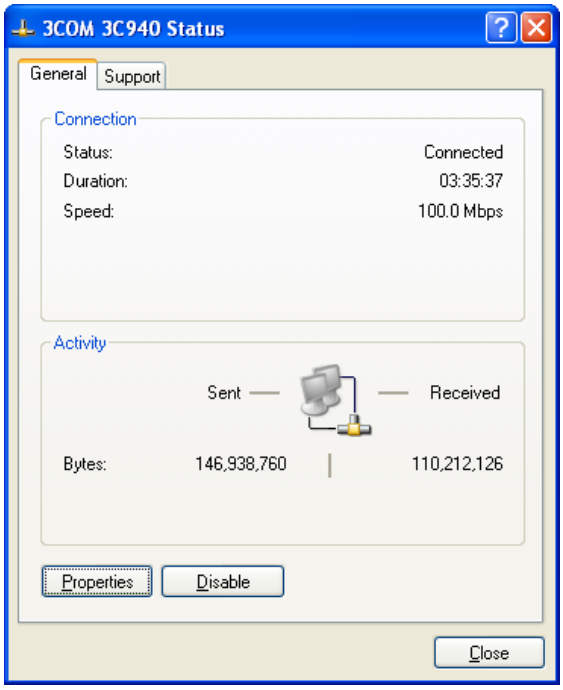
802.1X client configuration

Windows XP has native support for 802.1X. The following procedures show how to configure 802.1X Authentication in Windows XP.

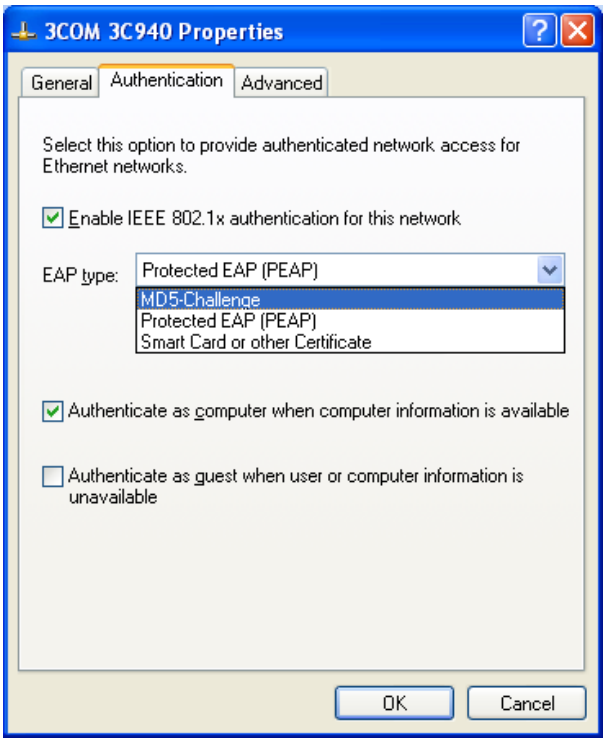
Please note that if you want to change the 802.1x authentication type of a wireless client, (i.e., switch to EAP-TLS from EAP-MD5), you must remove the current existing wireless network from your preferred connection first, and add it in again.

Configuration sample: EAP-MD5 authentication

1. Go to **Start** > **Control Panel**, and then double-click on **Network Connections**.
2. Right-click on the **Local Network Connection**.
3. Click **Properties** to open up the Properties setting window.

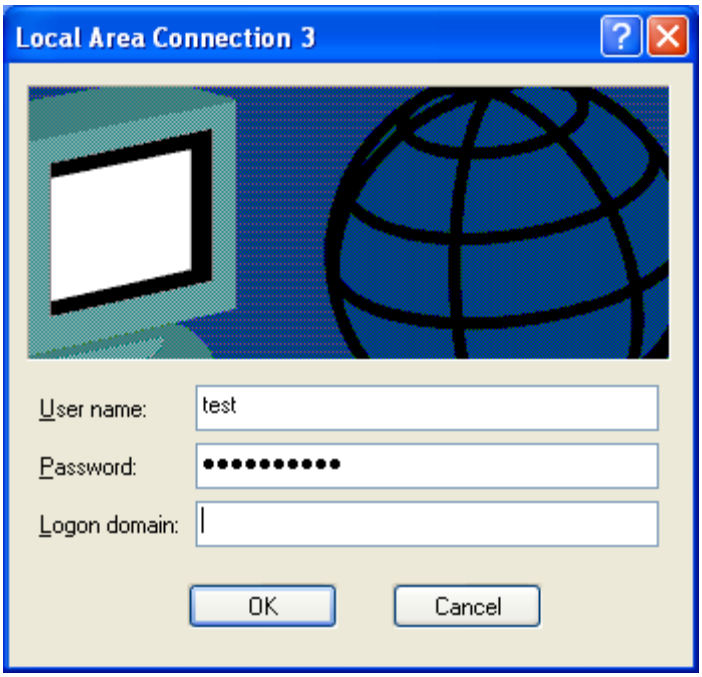


4. Click the **Authentication** tab.
5. Select **Enable network access control using IEEE 802.1X** to enable 802.1x authentication.
6. Select **MD-5 Challenge** from the drop-down list box for EAP type.



7. Click **OK**.
8. When the client has associated with the managed switch, a user authentication notice appears in the system tray. Click on the notice to continue.

9. Type the user name, password and the logon domain that your account belongs to.
10. Click **OK** to complete the validation process.



Security

This section describes how to control access to the managed switch, including user access and management control.

The Security page contains the following main topics:

- Port Limit Control
- Access Management
- HTTPs / SSH
- DHCP Snooping
- IP Source Guard
- ARP Inspection

Port limit control

The Port Limit Control Configuration 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 port security module that manages MAC addresses learned on the port. The limit control configuration consists of two sections, a system- and a port-wide.

The page includes the following fields:

System configuration

Object	Description
Mode	Indicates if Limit Control is globally enabled or disabled on the switchstack. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.
Aging Enabled	If this check box is selected, secured MAC addresses are subject to aging as discussed under Aging Period.
Aging Period	If Aging Enabled is selected, 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.

Object	Description
	To understand why aging may be required, consider the following scenario: Suppose an end-host is connected to a third 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, select **Aging Enabled**. 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 these 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 and a number of columns, which are:

Object	Description
Port	The port number for which the configuration below applies.
Mode	Enable/disable Limit Control on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Note 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 switch 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 the 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 are seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit is exceeded. **Shutdown**: If Limit + 1 MAC addresses are seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port and no new addresses will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1. Boot the stack or elect a new master switch. 2. Disable and re-enable Limit Control on the port or the switch. 3. Click the **Reopen** button. **Trap & Shutdown**: If Limit + 1 MAC addresses are 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.

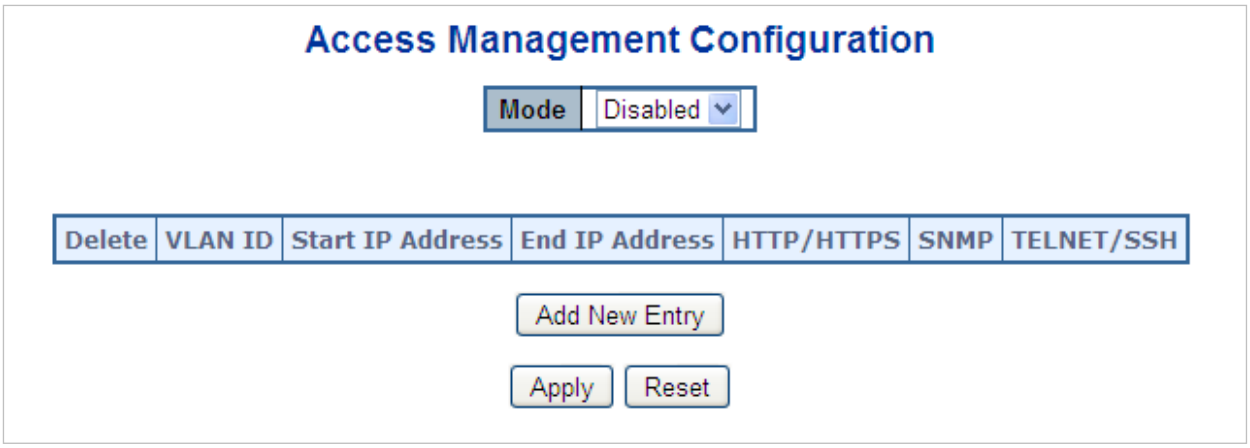
Object	Description
	Ready: The limit is not yet reached. This can be shown for all actions. **Limit Reached**: Indicates that the limit is reached on this port. This state can only be shown if Action is set to **None** or **Trap**. **Shutdown**: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to **Shutdown** or **Trap & Shutdown**.
Re-open Button	If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to **Shutdown** in the Action section. **Note**: Clicking the reopen button causes the page to be refreshed, resulting in the loss of non-committed changes.

Buttons

- Click **Save** to save changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Refresh** to refresh the page. Note that non-committed changes are lost.

Access management

Configure the access management table on the Access Management Configuration page. The maximum entry number is 16. If the application's type match any one of the access management entries, it will allow access to the switch.



The page includes the following fields:

Object	Description
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 apply .
VLAN ID	Indicates the VLAN ID for the access management entry.
Start IP address	Indicates the start IP address for the access management entry.

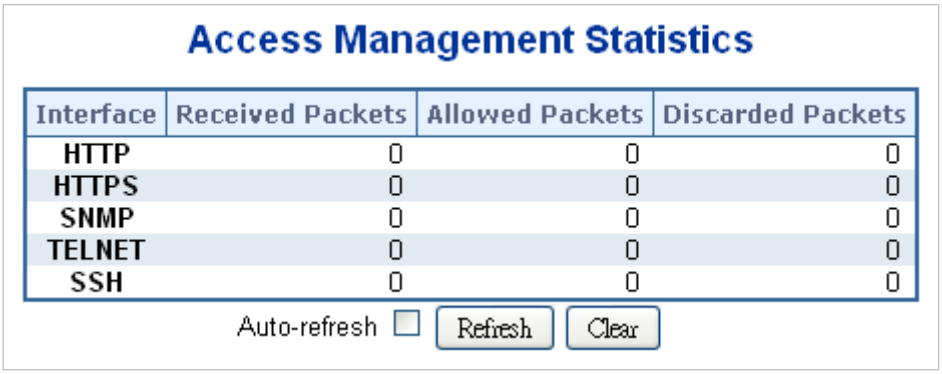
Object	Description
End IP address	Indicates the end IP address for the access management entry.
HTTP/HTTPS	Indicates the host can access the switch from the HTTP/HTTPS interface and that the host IP address matched the entry.
SNMP	Indicates the host can access the switch from the SNMP interface and that the host IP address matched the entry.
TELNET/SSH	Indicates the host can access the switch from the TELNET/SSH interface and that the host IP address matched the entry.

Buttons

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

Access management statistics

The Access Management Statistics page provides statistics for access management.



The page includes the following fields:

Object	Description
Interface	The interface that allowed the remote host can access the switch.
Receive Packets	The received packets number from the interface under access management mode is enabled.
Allow Packets	The allowed packets number from the interface under access management mode is enabled.
Discard Packets	The discarded packets number from the interface under access management mode is enabled.

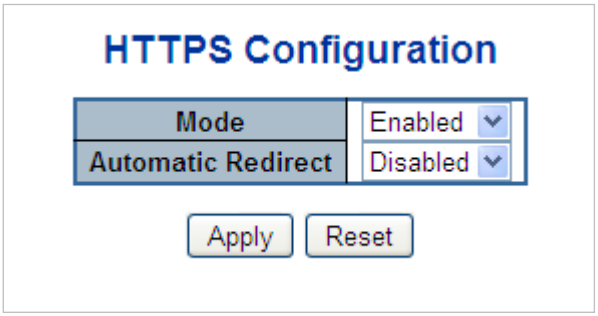
Buttons

- Click **Refresh** to refresh the page immediately.
- Click **Auto-refresh** to to refresh the page automatically. Automatic refresh occurs every three seconds.

- Click **Clear** to clear all statistics.

HTTPs

Configure HTTPS on the HTTPS Configuration page.



The page includes the following fields:

Object	Description
Mode	Indicates the HTTPS mode operation. When the current connection is HTTPS, applying the HTTPS disabled mode operation automatically redirects the web browser to an HTTP connection. Selections include: **Enabled**: Enable HTTPS mode operation. **Disabled**: Disable HTTPS mode operation.
Automatic Redirect	Indicates the HTTPS redirect mode operation. It is only significant if HTTPS mode **Enabled** is selected. It automatically redirects the web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled or redirects web browser to an HTTP connection when both are disabled. Selections include: **Enabled**: Enable HTTPS redirect mode operation. **Disabled**: Disable HTTPS redirect mode operation.

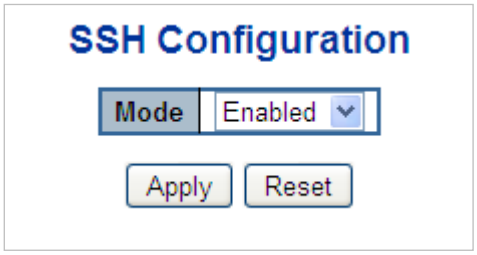
Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SSH

Configure SSH on the SSH Configuration page. This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other 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.



The page includes the following fields:

Object	Description
Mode	Indicates the SSH mode operation. Selections include: **Enabled**: Enable SSH mode operation. **Disabled**: Disable SSH mode operation..

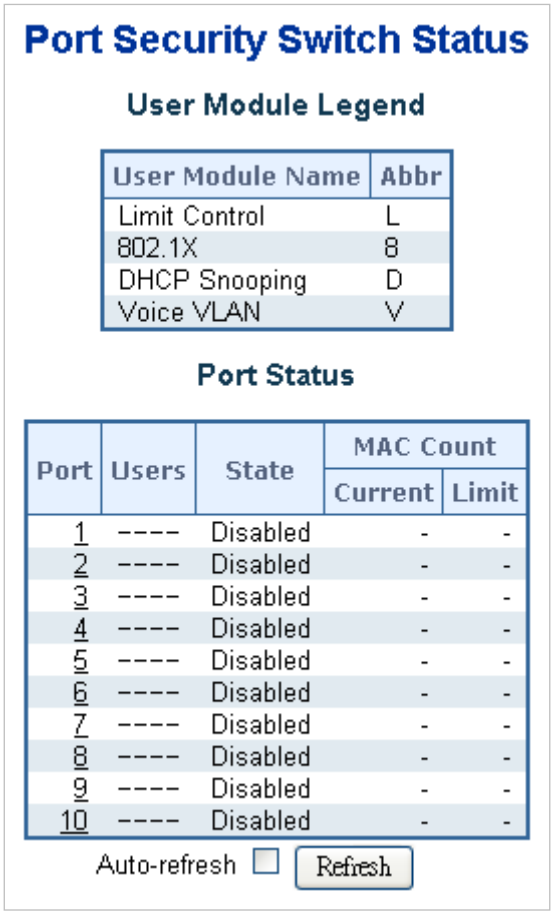
Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port security status

The Port Security Status page shows the Port Security status. Port security is a module with no direct configuration. Configuration comes indirectly from other 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.



The page includes the following fields:

User module legend

The legend shows all user modules that may request Port Security services.

Object	Description
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 switch and a number of columns, which are:

Object	Description
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 if that module has enabled Port Security. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter has enabled port security.
State	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.

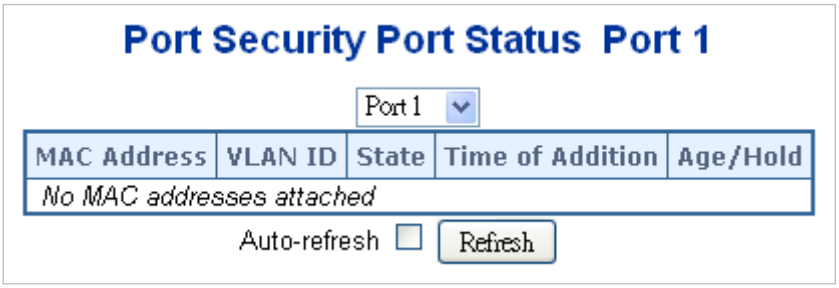
Object	Description
	Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. **Limit Reached**: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached 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

- Click **Refresh** to refresh the page immediately.
- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.

Port security detail

The Port Security Port Status 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 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 page includes the following fields:

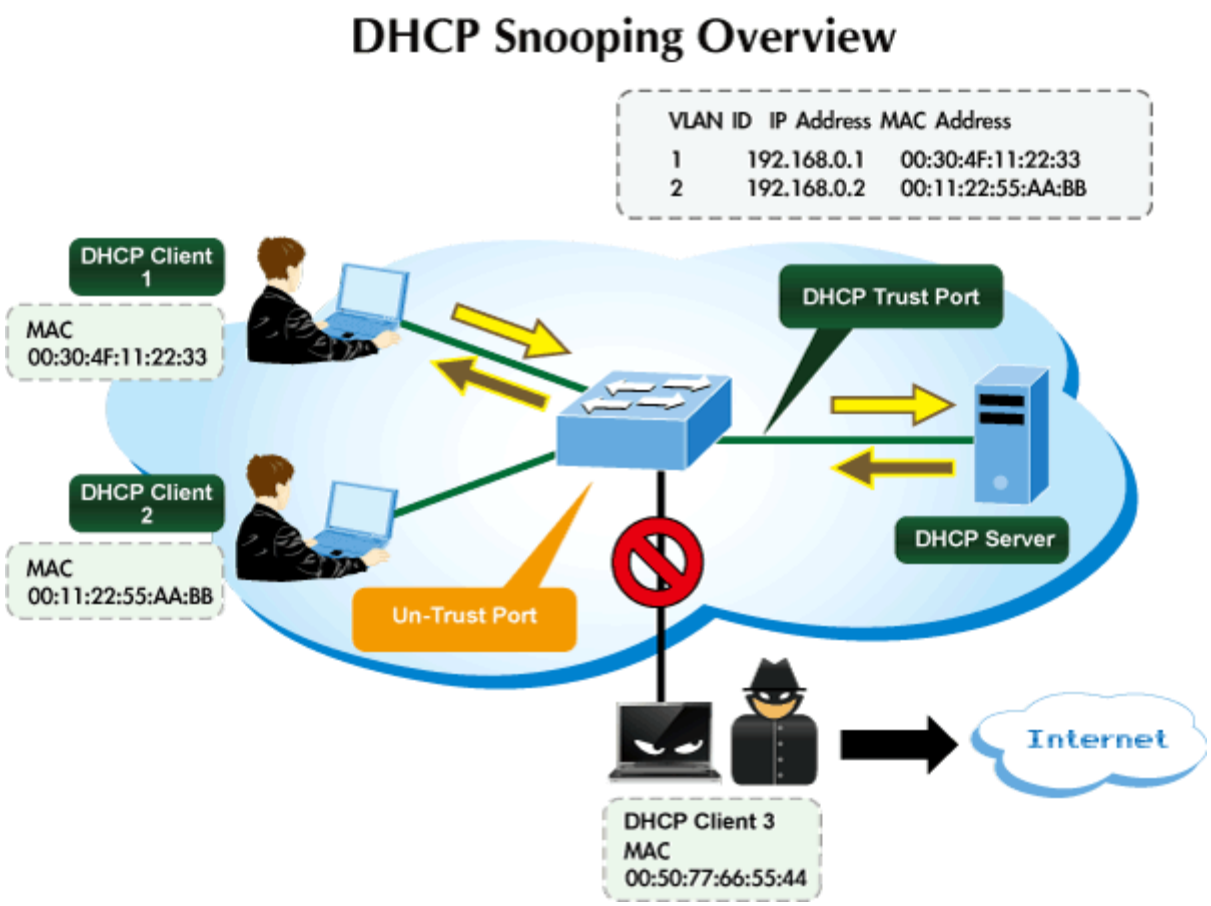
Object	Description
MAC Address & VLAN ID	The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.
State	Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will 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

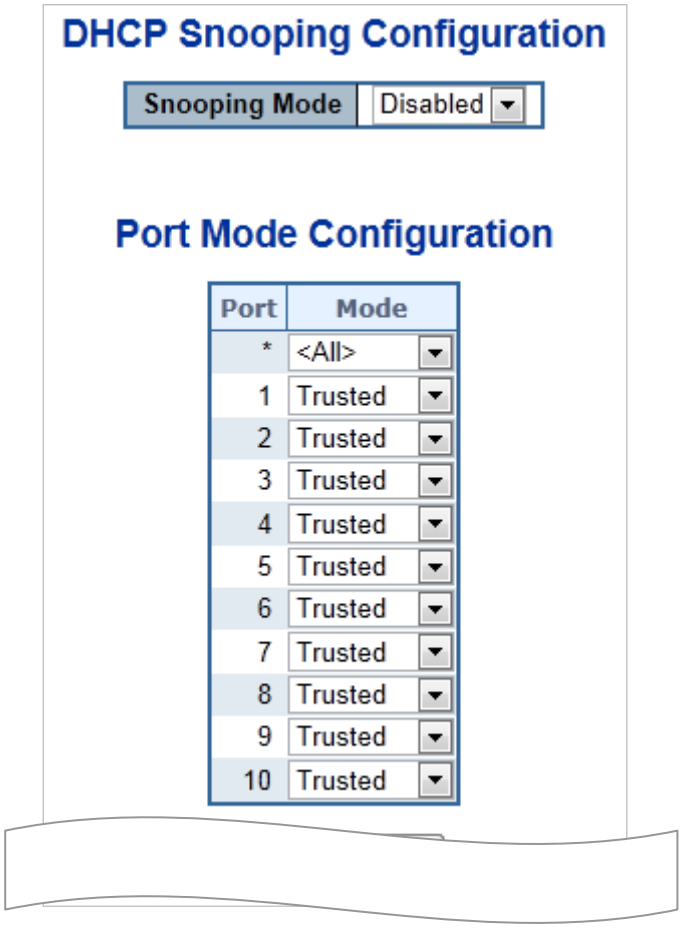
- Click **Refresh** to refresh the page immediately.
- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.

DHCP snooping

DHCP snooping is used to block intruders on the untrusted ports of DUT when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.



Configure DHCP Snooping on the DHCP Snooping Configuration page.



The page includes the following fields:

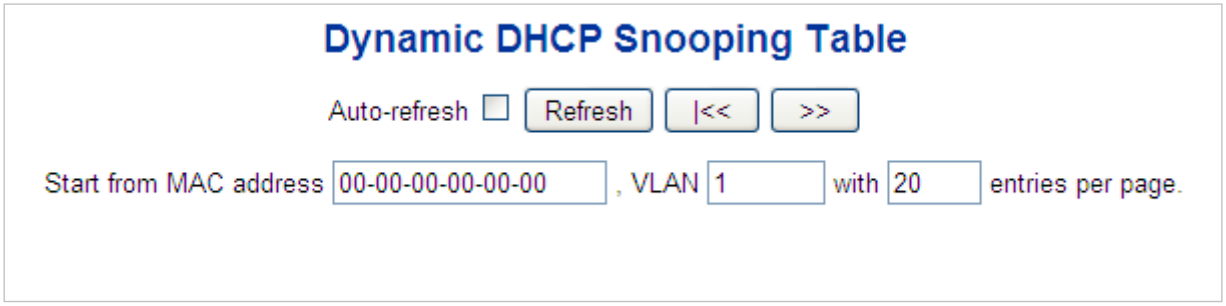
Object	Description
Snooping Mode	Indicates the DHCP snooping mode operation. Possible modes are: **Enabled**: Enable DHCP snooping mode operation. When the DHCP snooping mode operation is enabled, the request DHCP messages will be forwarded to trusted ports and only allow reply packets from trusted ports. **Disabled**: Disable the DHCP snooping mode operation.
Port Mode Configuration	Indicates the DHCP snooping port mode. Possible port modes are: **Trusted**: Configures the port as trusted sources of the DHCP message. **Untrusted**: Configures the port as untrusted sources of the DHCP message. **All**: All ports will have one specific setting.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Snooping table

The Dynamic DHCP Snooping Table page displays the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients that 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.



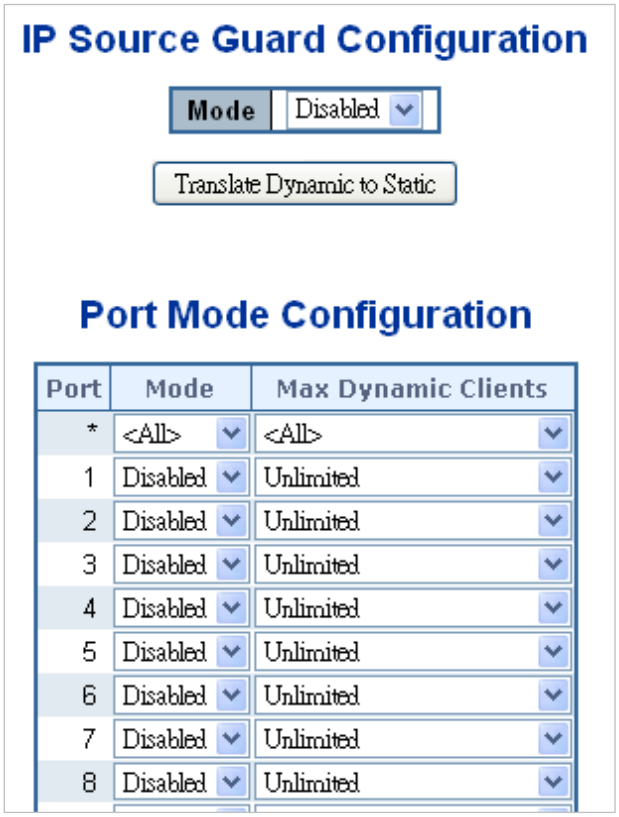
Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **>>** to use the last entry of the currently displayed table as a basis for the next lookup. “No more entries” is shown in the table.
- Click **I<<** to start over.

IP source guard configuration

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. The IP Source Guard Configuration page provides IP Source Guard-related configuration data.



The page includes the following fields:

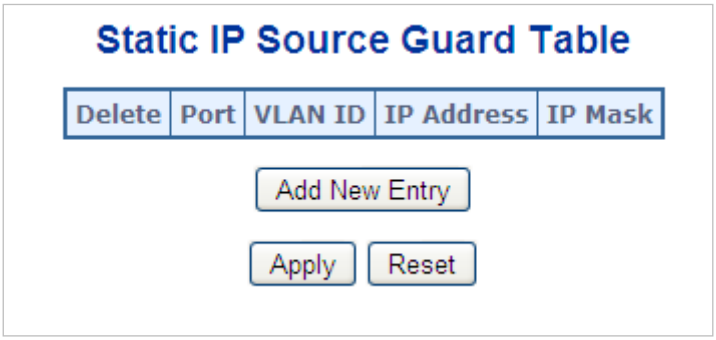
Object	Description
Mode of IP Source Guard Configuration	Enable/disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
Port Mode Configuration	Specify on which ports IP Source Guard is enabled. Only when both Global Mode and Port Mode on a given port are enabled will IP Source Guard be enabled on this port.
Max Dynamic Clients	Specify the maximum number of dynamic clients that can be learned on given ports. This value can be 0, 1, 2, and unlimited. If the port mode is enabled and the value of max dynamic client is equal 0, it only allows the forwarding of IP packets that are matched in static entries on the specific port.

Buttons

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

IP source guard static table

The Static IP Source Guard Table page appears as below:



The page includes the following fields:

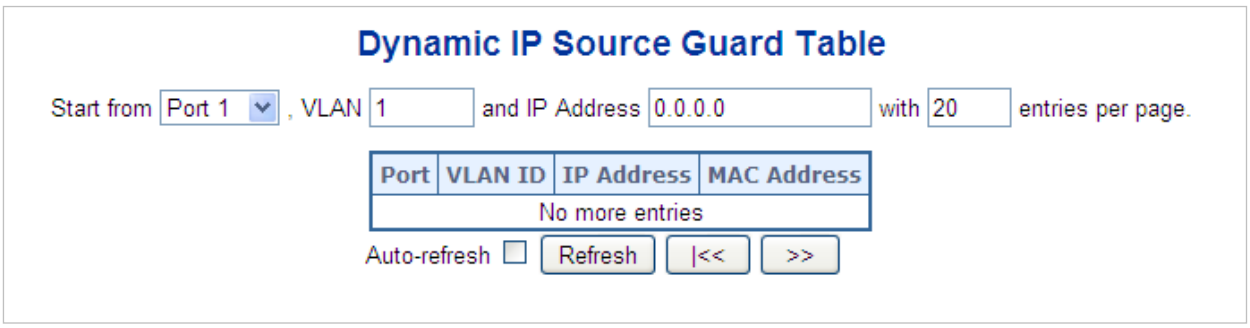
Object	Description
Delete	Select to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings.
VLAN ID	The VLAN ID for the settings.
IP Address	Allowed Source IP address.
MAC Address	Allowed Source MAC address.

Buttons

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

Dynamic IP source guard table

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 IP mask.



Navigating the dynamic IP source guard table

Each page shows up to 99 entries from the Dynamic IP source guard table, selected through the "entries per page" input field (default is 20). When first visited, the web page will show the first 20 entries from the beginning of the table. The first entry displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the table.

The **Start from** port address, **IP Address**, and **VLAN** input fields allow the user to select the starting point in the table. Clicking the **Refresh** button updates the displayed table starting from that or the closest next Dynamic IP source guard table match.

In addition, the two input fields will, after clicking the **Refresh** button, 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/IP 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 **I<<** button to start over.

The page includes the following fields:

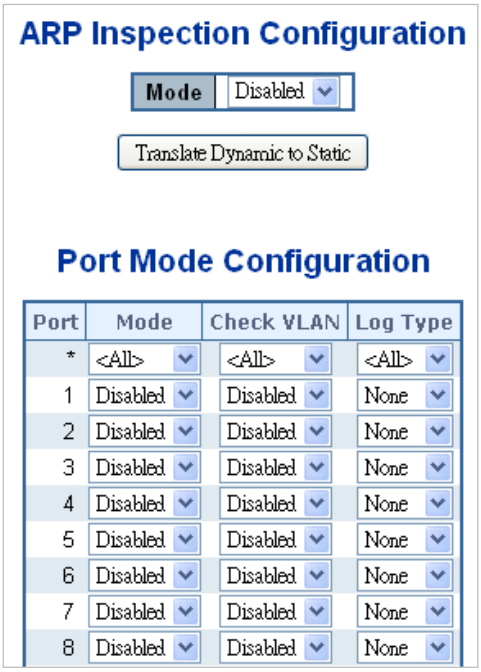
Object	Description
Port	The port number for which the status applies. Click the port number to see the status for this particular port.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
IP Address	The IP address of the entry.

Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the displayed table starting from the **MAC address** and **VLAN** input fields.
- Click **Clear** to flush all dynamic entries.
- Click **I<<** to update the table starting from the first entry in the MAC table (i.e., the entry with the lowest VLAN ID and MAC address).
- Click **>>** to update the table, starting with the entry after the last entry currently displayed.

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 DUT. The ARP Inspection Configuration page provides ARP Inspection related configuration.



The page includes the following fields:

Object	Description
Mode of ARP Inspection Configuration	Enable/disable the Global ARP Inspection.
Port Mode Configuration	Specify the ports on which ARP Inspection is enabled. Only when both Global Mode and Port Mode on a given port are enabled will ARP Inspection be enabled on this port. Possible modes are: **Enabled**: Enable ARP Inspection operation. **Disabled**: Disable ARP Inspection operation. To inspect the VLAN configuration, select **Enabled** under Check VLAN. The default setting of Check VLAN is disabled. When Check VLAN is set to **Disabled**, the log type of ARP Inspection refers to the port setting. When Check VLAN is set to **Enabled**, the log type of ARP Inspection will refer to the VLAN setting. Possible modes are: **Enabled**: Enable check VLAN operation. **Disabled**: Disable check VLAN operation. When the Global Mode and Port Mode on a given port are set to **Enabled**, and Check VLAN is set to **Disabled**, the log type of ARP Inspection will refer to the port setting. There are four log types which are: **None**: Log nothing. **Deny**: Log denied entries. **Permit**: Log permitted entries. **ALL**: Log all entries.

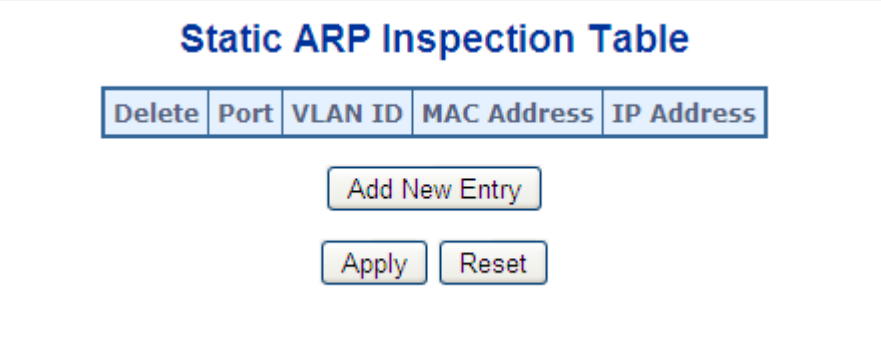
Buttons

- Click **Translate Dynamic to Static** to translate all dynamic entries to static entries.
- Click **Apply** to apply changes.

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

ARP inspection static table

The Static ARP Inspection Table page provides Static ARP Inspection data.



The page includes the following fields:

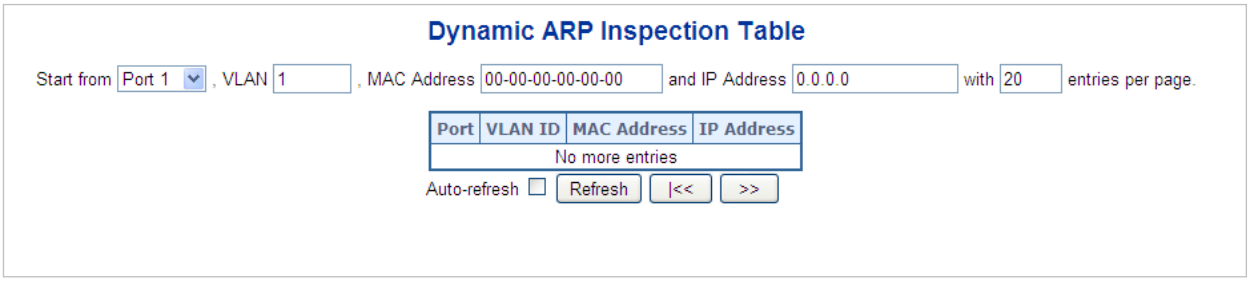
Object	Description
Delete	Select to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings.
VLAN ID	The VLAN ID for the settings.
MAC Address	Allowed Source MAC address in ARP request packets.
IP Address	Allowed Source IP address in ARP request packets.

Buttons

- Click **Add New Entry** to add a new entry to the Static ARP inspection table.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Dynamic ARP inspection 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, selected through the "entries per page" input field (default is 20). When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP inspection table. The first entry displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the table.

The **Start from** port address, **MAC Address**, **IP Address** and **VLAN** input fields allow the user to select the starting point in the table. Clicking the **Refresh** button updates the displayed table starting from that or the closest next Dynamic ARP inspection match.

In addition, the two input fields will, after clicking the **Refresh** button, 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 **I<<** button to start over.

The page includes the following fields:

Object	Description
Port	The port number for which the status applies. Click the port number to see the status for this particular port.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
IP Address	The IP address of the entry.

Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the displayed table starting from the **MAC address** and **VLAN** input fields.
- Click **Clear** to flush all dynamic entries.
- Click **I<<** to update the table starting from the first entry in the MAC table (i.e., the entry with the lowest VLAN ID and MAC address).
- Click **>>** to update the table, starting with the entry after the last entry currently displayed.

MAC address table

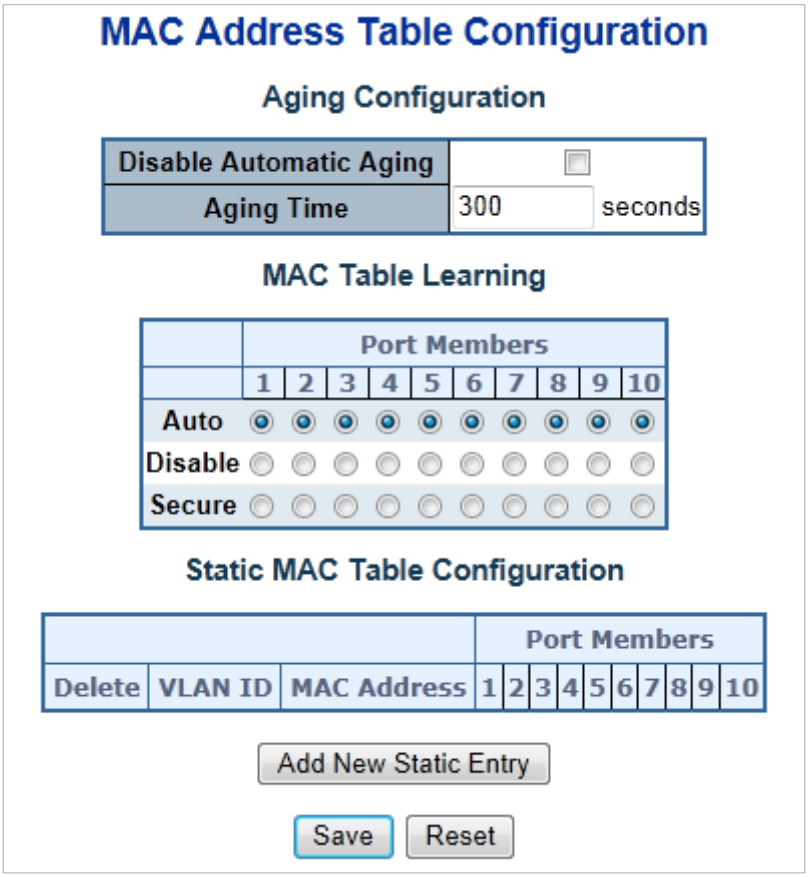
Switching of frames is based upon the DMAC address contained in the frame. The managed switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The 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) that shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MAC table configuration

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



The page includes the following fields:

Aging configuration

Object	Description
Disable Automatic Aging	Enables/disables the automatic aging of dynamic entries
Aging Time	The time after which a learned entry is discarded. By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging. (Range: 10-10000000 seconds; Default: 300 seconds)

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.

Object	Description
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 MAC table is sorted first by VLAN ID and then by MAC address.

Object	Description
Delete	Select 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. Select or deselect 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

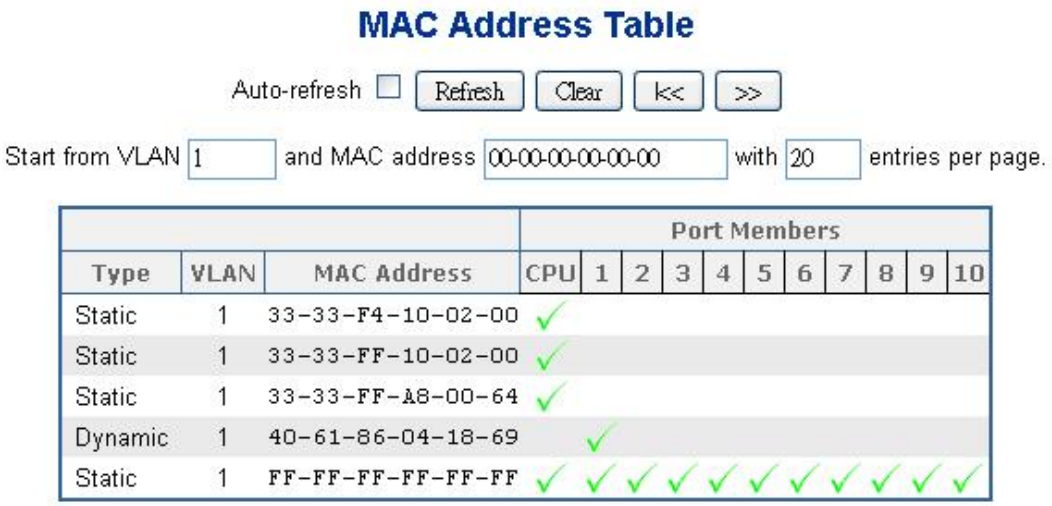
- Click **Save** to save changes.

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

MAC address table status

Dynamic 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 99 entries from the MAC table, selected through the "entries per page" input field (default is 20). When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first entry 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 updates the displayed table starting from that or the closest next MAC Table match.

In addition, the two input fields will, after clicking the **Refresh** button, assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **>>** button uses 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 **I<<** button to start over.

The page includes the following fields:

Object	Description
Type	Indicates if the entry is a static or dynamic entry.
VLAN	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port Members	The ports that are members of the entry.

Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the displayed table starting from the **MAC address** and **VLAN** input fields.
- Click **Clear** to flush all dynamic entries.
- Click **I<<** to update the table starting from the first entry in the MAC table (i.e., the entry with the lowest VLAN ID and MAC address).
- Click **>>** to update the table, starting with the entry after the last entry currently displayed.

LLDP

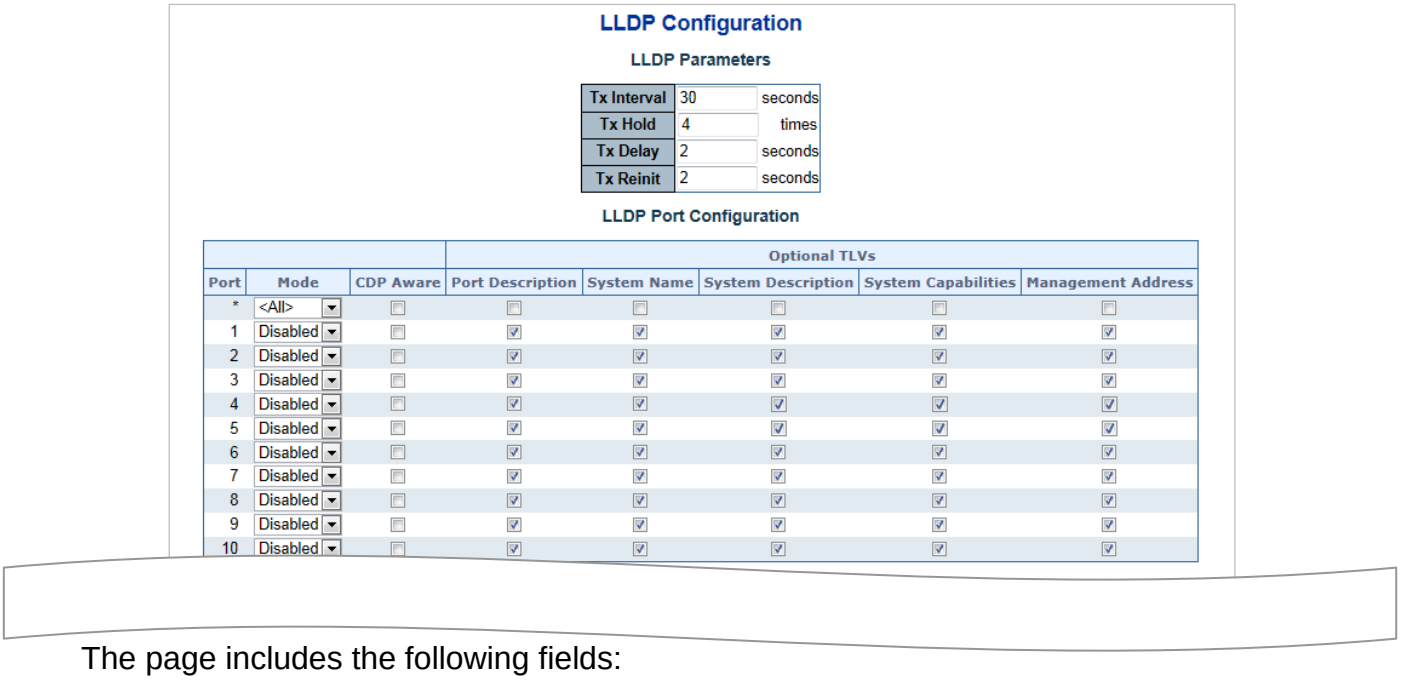
Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities, and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol – Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP (VoIP) phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

LLDP configuration

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



The page includes the following fields:

LLDP parameters

Object	Description
Tx Interval	The switch is periodically transmitting 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. Default: **30** seconds This attribute must comply with the following rule: (Transmission Interval * Hold Time Multiplier) ≤65536, and Transmission Interval >= (4 * Delay Interval)
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. TTL in seconds is based on the following rule: (Transmission Interval * Holdtime Multiplier) ≤ 65536. Therefore, the default TTL is 4*30 = 120 seconds.
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. This attribute must comply with the rule: (4 * Delay Interval) ≤Transmission Interval
Tx Reinit	When a port is disabled, LLDP is disabled, or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information is no longer valid. **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 current unit, as reflected by the page header.

Object	Description
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, and 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 neighbours' 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 neighbours 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 Description	Optional TLV: When selected, the "port description" is included in LLDP information transmitted.
System Name	Optional TLV: When selected, the "system name" is included in LLDP information transmitted.
System Description	Optional TLV: When selected, the "system description" is included in LLDP information transmitted.
System Capabilites	Optional TLV: When selected, the "system capability" is included in LLDP information transmitted. The system capabilities identify the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

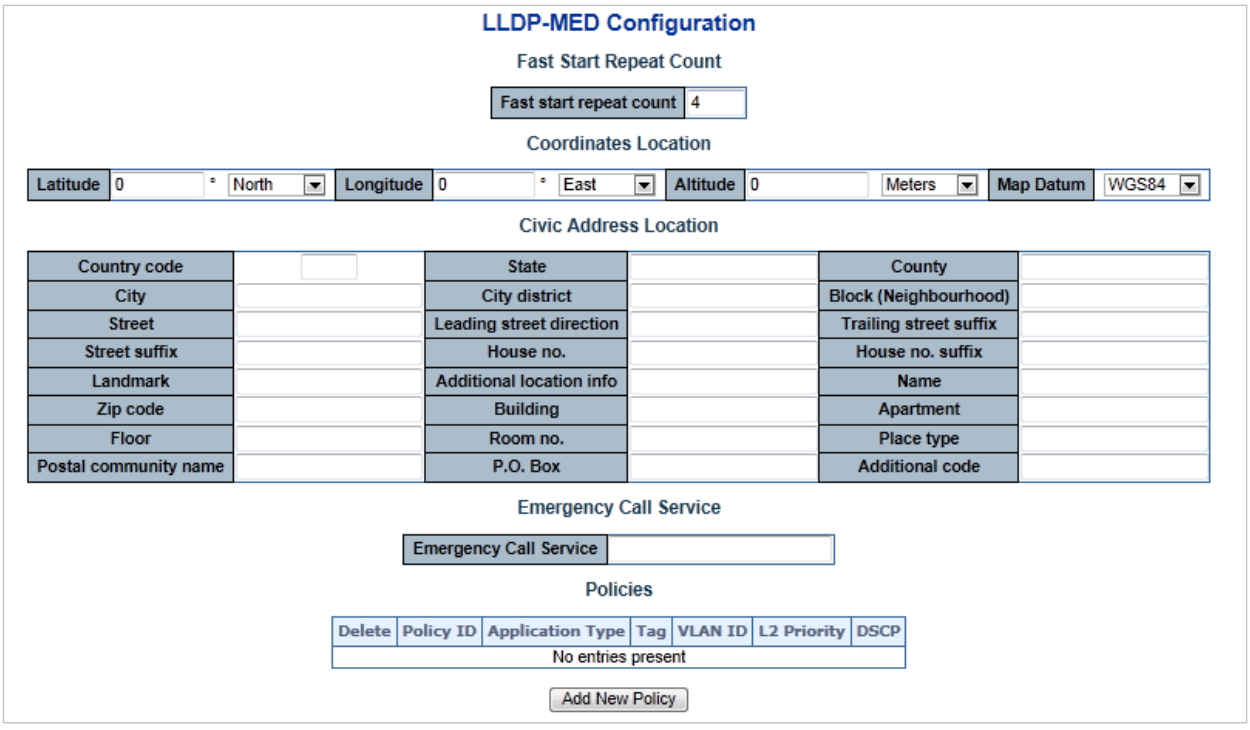
Object	Description
Management Address	Optional TLV: When selected, the "management address" is included in LLDP information transmitted. The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

LLDP-MED configuration

The LLDP-MED Configuration page permits configuration of the LLDP-MED.



The page includes the following fields:

Fast start repeat count

Object	Description
Fast start repeat count	Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (e.g., 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 to 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, we recommend repeating 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 four times, given that four LLDP frames with a one 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

Object	Description
Latitude	**Latitude** SHOULD be normalized to within 0-90° with a maximum of four 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° with a maximum of four 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 four digits. It is possible to select between two altitude types (floors or meters). **Meters**: Representing meters of Altitude defined by the vertical datum specified.

Object	Description
	Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude of 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** used for the coordinates given in this option. **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).

Object	Description
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

Object	Description
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.

Object	Description
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:

- Layer 2 VLAN ID (IEEE 802.1Q-2003)
- Layer 2 priority value (IEEE 802.1D-2004)
- 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:

- Voice
- Guest Voice
- Softphone Voice
- Video Conferencing
- Streaming Video
- 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.

Object	Description
Delete	Select this check box to delete the policy. It will be deleted during the next save.
Policy ID	ID for the policy. This is auto generated and is used when selecting the polices mapped to the specific ports.
Application Type	Intended use of the application types: **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. **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. **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. **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. **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. **Video Conferencing** – For use by dedicated video conferencing equipment and other similar appliances supporting real–time interactive video/audio services. **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. **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.

Object	Description
Tag	**Tag** indicates if 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 behavior 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.

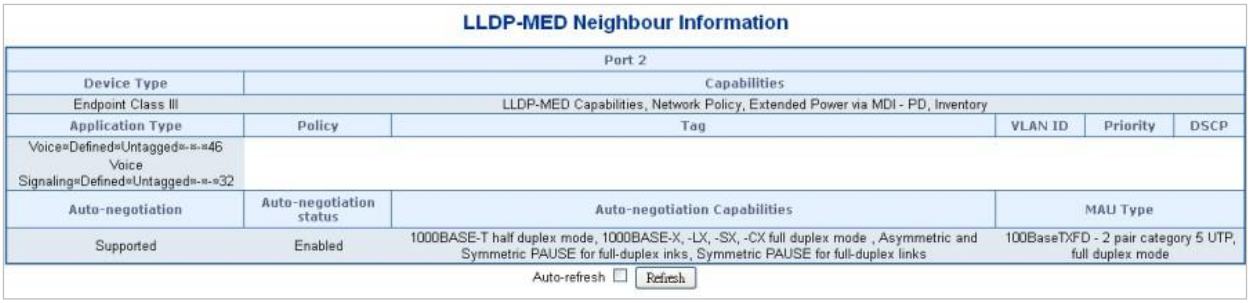
Object	Description
Port	The port number for which the configuration applies.
Policy ID	The set of policies for a given port. The set of policies is selected by selecting the check boxes that correspond to the policies

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

LLDP-MED neighbor

The LLDP-MED Neighbor Information page provides a status overview of all LLDP-MED neighbors. The table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:



LLDP-MED Neighbour Information

Port 2					
Device Type	Capabilities				
Endpoint Class III	LLDP-MED Capabilities, Network Policy, Extended Power via MDI - PD, Inventory				
Application Type	Policy	Tag	VLAN ID	Priority	DSCP
Voice=Defined=Untagged=-=-=46 Voice Signaling=Defined=Untagged=-=-=32					
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities	MAU Type		
Supported	Enabled	1000BASE-T half duplex mode, 1000BASE-X, -LX, -SX, -CX full duplex mode , Asymmetric and Symmetric PAUSE for full-duplex inks, Symmetric PAUSE for full-duplex links	100BaseTXFD - 2 pair category 5 UTP, full duplex mode		

Auto-refresh ☐ Refresh

The page includes the following fields:

Fast start repeat count

Object	Description
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** 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, any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) will 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 but 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)**

Object	Description
	The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities but 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, etc. 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, and inventory management
LLDP-MED Capabilities	LLDP-MED Capabilities describes the neighbor 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 as follows: **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. **Voice Signaling** – For use in network topologies that require a different policy for the voice signaling than for the voice media. **Guest Voice** – Supports 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. **Guest Voice Signaling** – For use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. **Softphone Voice** – For use by softphone applications on typical data-centric devices, such as PCs or laptops. **Video Conferencing** – For use by dedicated video conferencing equipment and other similar appliances supporting real–time interactive video/audio services.

Object	Description
	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. **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 indicating 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 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 by the operational MAU type field value rather than by auto-negotiation.
Auto-negotiation capabilities	**Auto-negotiation Capabilities** shows the link partner's MAC/PHY capabilities.

Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Neighbor

The LLDP Neighbor Information page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected.

The page includes the following fields:

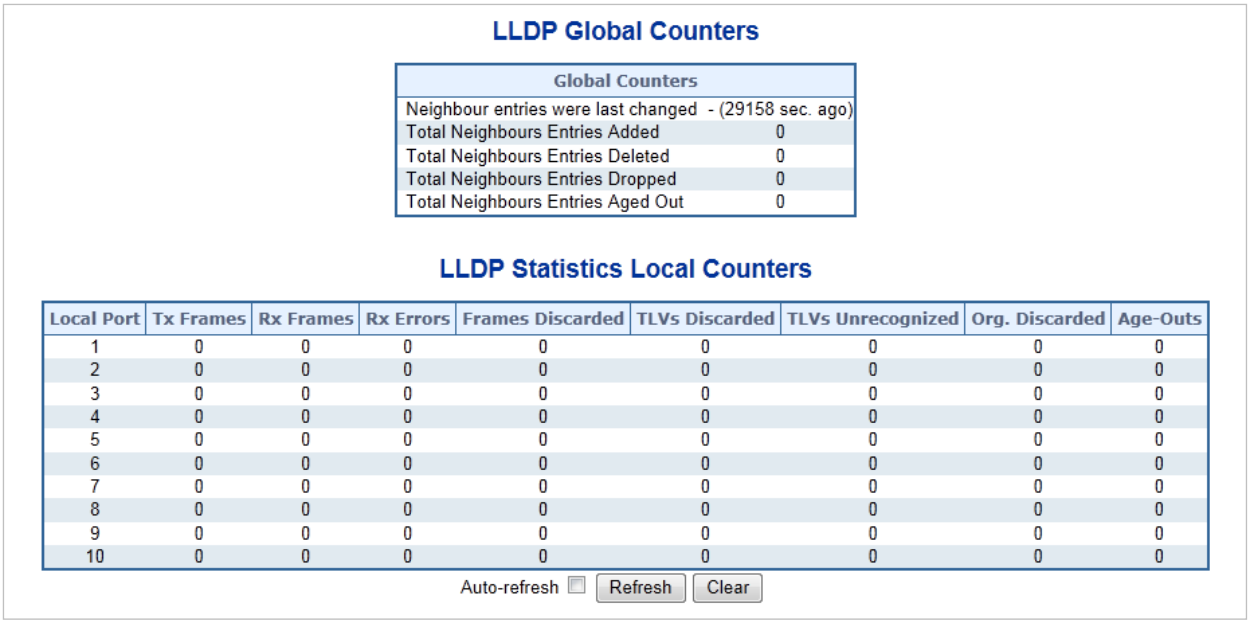
Object	Description
Local Port	The port on which the LLDP frame was received.
Chassis ID	The identification of the neighbor's LLDP frames.
Port ID	The identification of the neighbor port.
Port Description	The port description advertised by the neighbor unit.
System Name	The name advertised by the neighbor unit.
System Capabilities	System Capabilities describes the neighbor 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	The neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could, for instance, hold the neighbor's IP address.

Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Port statistics

The LLDP Global/Statistics Local Counters page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the switch, while local counters refers to counters for the currently selected switch.



The page includes the following fields:

Global counters

Object	Description
Neighbor 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 Neighbors Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbors Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to the entry table being full.
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.

LLDP statistics local counters

The displayed table contains a row for each port. The columns hold the following information:

Object	Description
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 Neighbors" 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 links 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 TLVs received.
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

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear the local counters. All counters (including global counters) are cleared upon reboot.

Network diagnostics

This section provides the physical layer and IP layer network diagnostics tools for troubleshooting. The diagnostic tools are designed for network managers to help them quickly diagnose problems and better service customers.

Use the Diagnostics menu items to display and configure basic administrative details of the managed switch. Under System, the following topics are provided to configure and view the system information:

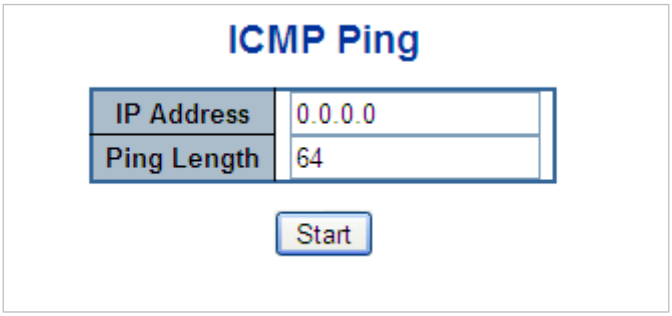
- Ping
- IPv6 Ping

- Remote IP Ping
- Cable Diagnostics

Ping

The ICMP Ping page allows you to issue ICMP ping packets to troubleshoot IP connectivity issues.

After clicking **Start**, five ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.



The page includes the following fields:

Object	Description
IP Address	The destination IP Address.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

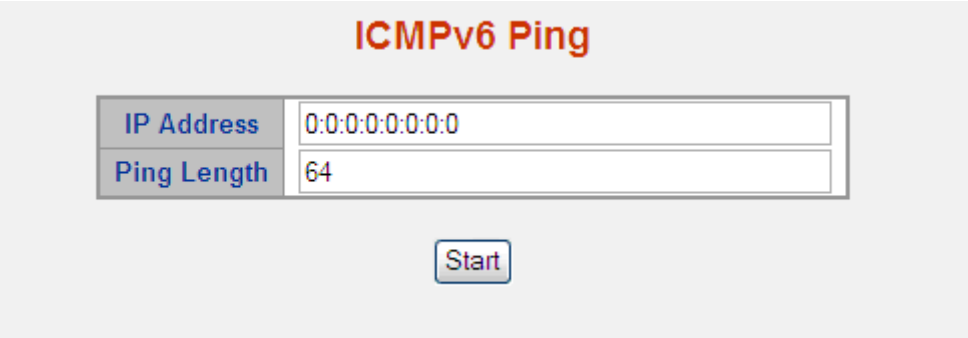
Note: Be sure the target IP address is within the same network subnet of the managed switch, otherwise the correct gateway IP address must be set up.

Buttons

- Click **Start** to transmit ICMP packets.
- Click **New Ping** to re-start diagnostics with ping.

IPv6 ping

The ICMPv6 Ping page allows you to issue ICMPv6 ping packets to troubleshoot IPv6 connectivity issues. After clicking **Start**, five ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.



The page includes the following fields:

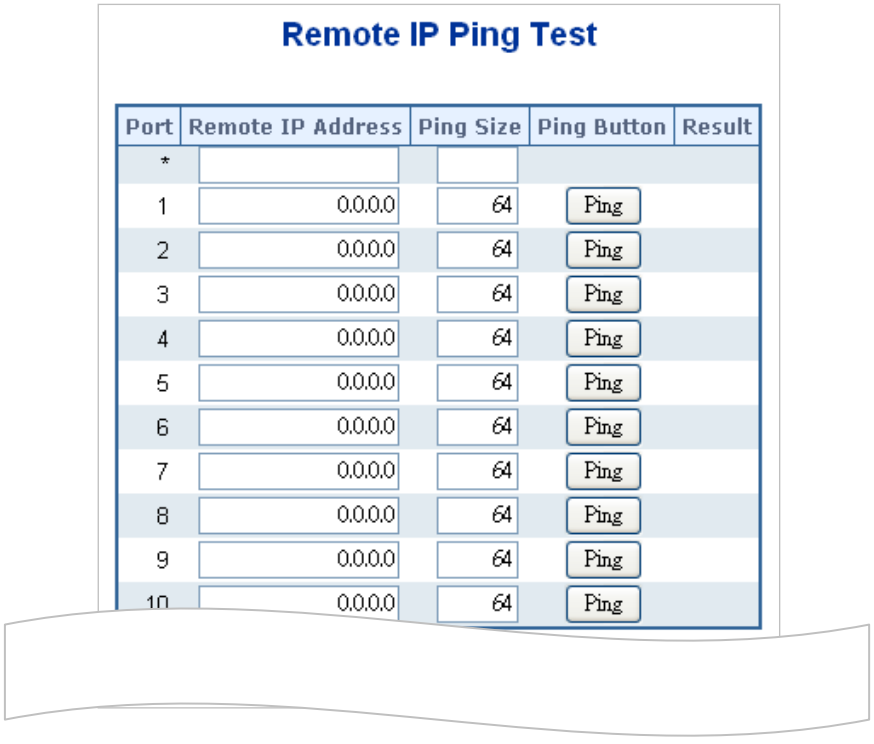
Object	Description
IP Address	The destination IP address.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Buttons

- Click **Start** to transmit ICMP packets.
- Click **New Ping** to re-start diagnostics with ping.

Remote IP ping test

This Remote ICMP Ping Test page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues on a special port. After clicking **Test**, five ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.



The page includes the following fields:

Object	Description
Port	The logical port for the settings.
Remote IP Address	The destination IP address.
Ping Size	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.
Result	Display the ping result.

Buttons

- Click **Ping** to start the ping process.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Clear** to clear the IP address and the result of the ping value.

Cable diagnostics

The VeriPHY Cable Diagnostics page is used for running cable diagnostics. Click **Start** to run the diagnostics. This will take approximately 15 seconds for a 1000Base-T Laptop/PC.

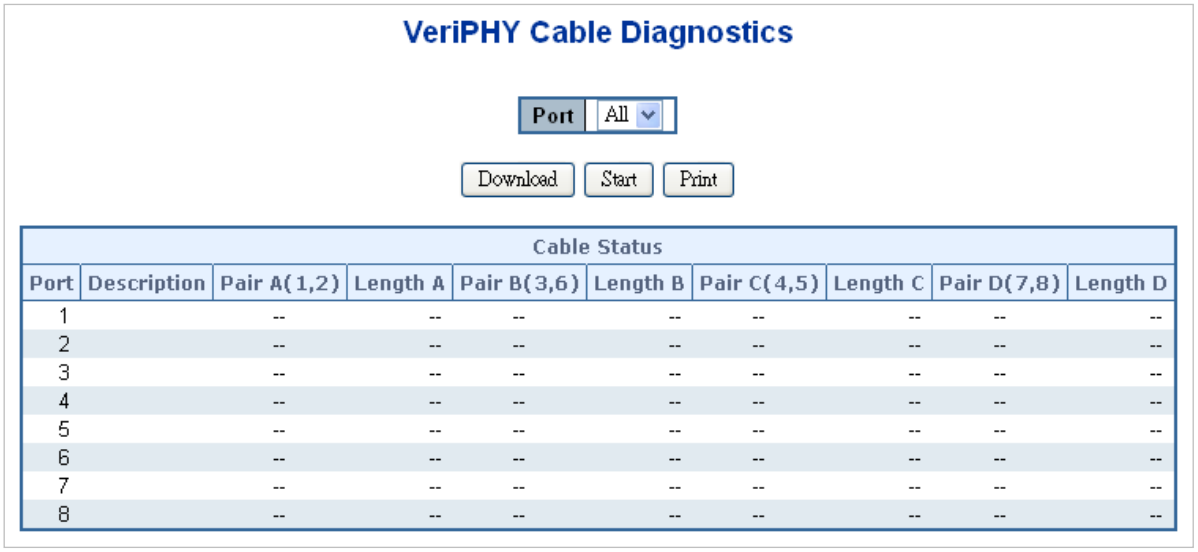
Note: Cable diagnostics is only accurate for cables of 7-140 meters in length.

Cable diagnostics performs tests on copper cables. These functions have the ability to identify the cable length and operating conditions, and to isolate a variety of common faults that can occur on the Cat5 twisted-pair cabling. There might be two states, which are as follows:

- If the link is established on the twisted-pair interface in 1000BASE-T mode, the cable diagnostics can run without disruption of the link or of any data transfer. A 1000Base-T Laptop/PC is preferred for testing the cable diagnostic function.
- If the link is established in 100BASE-TX or 10BASE-T, the cable diagnostics cause the link to drop while the diagnostics are running. This may require the following steps:
  - Select the **Auto Refresh** check box.
  - Click the **Fresh** button 45 seconds after the cable diagnostic function has started.

After the diagnostics are finished, the link is re-established and the following functions are available.

- Coupling between cable pairs
- Cable pair termination
- Cable length



The page includes the following fields:

Object	Description
Port	The port where you are requesting cable diagnostics.
Cable Status	**Port**: Port number. **Pair**: The status of the cable pair. **Length**: The length (in meters) of the cable pair. The resolution is 3 meters

Buttons

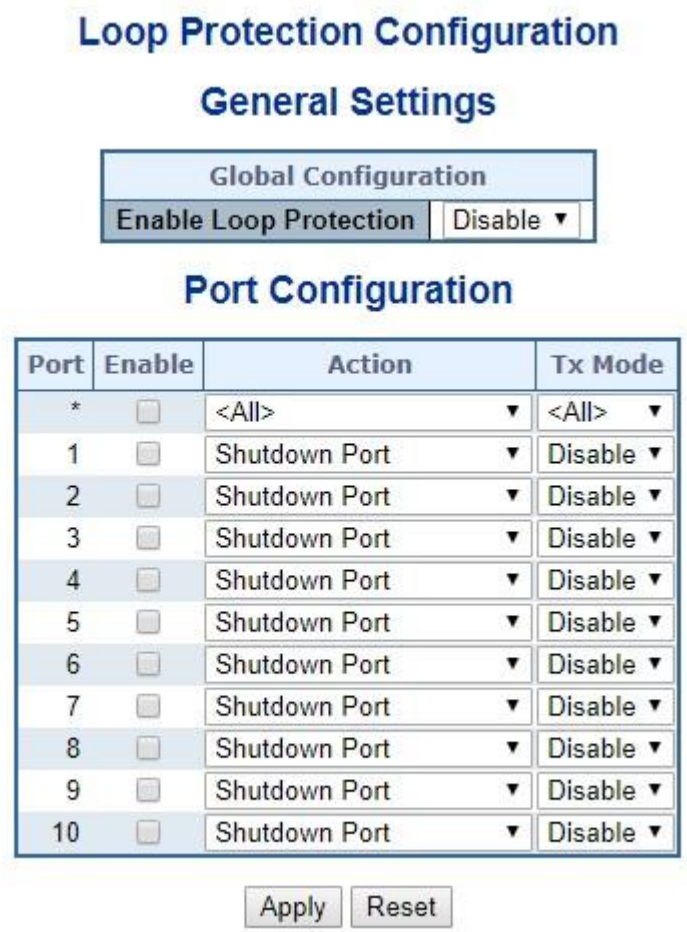
- Click **Start** to run the diagnostics.

Loop protection

This section describes the enable loop protection function that provides loop protection to prevent broadcast loops in the managed switch.

Loop protection configuration

The Loop Protection Configuration page allows the user to inspect and change the current loop protection configurations.



This page includes the following fields:

General settings

Object	Description
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 that a loop is detected and the port action shuts down the port. Valid values are 0 to 604800 seconds (seven days). A value of zero keeps a port disabled until the next device restart.

Port configuration

Object	Description
Port	The switch port number.
Enable	Controls loop protection enable/disable on this switch port.
Action	Configures the action performed when a loop is detected on a port. Selections include **Shutdown Port**, **Shutdown Port and Log** or **Log Only**.

Object	Description
Tx Mode	Controls if the port is actively generating loop protection PDUs or if it is just passively looking for looped PDU's.

Buttons

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

Loop protection status

The Loop Protection Status page shows the loop protection port status of the switch.

This page includes the following fields:

Object	Description
Port	The 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	Indicates if a loop is currently detected on the port.
Time of Last Loop	The time of the last loop event detected.

Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

RMON

RMON is an expansion of standard SNMP. RMON is a set of MIB definitions used to define standard network monitor functions and interfaces, enabling communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

The MID of RMON consists of 10 groups. The switch supports the most frequently used groups:

- **Statistics**: Maintain basic usage and error statistics for each subnet monitored by the agent.
- **History**: Record periodical statistic samples.
- **Alarm**: Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON agent records.
- **Event**: A list of all events generated by the RMON agent.

Alarm depends on the implementation of an event. **Statistics** and **History** display current or history subnet statistics. **Alarm** and **Event** provide a method to monitor any integer data change in the network, and provide some alerts upon abnormal events (sending Trap or record in logs).

RMON alarm configuration

Configure RMON alarm table on the RMON Alarm Configuration page. The entry index key is **ID**.

The page includes the following fields:

Object	Description
Delete	Select the **Delete** check box 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 broadcast and multicast packets delivered to a higher-layer protocol. **InDiscards**: The number of inbound packets that are discarded when the packets are normal. **InErrors**: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

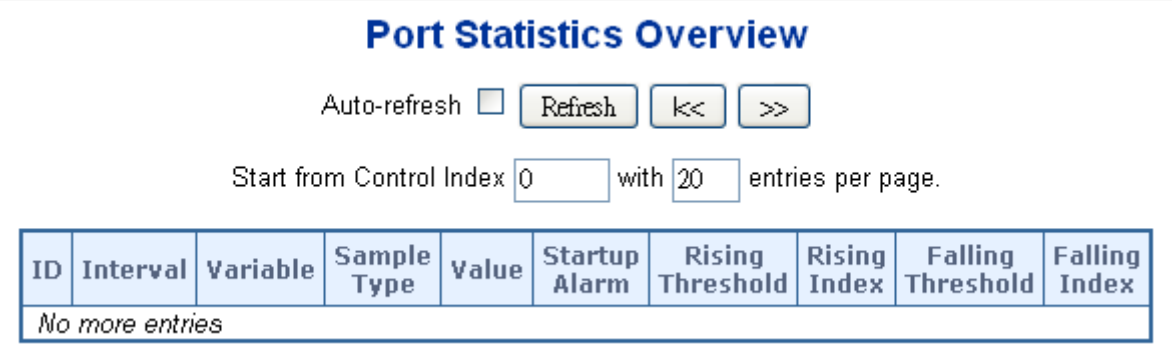
Object	Description
	InUnknownProtos: The number of inbound packets that were discarded because of an unknown or unsupported protocol. **OutOctets**: The number of octets transmitted out of the interface, including framing characters. **OutUcastPkts**: The number of unicast packets that requested to transmit. **OutNUcastPkts**: The number of broadcast and multicast packets that requested to transmit. **OutDiscards**: The number of outbound packets that are discarded when the packets are normal. **OutErrors**: 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: **Rising**: Triggers alarm when the first value is larger than the rising threshold. **Falling**: Triggers alarm when the first value is less than the falling threshold. **RisingOrFalling**: Triggers 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

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

RMON alarm status

The RMON Alarm Overview page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table (default is 20 entries per page). The range of entries per page can be typed into the **Start from Control Index** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the Alarm table. The first entry shown will be the one with the lowest ID found in the Alarm table.



The page includes the following fields:

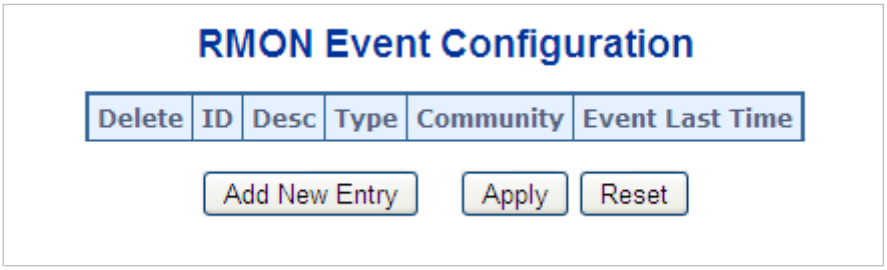
Object	Description
ID	Indicates the index of alarm control entry.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold.
Variable	Indicates the particular variable to be sampled
Sample Type	The method of sampling the selected variable and calculating the 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

- Click **Refresh** to refresh the page immediately.
- Click the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **I<<** to update the table starting from the first entry in the alarm table (i.e., the entry with the lowest ID).
- Click **>>** to update the table starting with the entry after the last entry currently displayed.

RMON event configuration

Configure the RMON Event table on the RMON Event Configuration page. The entry index key is **ID**.



The page includes the following fields:

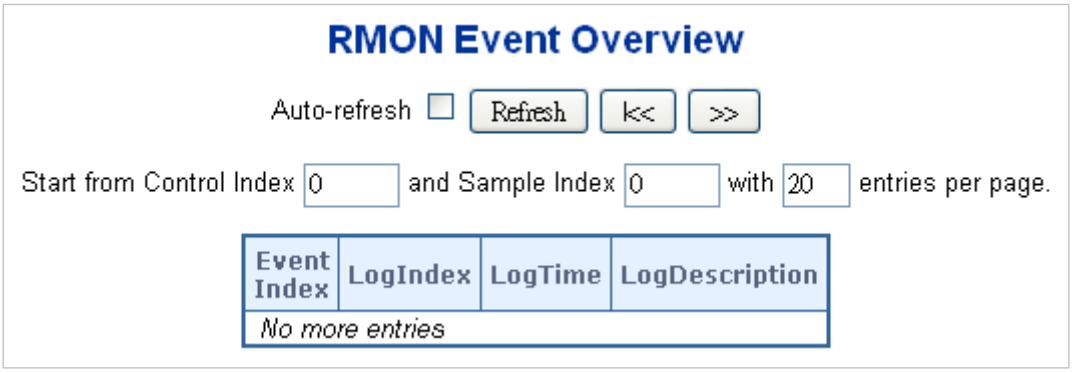
Object	Description
Delete	Select to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Desc	Indicates the event. The string length is from 0 to 127, default is a null string.
Type	Indicates the notification of the event. The possible types are: **none**: The total number of octets received on the interface, including framing characters. **log**: The number of unicast packets delivered to a higher-layer protocol. **snmptrap**: The number of broadcast and multicast packets delivered to a higher-layer protocol. **logandtrap**: The number of inbound packets that are discarded when 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

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

RMON event status

The RMON Event Overview page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table (default is 20 entries per page). The range of entries per page can be typed into the **Start from Control Index** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the Event table. The first entry shown will be the one with the lowest ID found in the Event table



The page includes the following fields:

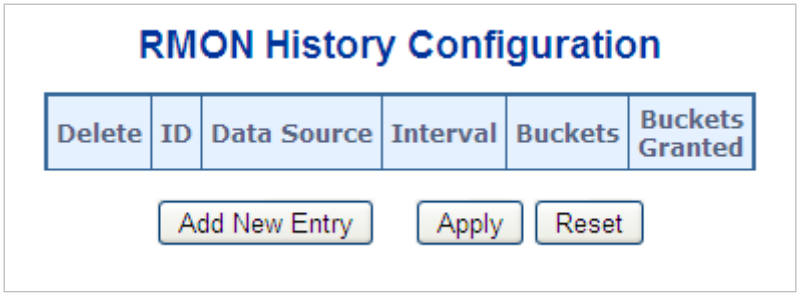
Object	Description
Event Index	Indicates the index of the event entry.
Log Index	Indicates the index of the log entry.
LogTime	Indicates event log time.
LogDescription	Indicates the event description.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **I<<** to update the table starting from the first entry in the alarm table (i.e., the entry with the lowest ID).
- Click **>>** to update the table starting with the entry after the last entry currently displayed.

RMON history configuration

Configure RMON History on the RMON History Configuration page. The entry index key is **ID**.



The page includes the following fields:

Object	Description
Delete	Select to delete the entry. It will be deleted during the next save.

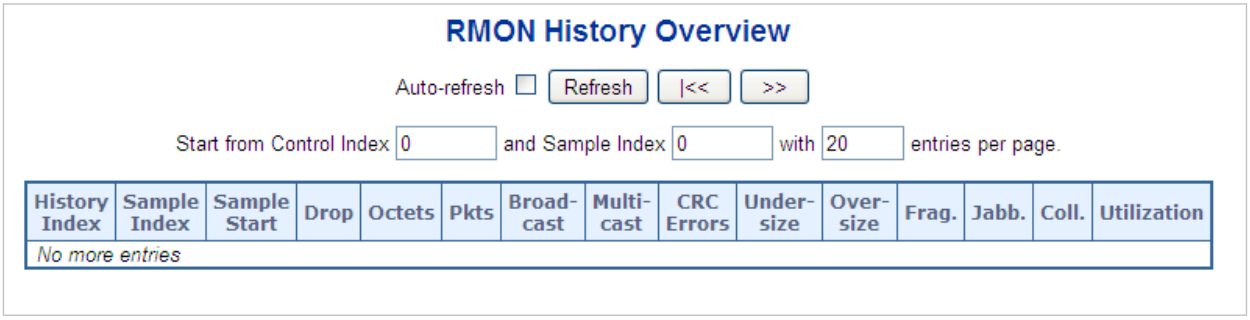
Object	Description
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID to be monitored. If in the switch, the value must add 1000*(switch ID-1). For example, if the port is switch 3 port 5, the value is 2005.
Interval	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
Buckets	Indicates the maximum data entries associated with this history control entry stored in RMON. The range is from 1 to 3600, default value is 50.
Buckets Granted	The number of data to be saved in the RMON.

Buttons

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

RMON history status

The RMON History Overview page provides details of RMON history entries.



The page includes the following fields:

Object	Description
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.

Object	Description
Multicast	The total number of good packets received that were directed to a multicast address.
CRC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets 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 with a size less than 64 octets received with invalid CRC.
Jabb.	The number of frames with a size 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

- Click **Refresh** to refresh the page immediately.
- Click the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **I<<** to update the table starting from the first entry in the alarm table (i.e., the entry with the lowest ID).
- Click **>>** to update the table starting with the entry after the last entry currently displayed.

RMON statistics configuration

Configure the RMON Statistics table on the RMON Statistics Configuration page. The entry index key is **ID**.

The page includes the following fields:

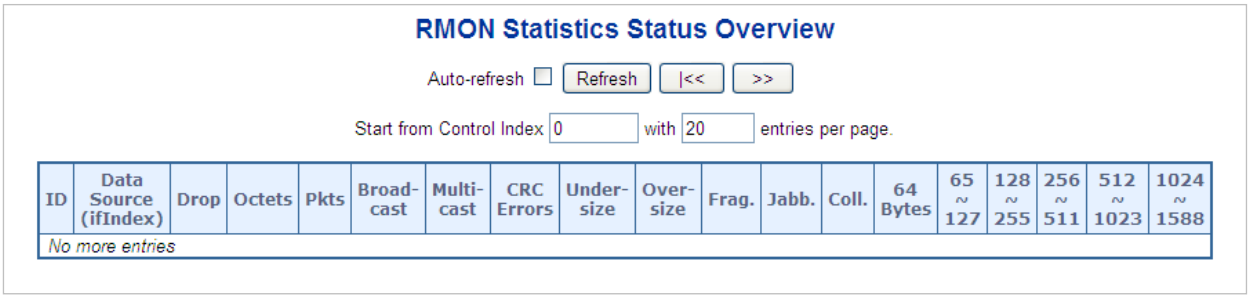
Object	Description
Delete	Select to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID to be monitored. If in the switch, the value must add 1000*(switch ID-1). For example, if the port is switch 3 port 5, the value is 2005.

Buttons

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

RMON statistics status

The RMON Statistics Status Overview page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table (default is 20 entries per page). The range of entries per page can be typed into the **Start from Control Index** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the Statistics table. The first entry shown will be the one with the lowest ID found in the Statistics table



The page includes the following fields:

Object	Description
ID	Indicates the index of statistics entry.
Data Source (ifIndex)	The port ID 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.
Broadcast	The total number of good packets received that were directed to the broadcast address.

Object	Description
Multicast	The total number of good packets received that were directed to a multicast address.
CRC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.
Undersize	The total number of packets received that were less than 64 octets.
Oversize	The total number of packets received that were longer than 1518 octets.
Frag.	The number of frames with a size less than 64 octets received with invalid CRC.
Jabb.	The number of frames with a size larger than 64 octets received with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
64 Bytes	The total number of packets (including bad packets) received that were 64 octets in length.
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

- Click **Refresh** to refresh the page immediately.
- Click the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **I<<** to update the table starting from the first entry in the alarm table (i.e., the entry with the lowest ID).
- Click **>>** to update the table starting with the entry after the last entry currently displayed.

Power over Ethernet (PoE)

Providing up to 8 PoE in-line power interfaces, the managed switch can easily build a power central-controlled IP phone system, IP camera system, and Access Point (AP) group for the enterprise. For example, 8/20 cameras/APs can be installed for company surveillance demands, or to build a wireless roaming environment in the office. Without power-socket limitation, the managed switch makes the installation of cameras or WLAN APs simple and efficient.

PoE Powered Devices (PD)

3~5 Watts	**Voice over IP phones** Enterprises can install POE VoIP phones, ATA, and other Ethernet/non-Ethernet end-devices to the central location where UPS is installed for uninterrupted power systems and power control systems.
6~12 Watts	**Wireless LAN Access Points** Museums, airports, hotels, campuses, factories, warehouses, etc. can install APs in any location.
10~12 Watts	**IP Surveillance** Enterprises, museums, campuses, hospitals, banks, etc. can install IP cameras regardless of installation location without the need to install AC sockets.
3~12 Watts	**PoE Splitter** PoE splitters split the PoE 52 VDC over the Ethernet cable into a 5/12 VDC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.
3~25 Watts	**High Power PoE Splitter** High PoE splitters split the PoE 56 VDC over the Ethernet cable into a 24/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.
30 Watts	**High Power Speed Dome** This state-of-the-art design is designed to fit into various network environments like traffic centers, shopping malls, railway stations, warehouses, airports, and production facilities for the most demanding outdoor surveillance applications without the need to install AC sockets.

System configuration

In a PoE system, operating power is applied from a power source (PSU-power supply unit) over the LAN infrastructure to powered devices (PDs), which are connected to ports. Under some conditions, the total output power required by PDs can exceed the maximum available power provided by the PSU. The system may include a PSU capable of supplying less power than the total potential power consumption of all the PoE ports in the system. To keep the majority of the ports active, power management is implemented.

The PSU input power consumption is monitored by measuring voltage and current, and is equal to the system's aggregated power consumption. The power management concept allows all ports to be active and activates additional ports, as long as the aggregated power of the system is lower than the power level at which additional PDs cannot be connected. When this value is exceeded, ports will be deactivated according

to user-defined priorities. The power budget is managed according to the following user-definable parameters:

- Maximum available power
- Ports priority
- Maximum allowable power per port

There are five modes for configuring how the ports/PDs may reserve power and when to shut down ports.

Classification mode

In this mode, each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist: 4, 7, 15.4, and 30.8 W.

Class	Usage	Range of maximum power used by the PD	Class Description
0	Default	0.44 to 12.95 W	Classification unimplemented
1	Optional	0.44 to 3.84 W	Very low power
2	Optional	3.84 to 6.49 W	Low power
3	Optional	6.49 to 12.95 W (or to 15.4 W)	Mid power
4	Optional	12.95 to 25.50 W (or to 30.8 W)	High power

Note: The maximum power fields have no effect in classification mode.

Allocation 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. The ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver.

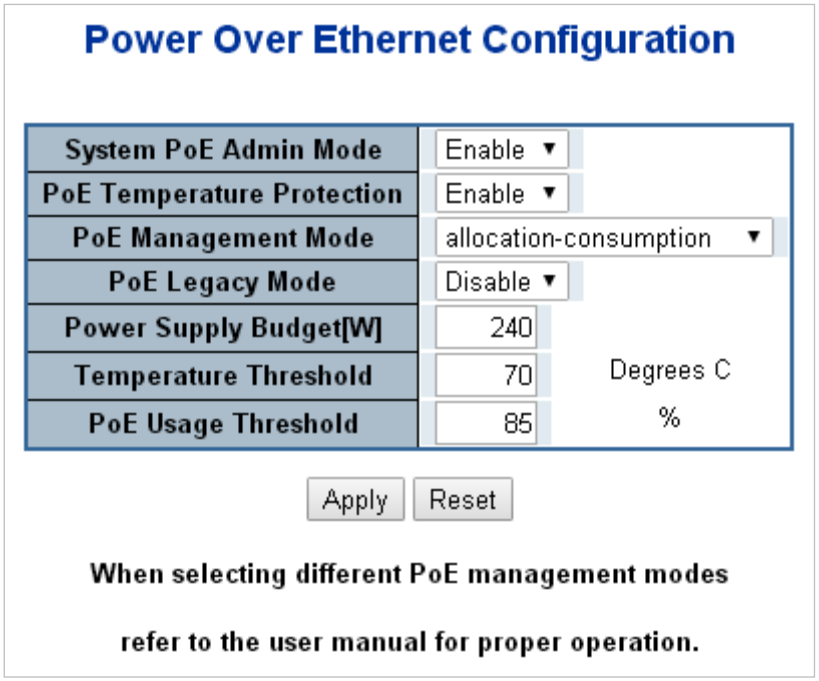
Note: In this mode, the port power is not turned on if the PD requests more available power.

LLDP mode

In this mode, the PoE power ports are managed and determined by LLDP Media protocol.

PoE configuration

Inspect and configure the current PoE configuration settings on the Power over Ethernet Configuration page.



The page includes the following fields:

Object	Description
System PoE Admin Mode	Enables/disables the PoE function, determining whether or not the PoE ports supply power.
PoE Temperature Protection	Enables/disables PoE temperature protection.
PoE Management Mode	There are six modes for configuring how the ports/PDs may reserve power and when to shut down ports. **Class-Consumption mode:** System offers PoE power according to PD real power consumption. **Class-Reserved-Power mode:** System reserves PoE power to PD according to PoE class level. **Allocation-Consumption mode:** System offers PoE power according to PD real power consumption. **Allocation-Reserved-Power mode:** Users can assign how much PoE power for per port and the system reserves PoE power to the PD. **LLDP-Consumption mode:** System offers PoE power according to PD real power consumption. **LLDP-Reserved-Power mode:** System reserves PoE power to the PD according to LLDP configuration.
Power Supply Budget [W]	Sets the limit value of the total PoE port provided power to the PDs. The managed switch available maximum value is 440.
Temperature Threshold	Sets the temperature protection threshold value. If the system temperature is over this value, then the system lowers the total PoE power budget automatically.
PoE Usage Threshold	Sets the PoE power budget limitation.

Buttons

- Click **Apply** to apply changes.

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

Power Input Unit	Power Input Voltage	PoE Power Budget	PoE Output Type
1	48 V (46~51 V)	240 W	IEEE 802.3af
1	56 V (51~56 V)	260 W	IEEE 802.3af/at
2	48 V (46~51V) + 48 V (46~51 V)	240 W	IEEE 802.3af
2	56 V (51~56 V) + 56 V (51~56 V)	320 W	IEEE 802.3af/at

Note: The wire gauge for the terminal block should be in the range of 12 ~ 22 AWG at 25°C.

PD classifications

A PD may be classified by the PSE based on the classification information provided by the PD. The intent of PD classification is to provide information about the maximum power required by the PD during operation. The PD provides a signature about Class level to improve power management at the PSE.

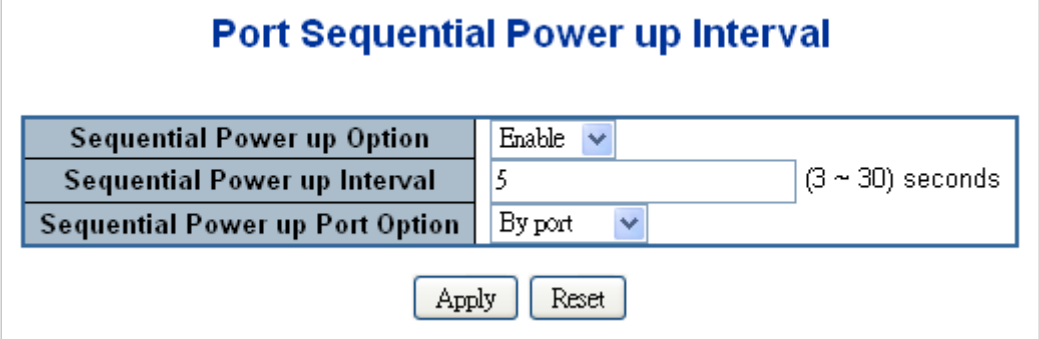
The PD is classified based on power. The classification of the PD is the maximum power that the PD draws across all input voltages and operational modes.

A PD will return to Class 0 to 4 in accordance with the maximum power draw as specified below:

Class	Usage	Range of maximum power used by the PD	Class Description
0	Default	12.95 W (or to 15.4 W for AF mode) 25.5 W (or to 30.8 W for AT mode)	Mid power or high power
1	Optional	0.44 to 3.84 W	Very low power
2	Optional	3.84 to 6.49 W	Low power
3	Optional	6.49 to 12.95 W (or to 15.4 W)	Mid power
4	Optional	12.95 to 25.50 W (or to 30.8 W)	High power

Port sequential

The Port Sequential Power up Interval page permits the user to configure the PoE ports' start up interval time. The PoE ports start up one by one.



Note: The PoE port will start up after the system program has completely finished running.

The page includes the following fields:

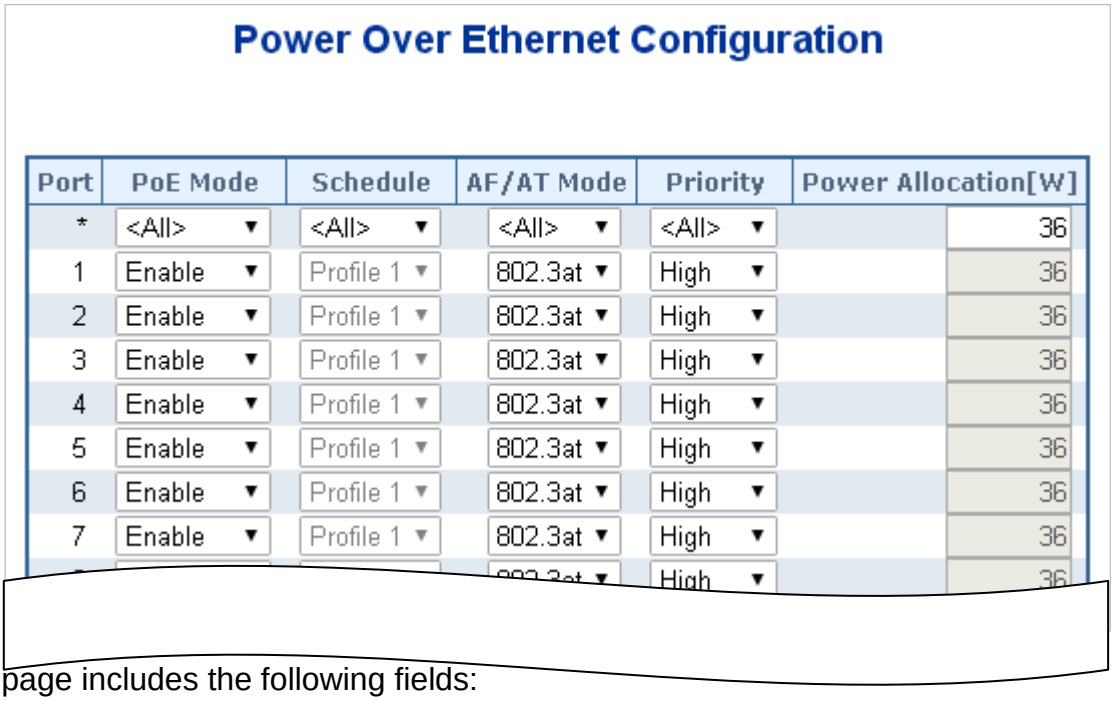
Object	Description
Sequential Power up Option	Enables/disables the sequential power-up function.
Sequential Power up Interval	Configures the PoE port start up interval time.
Sequential Power up Port Option	There are two modes for starting up the PoE port: **By Port:** The PoE port will start up by following the port number. **By Priority:** The PoE Port will start up by following the PoE priority.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port configuration

Inspect and configure the current PoE port settings on the PoE Ethernet Configuration page.



The page includes the following fields:

Object	Description
PoE Mode	There are three PoE modes: **Enable**: Enables the PoE function. **Disable**: Disables the PoE function

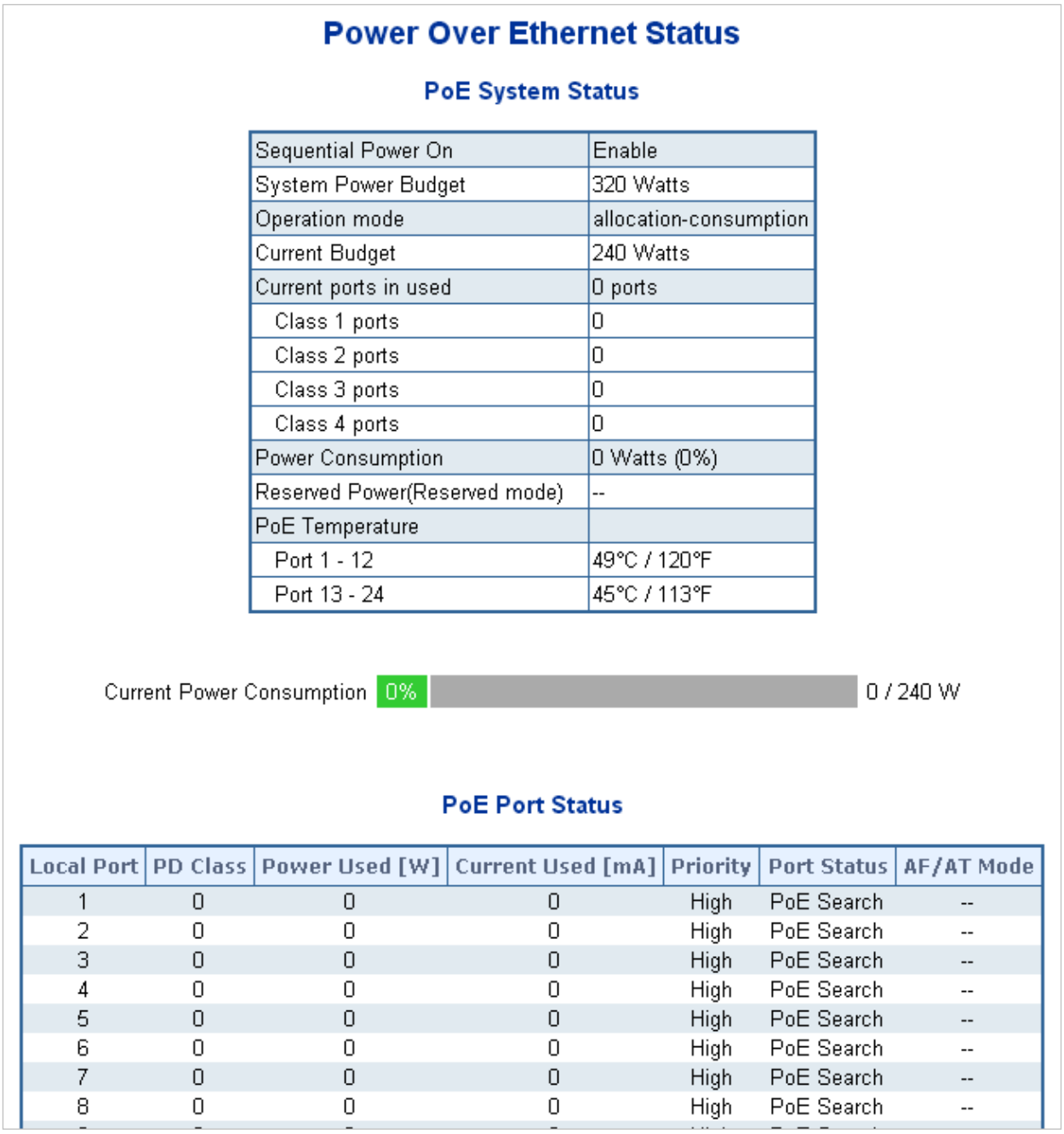
Object	Description
	Schedule: Enables the PoE function in schedule mode
Schedule	Indicates the schedule profile mode. Possible profiles are: **Profile1** **Profile2** **Profile3** **Profile4**
AF/AT Mode	Permits the user to select 802.3at or 802.3af compatibility mode. The default vaule is 802.3at mode. This function affects PoE power reservation on Classification power limit mode only. In 802.3af mode, the system is going to reserve 15.4W maximum for the PD that supports Class 3 level. In IEEE 802.3at mode, the system is going to reserve 30.8W for the PD that supports Class 4 level. Class 1 to Class 3 level in 802.3at mode reserves the same PoE power as 802.3af mode.
Priority	Priority represents PoE port priority. There are three levels of power priority: **Low**, **High**, and **Critical**. Priority is used when total power consumption is over the total power budget. In this case, the port with the lowest priority is turned off and power is provided to the port with higher priority.
Power Allocation	Limits the port PoE supply Watts. The per port maximum value must less than 30.8W, and total port values must less than the power reservation value. After a power overload has been detected, the port automatically shuts down and remains in detection mode until the PD’s power consumption is lower than the power limit value.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

PoE status

Inspect the total power consumption, total power reserved, and current status for all PoE ports on the PoE Status page.



Power Over Ethernet Status

PoE System Status

Sequential Power On	Enable
System Power Budget	320 Watts
Operation mode	allocation-consumption
Current Budget	240 Watts
Current ports in used	0 ports
Class 1 ports	0
Class 2 ports	0
Class 3 ports	0
Class 4 ports	0
Power Consumption	0 Watts (0%)
Reserved Power(Reserved mode)	--
PoE Temperature	
Port 1 - 12	49°C / 120°F
Port 13 - 24	45°C / 113°F

Current Power Consumption 0% 0 / 240 W

PoE Port Status

Local Port	PD Class	Power Used [W]	Current Used [mA]	Priority	Port Status	AF/AT Mode
1	0	0	0	High	PoE Search	--
2	0	0	0	High	PoE Search	--
3	0	0	0	High	PoE Search	--
4	0	0	0	High	PoE Search	--
5	0	0	0	High	PoE Search	--
6	0	0	0	High	PoE Search	--
7	0	0	0	High	PoE Search	--
8	0	0	0	High	PoE Search	--

The page includes the following fields:

Object	Description
Sequential Power On	Displays the current sequential power on mode.
System Power Budget	Displays the maximum PoE power budget.
Operation mode	Displays the current PoE operation mode.
Current Budget	Displays the current maximum PoE budget.
Current ports in used	Dispalys the current PoE in-use ports.

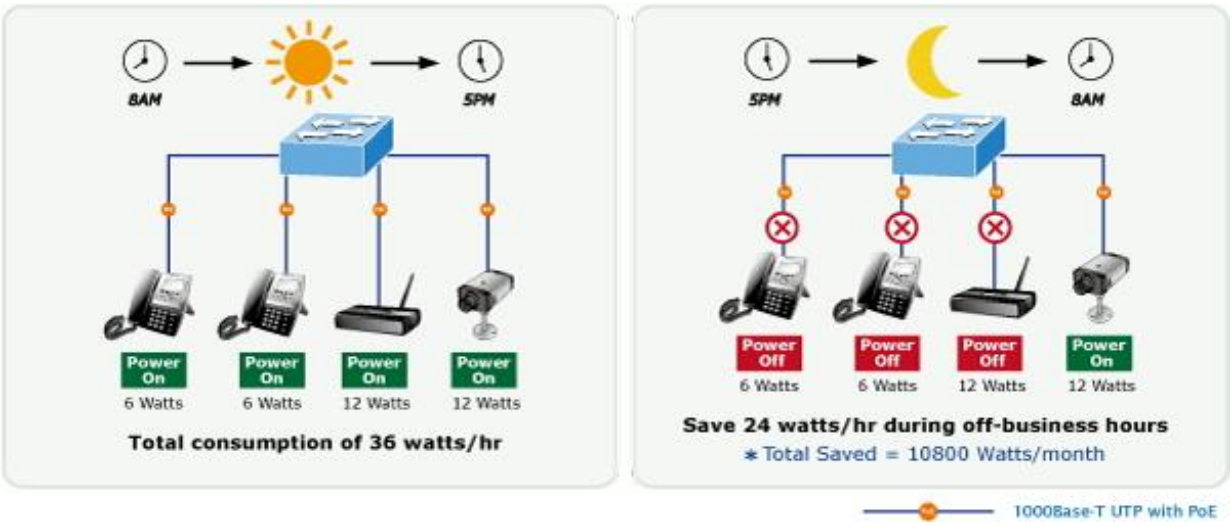
Object	Description
Class 1 ~ 4 ports	Displays the current PoE class 1 ~ 4 ports.
Power Consumption	Dispalys the current power consumption (total Watts and percentage).
Reserved Power (Reserved mode)	Shows how much the total power is reserved for all PDs.
PoE Temperature	Displays the current operating temperature of the first PoE chip unit. Chipset 1 = port 1 ~ 12 Chipset 2 = port 13 ~ 24
Current Power Consumption	Shows the total W usage of the managed switch.
Local Port	This is the logical port number for this row.
PD Class	Displays the class of the PD attached to the port as established by the classification process. Class 0 is the default for PDs. The PD is powered based on PoE class level if the system is working in classification mode. A PD will return Class to 0 to 4 in accordance with the maximum power draw as specified in “PD classifications” on page 290.
Power Used [W]	Shows how much power the PD is currently using.
Current Used [mA]	Shows how much current the PD is currently using.
Priority	Shows the port's priority configured by the user.
Port Status	Shows the port's status.
AF / AT Mode	Displays per PoE ports operating in 802.3af or 802.3at mode.
Total	Shows the total power and current usage of all PDs.

Buttons

- Select the **Auto-refresh** check box to enable an automatic refresh of the page at regular intervals.
- Click **Refresh** to refresh the page immediately.

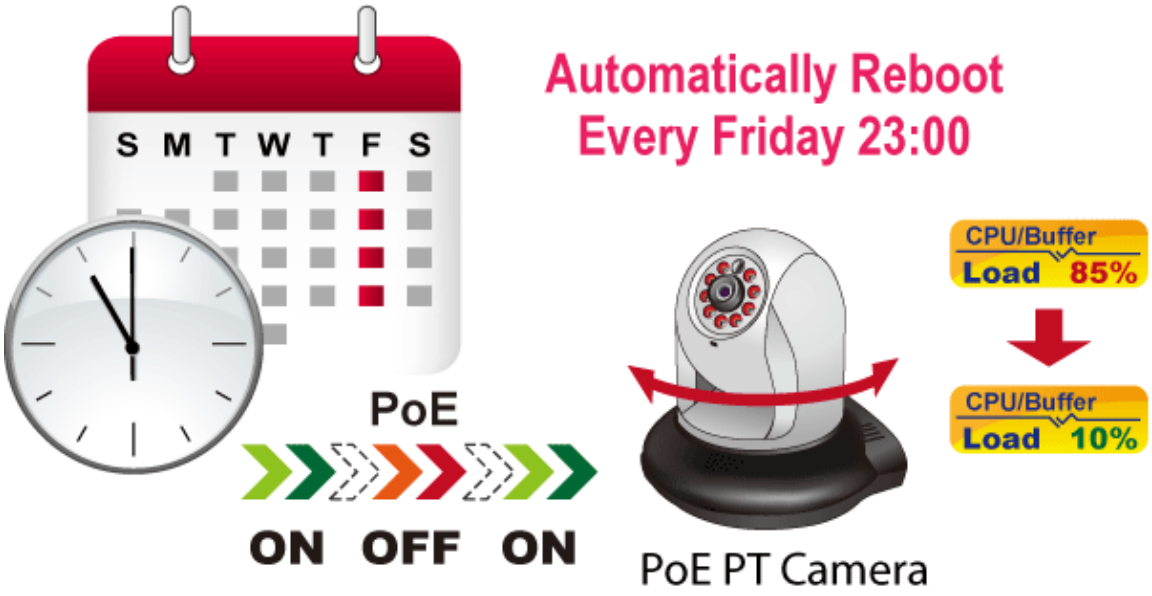
PoE schedule

In addition to its functional use for IP surveillance, the managed switch can also be implemented in any PoE network including VoIP and Wireless LAN. Under the trend of energy saving worldwide and contributing to worldwide environmental protection, the managed switch can effectively control power supply in addition to its capability to provde high Watt power. The PoE schedule function can enable or disable PoE power feeding for each PoE port during specified time intervals, and is a powerful function to help SMB or Enterprises save power and reduce cost.

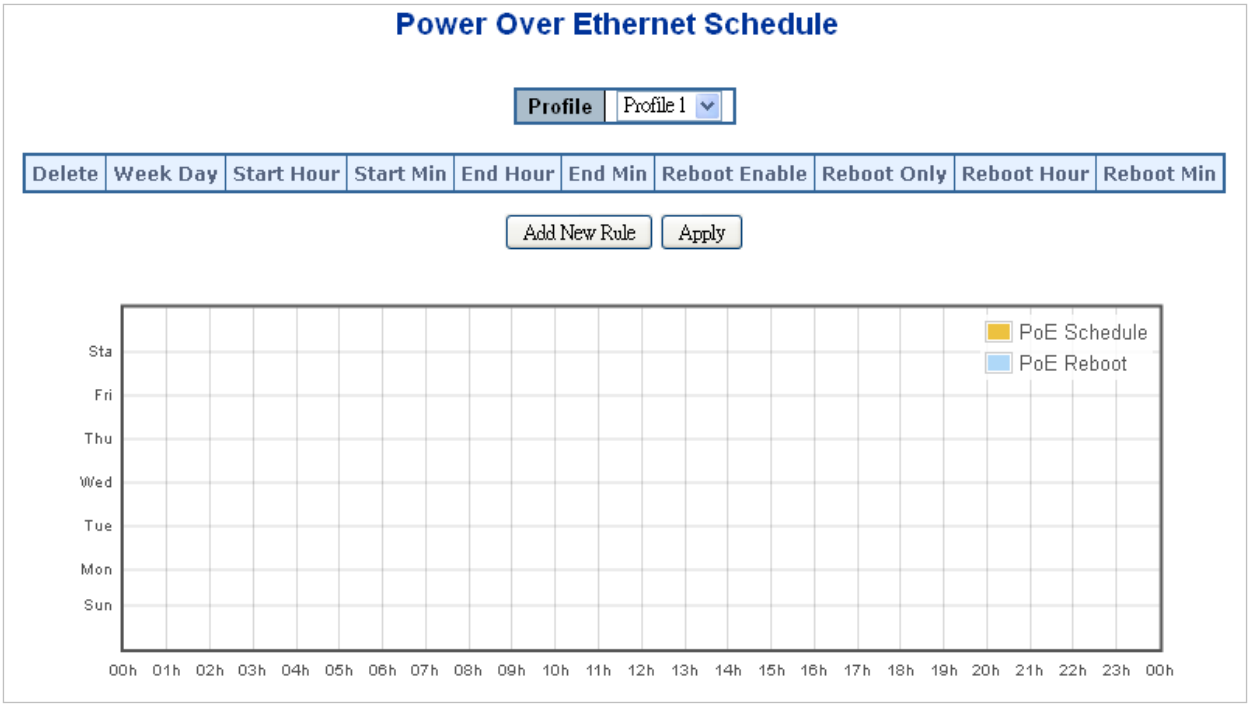


Scheduled power recycling

The managed switch allows each of the connected PoE IP cameras to reboot at a specific time each week, thus reducing the chance of IP camera crashes resulting from buffer overflow.



Define the PoE schedule and schedule power recycling on the PoE Schedule page.



Click the **Add New Rule** button to start setting the PoE schedule function. Click **Apply** after creating a schedule for the selected profile. Then, go to the PoE Port Configuration page and select **Schedule** from the PoE Mode drop-down list, and the profile number from the Schedule drop-down list, for each port to which you want to apply the schedule profile.

The page includes the following fields:

Object	Description
Profile	Set the schedule profile mode. Possible profiles are: **Profile1** **Profile2** **Profile3** **Profile4**
Week Day	Set the weekday for enabling the PoE function.
Start Hour	Set the hour for enabling the PoE function.
Start Min	Set the minute for enabling the PoE function.
End Hour	Set the hour for disabling the PoE function.
End Min	Set the minute for disabling the PoE function.
Reboot Enable	Enables or disables a PoE port reboot according to the PoE reboot schedule. Note that if you want the PoE schedule and PoE reboot schedule to work at the same time, use this function and do not use the Reboot Only function. This function permits the administrator to reboot the PoE device at the indicated time as required.

Object	Description
Reboot Only	Permits a reboot of the PoE function according to the PoE reboot schedule. Note that if the administrator enables this function, the PoE schedule will not set the time to a profile. This function only applies to PoE port reset at the indicated time.
Reboot Hour	Sets the hour for PoE reboots. This function is only for the PoE reboot schedule.
Reboot Min	Sets what the minute for PoE reboots. This function is only for the PoE reboot schedule.

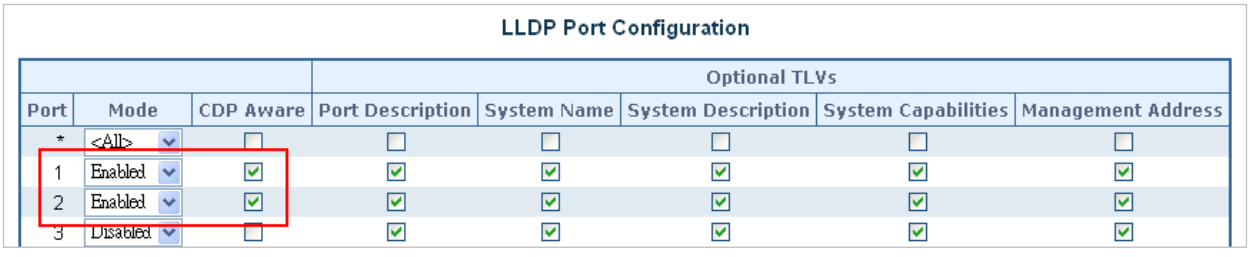
Buttons

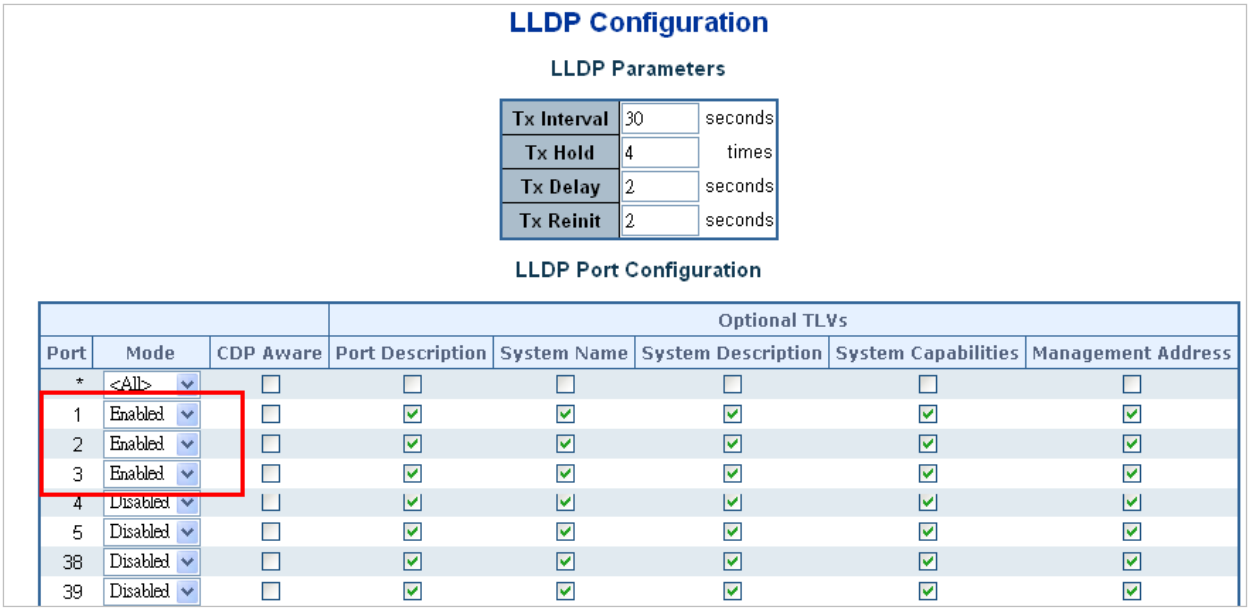
- Click **Add New Rule** to set the PoE schedule function.
- Click **Apply** to apply changes.
- Click **Delete** to delete the entry.

LLDP PoE neighbors

The LLDP Neighbor PoE Information page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each port on which an LLDP PoE neighbor is detected.

The administrator must enable the LLDP port in the LLDP Configuration page (see below). In this example, the LLDP function from port 1 to port 2 was enabled. After plugging in a PD that supports the PoE LLDP function, the PD's PoE information appears in the LLDP Neighbor PoE Information page.





LLDP Configuration

LLDP Parameters

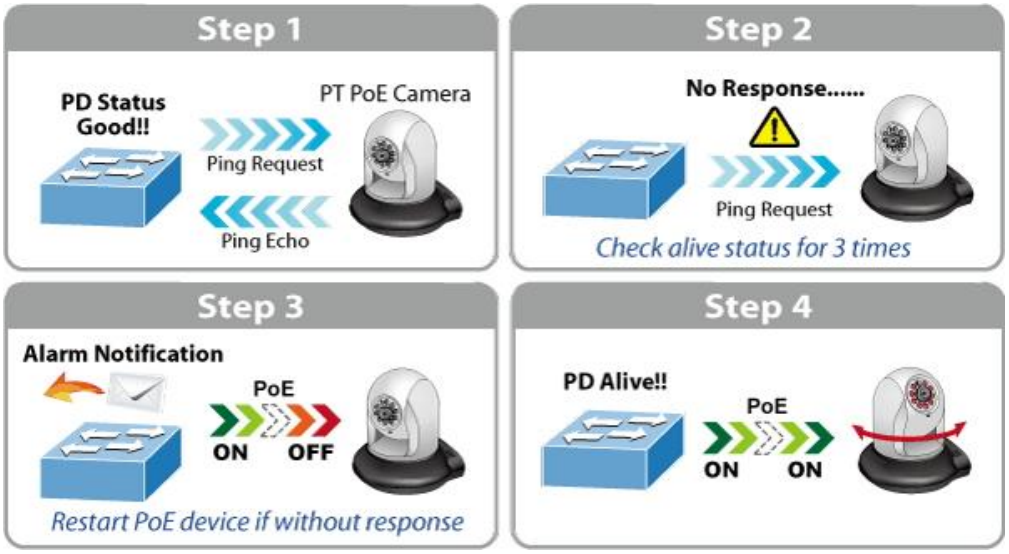
Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Port Configuration

			Optional TLVs				
Port	Mode	CDP Aware	Port Description	System Name	System Description	System Capabilities	Management Address
*	<All>	☐	☐	☐	☐	☐	☐
1	Enabled	☐	☑	☑	☑	☑	☑
2	Enabled	☐	☑	☑	☑	☑	☑
3	Enabled	☐	☑	☑	☑	☑	☑
4	Disabled	☐	☑	☑	☑	☑	☑
5	Disabled	☐	☑	☑	☑	☑	☑
38	Disabled	☐	☑	☑	☑	☑	☑
39	Disabled	☐	☑	☑	☑	☑	☑

PoE alive check configuration

The managed switch can be configured to monitor a connected PD's status in real-time via ping action. After the PD stops working and does not respond, the managed switch restarts PoE port power so that the PD is once again recognized and working.



Configure PD alive check on the PD Ping Alive Check page.

The page includes the following fields:

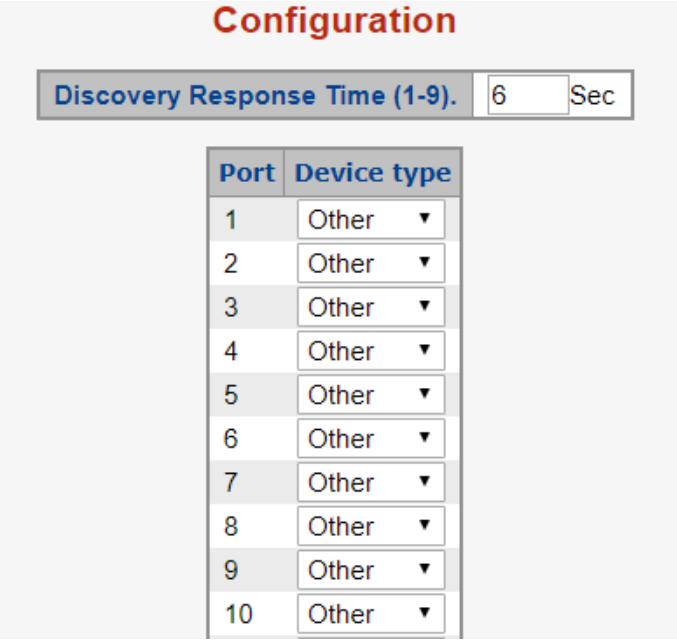
Object	Description
Mode	Enables/disables the per port PD alive check function. All ports are disabled by default.
Ping PD IP Address	Set the PoE device IP address in this field. The PD's IP address must be set to the same network segment as the managed switch.
Interval Time (10~300s)	Set the length of time a ping request should be issued to the PD. Interval time range is from 10 to 300 seconds.
Retry Count (1~5)	Set the number of times that system retry pings to the PD. For example, if the count is set to 2, and the system retries pings to the PD and the PD doesn't respond continuously, the PoE port will be reset.
Action	Set the action to be applied if the PD does not respond. Action selections are as follows: **PD Reboot**: The system resets the PoE port that connected the PD. **Reboot & Alarm**: The system resets the PoE port and issues an alarm message via syslog, SMTP. **Alarm**: The system issues an alarm message via syslog, SMTP.
Reboot Time (30~180s)	Set the PoE device rebooting time. This is useful due to the different rebooting time of PoE devices. The PD alive check is not a defining standard, so the PoE device doesn't report reboot complete information to the managed switch. As a result, the user must ensure how long the PD reboot takes, and then set the time value in this column. The system checks the PD again according to the reboot time. If you cannot determine the precise booting time, we suggest set it to a longer time.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port identification

Configure each port response time for TruVision Navigator in the port identification Configuration page.



Chapter 5
Command line interface

Accessing the CLI

When accessing the management interface for the managed switch via a Telnet connection, the managed switch can be managed by entering command keywords and parameters at the prompt. Using the managed switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

This chapter describes how to use the Command Line Interface (CLI).

Telnet login

The managed switch supports telnet for remote management. The switch asks for a user name and password for remote login when using telnet. Use **“admin”** for the both the username and password.

Chapter 6
Command line mode

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes support specific software commands.

Command Groups:

System	System settings and reset options
IP	IP configuration and Ping
Port	Port management
MAC	MAC address table
VLAN	Virtual LAN
PVLAN	Private VLAN
Security	Security management
STP	Spanning Tree Protocol
Aggr	Link Aggregation
LACP	Link Aggregation Control Protocol
LLDP	Link Layer Discovery Protocol
LLDPMED	Link Layer Discovery Protocol Media
Thermal	Thermal Protection
PoE	Power Over Ethernet
EVC	Ethernet Virtual Connections
EPS	Ethernet Protection Switching
MEP	Maintainence entity End Point
QoS	Quality of Service
Mirror	Port mirroring
Config	Load/Save of configuration via TFTP
Firmware	Download of firmware via TFTP
UPnP	Universal Plug and Play
MVR	Multicast VLAN Registration
Voice VLAN	Specific VLAN for voice traffic

ERPS	Ethernet Ring Protection Switching
Loop Protect	Loop Protection
IPMC	MLD/IGMP Snooping
VCL	VLAN Control List
SMTP	SMTP Control Configure
DIDO	DIDO control configure
Show	Show control configuration

System Command

System Configuration

Description:

Show system configuration.

Syntax:

System Configuration [all] [<port_list>]

Parameters:

all : Show all switch configuration, default: Show system configuration

port : Show switch port configuration

<port_list>: Port list or 'all', default: All ports

Example:

To display system information:

```
NS3502-8P-2T-2S-V2:/>System configuration
System Contact  :
System Name     : NS3502-8P-2T-2S-V2
System Location :
MAC Address     : 9c-f6-1a-02-7d-70
Temperature     : 27.0 C - 80.6 F
System Time     : 1970-01-01 Thu 03:28:50+00:00
System Uptime   : 03:28:50
Software Version: 1.0b121221
Software Date   : 2012-12-21T14:58:31+0800
Previous Restart: Cold
Power Status    : PWR1 :ON,PWR2 :OFF
NS3502-8P-2T-2S-V2:/>
```

System Log Configuration

Description:

Show system log configuration.

Syntax:

System Log Configuration

Example:

To display system log information:

```
NS3502-8P-2T-2S-V2:/>System log configuration
System Log Configuration:
=========================

System Log Server Mode     : Disabled
System Log Server Address  :
System Log Level           : Info
NS3502-8P-2T-2S-V2:/>
```

System Timezone Configuration

Description:

Show System Timezone configuration.

Syntax:

System Timezone Configuration

System Version

Description:

Show system version information.

Syntax:

System Version

Example:

To display system version:

```
NS3502-8P-2T-2S-V2:/>System version
Version      : 1.0b121221
Build Date   : 2012-12-21T14:58:31+0800
NS3502-8P-2T-2S-V2:/>
```

System Log Server Mode

Description:

Show or set the system log server mode.

Syntax:

System Log Server Mode [enable|disable]

Parameters:

enable : Enable system log server mode

disable: Disable system log server mode

(default: Show system Log server mode)

Default Setting:

disable

Example:

To show the log server mode:

```
NS3502-8P-2T-2S-V2:/>System log server mode
System Log Server Mode     : Disabled
```

System Name

Description:

Set or show the system name.

Syntax:

System Name [<name>]

Parameters:

<name>: System name string. (1-255)

Use "" to clear the string

System name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-).

No blank or 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.

System Timezone Offset

Description:

Set or show the system timezone offset.

Syntax:

System Timezone Offset [<offset>]

Parameters:

<offset>: Time zone offset in minutes (-7200 to 7201) relative to UTC

System Contact

Description:

Set or show the system contact.

Syntax:

System Contact [<contact>] [clear]

Parameters:

<contact>: System contact string. (1-255)

Use 'clear' or "" to clear the string

In CLI, No blank or space characters are permitted as part of a contact.

clear : Clear system contact

Default Setting:

empty

System Log Server Address

Description:

Show or set the system log server address.

System Log Server Address [<ip_addr_string>]

Parameters:

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

Default Setting:

empty

Example:

To set log server address:

```
NS3502-8P-2T-2S-V2:/> log server address 192.168.0.21
```

System Timezone Acronym

Description:

Set or show the system timezone acronym.

Syntax:

System Timezone Acronym [<acronym>]

Parameters:

<acronym>: Time zone acronym (0 - 16 characters)

Default Setting:

empty

System DST Configuration

Description:

Show Daylight Saving Time configuration.

Syntax:

System DST Configuration

System Location

Description:

Set or show the system location.

Syntax:

System Location [<location>]

Parameters:

<location>: System location string. (1-255)

Use 'clear' or "" to clear the string

In CLI, no blank or space characters are permitted as part of a location.

Default Setting:

empty

Example:

To set device location:

```
NS3502-8P-2T-2S-V2:/>System location MyOffice
```

System Log Level

Description:

Show or set the system log level.

It uses to determine what kind of message will send to syslog server.

Syntax:

System Log Level [info|warning|error]

Parameters:

info : Send informations, warnings and errors

warning : Send warnings and errors

error : Send errors

Default Setting:

info

Example:

To set log level:

```
NS3502-8P-2T-2S-V2:/> log level warning
```

System DST Mode

Description:

Set or show the daylight saving time mode.

Syntax:

System DST Mode [disable|recurring|non-recurring]

Parameters:

disable: Disable Daylight Saving Time
recurring : Enable Daylight Saving Time as recurring mode
non-recurring : Enable Daylight Saving Time as non-recurring mode

Default Setting:

Disabled

System DST Start

Description:

Set or show the daylight saving time start time settings.

Syntax:

System DST start <week> <day> <month> <date> <year> <hour> <minute>

Parameters:

<week> : Week (1-5), 0: ignored
<day> : Day (1-7), 0: ignored
<month> : Month (1-12), 0: ignored
<date> : Date (1-31), 0: ignored
<year> : Year (2000-2097)
<hour> : Hour (0-23)
<minute>: Minutes (0-59)

System Log Lookup

Description:

Show the system log.

Syntax:

System Log Lookup [<log_id>] [all|info|warning|error]

Parameters:

<log_id>: System log ID or range (default: All entries)
all : Show all levels (default)
info : Show informations
warning : Show warnings
error : Show errors

System DST End

Description:

end: Set or show the daylight saving time end time settings.

Syntax:

System DST end <week> <day> <month> <date> <year> <hour> <minute>

Parameters:

<week> : Week (1-5), 0: ignored
<day> : Day (1-7), 0: ignored
<month> : Month (1-12), 0: ignored
<date> : Date (1-31), 0: ignored

<year> : Year (2000-2097)
<hour> : Hour (0-23)
<minute>: Minutes (0-59)

System Log Clear

Description:
Clear the system log.
Syntax:
System Log Clear [all|info|warning|error]
Parameters:
all : Show all levels (default)
info : Show informations
warning : Show warnings
error : Show errors

System Reboot

Description:
Reboot the system.
Syntax:
System Reboot
Example:
To reboot device without changing any of the settings:

```
NS3502-8P-2T-2S-V2:/>system reboot
```

System DST Offset

Description:
Set or show the daylight saving time offset.
Syntax:
System DST Offset [<dst_offset>]
Parameters:
<dst_offset>: DST offset in minutes (1 to 1440)

System Restore Default

Description:
Restore factory default configuration.
Syntax:
System Restore Default [keep_ip]
Parameters:
keep_ip: Keep IP configuration, default: Restore full configuration
Example:
To restore default value but not reset IP address:

```
NS3502-8P-2T-2S-V2:/>system restore default keep_ip
```

System Load

Description:

Show current CPU load: 100ms, 1s and 10s running average (in percent, zero is idle).

Syntax:

System Load

Example:

To show current CPU load:

```
NS3502-8P-2T-2S-V2:/>system load
Load average(100ms, 1s, 10s):   1%,   1%,   1%
```

IP Command

IP Configuration

Description:

Show IP configuration.

Syntax:

IP Configuration

Example:

Show IP configuration:

```
NS3502-8P-2T-2S-V2:/>ip configuration

IP Configuration:
=================

DHCP Client      : Disabled
IP Address       : 192.168.0.101
IP Mask          : 255.255.255.0
IP Router        : 192.168.0.253
DNS Server       : 0.0.0.0
VLAN ID          : 1
DNS Proxy        : Disabled

IPv6 AUTOCONFIG mode   : Disabled
IPv6 Link-Local Address: fe80::6082:cdb9:19ab:c0e2
IPv6 Address           : ::192.168.0.100
IPv6 Prefix            : 96
IPv6 Router            : ::
```

IP DHCP

Description:

Set or show the DHCP client mode.

Syntax:

IP DHCP [enable|disable]

Parameters:

enable : Enable or renew DHCP client

disable: Disable DHCP client

Default Setting:

Disable

Example:

Disable DHCP sever:

```
NS3502-8P-2T-2S-V2:/>ip dhcp disable
```

IP Setup

Description:

Set or show the IP setup.

Syntax:

IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]

Parameters:

<ip_addr> : IP address (a.b.c.d), default: Show IP address

<ip_mask> : IP subnet mask (a.b.c.d), default: Show IP mask

<ip_router>: IP router (a.b.c.d), default: Show IP router

<vid> : VLAN ID (1-4095), default: Show VLAN ID

Default Setting:

IP Address : 192.168.0.100
IP Mask : 255.255.255.0
IP Router : 192.168.0.1
DNS Server : 0.0.0.0
VLAN ID : 1

Example:

Set IP address:

```
NS3502-8P-2T-2S-V2:/>ip setup 192.168.0.100 255.255.255.0
```

IP Ping

Description:

Ping IP address (ICMP echo).

Syntax:

IP Ping <ip_addr_string> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]

Parameters:

<ip_addr_string>: IPv4 host address (a.b.c.d) or a host name string

length : PING Length keyword

<ping_length> : Ping ICMP data length (2-1452; Default is 56), excluding MAC, IP and ICMP headers

count : PING Count keyword

<ping_count> : Transmit ECHO_REQUEST packet count (1-60; Default is 5)

interval : PING Interval keyword

<ping_interval> : Ping interval (0-30; Default is 0)

IP DNS

Description:

Set or show the DNS server address.

Syntax:

IP DNS [<ip_addr>]

Parameters:

<ip_addr>: IP address (a.b.c.d), default: Showdne IP address

Default Setting:

0.0.0.0

Example:

Set DNS IP address:

```
NS3502-8P-2T-2S-V2:/>ip dns 168.95.1.1
```

IP DNS Proxy

Description:

Set or show the IP DNS Proxy mode.

Syntax:

IP DNS_Proxy [enable|disable]

Parameters:

enable : Enable DNS Proxy

disable: Disable DNS Proxy

Default Setting:

disable

Example:

Enable DNS proxy function:

```
NS3502-8P-2T-2S-V2:/>ip dns_proxy enable
```

IPv6 AUTOCINFIG

Description:

Set or show the IPv6 AUTOCONFIG mode.

Syntax:

IP IPv6 AUTOCONFIG [enable|disable]

Parameters:

enable : Enable IPv6 AUTOCONFIG mode

disable: Disable IPv6 AUTOCONFIG mode

Default Setting:

disable

Example:

Enable IPv6 autoconfig function:

```
NS3502-8P-2T-2S-V2:/>ip ipv6 autoconfig enable
```

IPv6 Setup

Description:

Set or show the IPv6 setup.

Syntax:

IP IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>]

Parameters:

<ipv6_addr>: 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, 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 only appear once. It also uses a following legally IPv4 address. For example,'::192.1.2.34'.

<ipv6_prefix>: IPv6 subnet mask , default: Show IPv6 prefix

<ipv6_router>: IPv6 router , default: Show IPv6 router. 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 only appear once. It also uses a following legally IPv4 address. For example,'::192.1.2.34'.

Default Setting:

IPv6 AUTOCONFIG mode : Disabled
IPv6 Link-Local Address: fe80::6082:cdb9:19ab:c0e2
IPv6 Address : ::192.168.0.100
IPv6 Prefix : 96
IPv6 Router : ::

Example:

Set IPv6 address:

```
NS3502-8P-2T-2S-V2:/>ip ipv6 setup 2001::0002 64 2100::0001
```

IPv6 State

Description:

Set or show the IPv6 Interface operational state.

Syntax:

IP IPv6 State <ipv6_addr> [enable|disable]

Parameters:

<ipv6_addr>: 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, 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 only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

enable : Enable the designated IPv6 Interface

disable: Disable the designated IPv6 Interface

IPv6 Ping6

Description:

Ping IPv6 address (ICMPv6 echo).

Syntax:

IP IPv6 Ping6 <ipv6_addr> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]

Parameters:

<ipv6_addr> : IPv6 host 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, 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 only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

length : PING Length keyword

<ping_length> : Ping ICMP data length (2-1452; Default is 56), excluding MAC, IP and ICMP headers

count : PING Count keyword

<ping_count> : Transmit ECHO_REQUEST packet count (1-60; Default is 5)

interval : PING Interval keyword

<ping_interval>: Ping interval (0-30; Default is 0)

IP NTP Configuration

Description:

Show NTP configuration.

Syntax:

IP NTP Configuration

Default Setting:

IP NTP Configuration:
==========
NTP Mode : Disabled
Idx Server IP host address (a.b.c.d) or a host name string
--- ----------
1 pool.ntp.org
2 europe.pool.ntp.org
3 north-america.pool.ntp.org
4 asia.pool.ntp.org
5 oceania.pool.ntp.org

IP NTP Mode

Description:

Set or show the NTP mode.

Syntax:

IP NTP Mode [enable|disable]

Parameters:

enable : Enable NTP mode

disable : Disable NTP mode

(default: Show NTP mode)

Default Setting:

disable

Example:

Enable NTP mode:

```
NS3502-8P-2T-2S-V2:/>ip ntp mode enable
```

IP NTP Server Add

Description:

Add NTP server entry.

Syntax:

IP NTP Server Add <server_index> <ip_addr_string>

Parameters:

<server_index> : The server index (1-5)

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

Example:

To add NTP server:

```
NS3502-8P-2T-2S-V2:/>ip ntp server add 1 60.249.136.151
```

IP NTP Server IPv6 Add

Description:

Add NTP server IPv6 entry.

Syntax:

IP NTP Server Ipv6 Add <server_index> <server_ipv6>

Parameters:

<server_index>: The server index (1-5)

<server_ipv6> : IPv6 server 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 only appear once. It also uses a following legally IPv4 address. For example,'::192.1.2.34'.

Example:

To add IPv6 NTP server:

```
NS3502-8P-2T-2S-V2:/>ip ntp server ipv6 add 1 2001:7b8:3:2c::123
```

IP NTP Server Delete

Description:

Delete NTP server entry.

Syntax:

IP NTP Server Delete <server_index>

Parameters:

<server_index>: The server index (1-5)

Example:

To delete NTP server:

```
NS3502-8P-2T-2S-V2:/>ip ntp server delete 1
```

Port Management Command

Port Configuration

Description:

Show port configuration.

Syntax:

Port Configuration [<port_list>] [up|down]

Parameters:

<port_list>: Port list or 'all', default: All ports

up : Show ports, which are up

down **:** Show ports, which are down

(default: Show all ports)

Example:

Display port1~4 status

```
NS3502-8P-2T-2S-V2:/>port configuration 1-4

Port Configuration:
===================


Port  State    Mode    Flow Control  MaxFrame  Power     Excessive
Link
----  -------- ------  ------------  --------  --------  ---------  ----
1     Enabled  Auto    Disabled      9600      Disabled  Discard    Down
2     Enabled  Auto    Disabled      9600      Disabled  Discard    Down
3     Enabled  Auto    Disabled      9600      Disabled  Discard    Down
4     Enabled  Auto    Disabled      9600      Disabled  Discard    Down
```

Port Mode

Description:

Set or show the port speed and duplex mode.

Syntax:

Port Mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx]

Parameters:

<port_list>: Port list or 'all', default: All ports

auto : Auto negotiation of speed and duplex

10hdx : 10 Mbps, half duplex

10fdx : 10 Mbps, full duplex

100hdx : 100 Mbps, half duplex

100fdx : 100 Mbps, full duplex

1000fdx : 1 Gbps, full duplex

(default: Show configured and current mode)

Default Setting:

Auto

Example:

Set 10Mbps (half duplex) speed for port1

```
NS3502-8P-2T-2S-V2:/>port mode 1 10hdx
```

Port Flow Control

Description:

Set or show the port flow control mode.

Syntax:

Port Flow Control [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable flow control
disable : Disable flow control
(default: Show flow control mode)

Default Setting:

Disable

Example:

Enable flow control function for port1

```
NS3502-8P-2T-2S-V2:/>port flow control 1 enable
```

Port State

Description:

Set or show the port administrative state.

Syntax:

Port State [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable port
disable : Disable port
(default: Show administrative mode)

Default Setting:

Enable

Example:

Disable port1

```
NS3502-8P-2T-2S-V2:/>port state 1 disable
```

Port Maximum Frame

Description:

Set or show the port maximum frame size.

Syntax:

Port MaxFrame [<port_list>] [<max_frame>]

Parameters:

<port_list>: Port list or 'all', default: All ports
<max_frame>: Port maximum frame size (1518-9600), default: Show maximum frame size

Default Setting:

9600

Example:

Set 2048 frame size for port1

```
NS3502-8P-2T-2S-V2:/>port maxframe 1 2048
```

Port Power

Description:

Set or show the port PHY power mode.

Syntax:

Port Power [<port_list>] [enable|disable|actiphy|dynamic]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable all power control
disable: Disable all power control
actiphy: Enable ActiPHY power control
dynamic: Enable Dynamic power control

Default Setting:

disable

Example:

Disable port power function for port1-4

```
NS3502-8P-2T-2S-V2:/>port power 1-4 enable
```

Port Excessive

Description:

Set or show the port excessive collision mode.

Syntax:

Port Excessive [<port_list>] [discard|restart]

Parameters:

<port_list>: Port list or 'all', default: All ports
discard : Discard frame after 16 collisions
restart : Restart backoff algorithm after 16 collisions
(default: Show mode)

Default Setting:

Discard

Example:

```
NS3502-8P-2T-2S-V2:/>port excessive 1 restart
```

Port Statistics

Description:

Show port statistics.

Syntax:

Port Statistics [<port_list>] [<command>] [up|down]

Parameters:

<port_list>: Port list or 'all', default: All ports
<command> : The command parameter takes the following values:
clear : Clear port statistics
packets : Show packet statistics
bytes : Show byte statistics
errors : Show error statistics
discards : Show discard statistics
filtered : Show filtered statistics
0..7 : Show priority statistics

(default: Show all port statistics)
up : Show ports, which are up
down : Show ports, which are down
(default: Show all ports)

Port VeriPHY

Description:
Run cable diagnostics.
Syntax:
Port VeriPHY [<port_list>]
Parameters:
<port_list>: Port list or 'all', default: All ports

Port SFP

Description:
Show SFP port information.
Syntax:
Port SFP [<port_list>]
Parameters:
<port_list>: Port list or 'all', default: All ports
Example:
Show SFP information for port9-10

```
NS3502-8P-2T-2S-V2:/>port sfp

Port  Type          Speed     Wave Length(nm)  Distance(m)
----  --------------        --------       ---------------       -----------
9    1000Base-LX    1000-Base    1310           10000
10    1000Base-LX    1000-Base    1310           10000
```

Port Description

Description:
Set or show Port Description.
Syntax:
Port Description [<port_list>] [<descr_text>]
Parameters:
<port_list> : Port list or 'all', default: All ports
<descr_text>: Text of port description

MAC Address Table Command

MAC Configuration

Description:
Show MAC address table configuration.

Syntax:

MAC Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show Mac address state

```
NS3502-8P-2T-2S-V2:/>mac configuration

MAC Configuration:
==================

MAC Address    : 9c-f6-1a-03-1c-48
MAC Age Time: 300

Port  Learning
----  --------
1     Auto
2     Auto
3     Auto
4     Auto
5     Auto
6     Auto
7     Auto
8     Auto
9     Auto
10    Auto
```

MAC Add

Description:

Add MAC address table entry.

Syntax:

MAC Add <mac_addr> <port_list> [<vid>]

Parameters:

<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)

<port_list>: Port list or 'all' or 'none'

<vid> : VLAN ID (1-4095), default: 1

Example:

Add Mac address 00-30-4F-01-01-02 in port1 and vid1

```
NS3502-8P-2T-2S-V2:/>mac add 9c-f6-1a-03-1c-48 1 1
```

MAC Delete

Description:

Delete MAC address entry.

Syntax:

MAC Delete <mac_addr> [<vid>]

Parameters:

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

<vid> : VLAN ID (1-4095), default: 1

Example:

Delete Mac address 00-30-4F-a1-01-d2 in vid1

```
NS3502-8P-2T-2S-V2:/>mac delete 33-33-4F-a1-01-d2
```

MAC Lookup

Description:

Lookup MAC address entry.

Syntax:

MAC Lookup <mac_addr> [<vid>]

Parameters:

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

<vid> : VLAN ID (1-4095), default: 1

Example:

Lookup state of Mac address **00-30-4F-a1-01-d2**

```
NS3502-8P-2T-2S-V2:/>mac lookup 33-33-4F-a1-01-d2
```

MAC Age Time

Description:

Set or show the MAC address age timer.

Syntax:

MAC Agetime [<age_time>]

Parameters:

<age_time>: MAC address age time (0,10-1000000) 0=disable,
(default: Show age time)

Default Setting:

300

Example:

Set agetime value in 30

```
NS3502-8P-2T-2S-V2:/>mac agetime 30
```

MAC Learning

Description:

Set or show the port learn mode.

Syntax:

MAC Learning [<port_list>] [auto|disable|secure]

Parameters:

<port_list>: Port list or 'all', default: All ports

auto : Automatic learning

disable: Disable learning

secure : Secure learning

(default: Show learn mode)

Default Setting:

Auto

Example:

Set secure learning mode in port1

```
NS3502-8P-2T-2S-V2:/>mac learning 1 secure
```

MAC Dump

Description:

Show sorted list of MAC address entries.

Syntax:

MAC Dump [<mac_max>] [<mac_addr>] [<vid>]

Parameters:

<mac_max> : Maximum number of MAC addresses 1-8192, default: Show all addresses

<mac_addr>: First MAC address (xx-xx-xx-xx-xx-xx), default: MAC address zero

<vid> : First VLAN ID (1-4095), default: 1

Example:

Show all of MAC table

```
NS3502-8P-2T-2S-V2:/>mac dump
Type    VID  MAC Address       Ports
------  ---  ----------------  -----
Static  1    00-30-4F-a6-34-9d  None,CPU
Dynamic 1    33-33-4F-a1-01-d2 1
Static  1    33-33-00-00-00-01  1,2,4-10,CPU
Static  1    33-33-00-00-00-02  1,2,4-10,CPU
Static  1    33-33-ff-16-81-68  1,2,4-10,CPU
Static  1    33-33-ff-a8-00-64  1,2,4-10,CPU
Static  1    ff-ff-ff-ff-ff-ff  1-10,CPU
NS3502-8P-2T-2S-V2:/>
```

MAC Statistics

Description:

Show MAC address table statistics.

Syntax:

MAC Statistics [<port_list>]

Parameters:

<port_list>: Port list or 'all',
(default: All ports)

Example:

Set all of MAC statistics

```
NS3502-8P-2T-2S-V2:/>mac statistics
Port  Dynamic Addresses
----  ----------------
1     1
2     0
3     0
4     0
5     0
6     0
7     0
```

```
8     0
9     0
10    0

Total Dynamic Addresses: 1
Total Static Addresses : 6
NS3502-8P-2T-2S-V2:/>
```

MAC Flush

Description:

Flush all learned entries.

Syntax:

MAC Flush

VLAN Configuration Command

VLAN Configuration

Description:

Show VLAN configuration.

Syntax:

VLAN Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all',
(default: All ports)

Example:

Show VLAN status of port1

```
NS3502-8P-2T-2S-V2:/>vlan configuration 1

VLAN Configuration:
====================


Mode : IEEE 802.1Q
Port  PVID  IngrFilter  FrameType   LinkType  Q-in-Q Mode  Eth type
----  ----  ----------  ----------  --------  -----------  --------
1     1     Disabled    All         UnTag     Disable      N/A

VID   VLAN Name                      Ports
----  ------------------------------  -----
1     default                         1-10

VID   VLAN Name                      Ports
----  ------------------------------  -----
VLAN forbidden table is empty
```

VLAV PVID

Description:

Set or show the port VLAN ID.

Syntax:

VLAN PVID [<port_list>] [<vid>|none]

Parameters:

<port_list>: Port list or 'all', default: All ports

<vid>|none : Port VLAN ID (1-4095) or 'none',

(default: Show port VLAN ID)

Default Setting:

1

Example:

Set PVID2 for port10

```
NS3502-8P-2T-2S-V2:/>vlan pvid 10 2
```

VLAN Frame Type

Description:

Set or show the port VLAN frame type.

Syntax:

VLAN FrameType [<port_list>] [all|tagged]

Parameters:

<port_list>: Port list or 'all', default: All ports

all : Allow tagged and untagged frames

tagged : Allow tagged frames only

(default: Show accepted frame types)

Default Setting:

All

Example:

Set port10 that allow tagged frames only

```
NS3502-8P-2T-2S-V2:/>vlan frametype 10 tagged
```

VLAN Ingress Filter

Description:

Set or show the port VLAN ingress filter.

Syntax:

VLAN IngressFilter [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable VLAN ingress filtering

disable : Disable VLAN ingress filtering

(default: Show VLAN ingress filtering)

Default Setting:

Disable

Example:

Enable VLAN ingress filtering for port10

```
NS3502-8P-2T-2S-V2:/>vlan ingressfilter 10 enable
```

VLAN Mode

Description:

Set or show the VLAN Mode.

Syntax:

VLAN Mode [portbased|dot1q]

Parameters:

portbased : Port-Based VLAN Mode
dot1q : 802.1Q VLAN Mode
(default: Show VLAN Mode)

Default Setting:

IEEE 802.1Q

Example:

Set VLAN mode in port base

```
NS3502-8P-2T-2S-V2:/>vlan mode portbased
```

VLAN Link Type

Description:

Set or show the port VLAN link type.

Syntax:

VLAN LinkType [<port_list>] [untagged|tagged]

Parameters:

<port_list>: Port list or 'all', default: All ports
untagged : VLAN Link Type Tagged
tagged : VLAN Link Type Untagged
(default: Show VLAN link type)

Default Setting:

Un-tagged

Example:

Enable tagged frame for port2

```
NS3502-8P-2T-2S-V2:/>vlan linktype 2 tagged
```

VLAN Q-in-Q Mode

Description:

Set or show the port Q-in-Q mode.

Syntax:

VLAN QinQ [<port_list>] [disable|man|customer]

Parameters:

<port_list>: Port list or 'all', default: All ports
disable : Disable Q-in-Q VLAN Mode
man : Q-in-Q MAN Port Mode
customer : Q-in-Q Customer Port Mode
(default: Show VLAN QinQ Mode)

Example:

Set port2 in man port

```
NS3502-8P-2T-2S-V2:/>vlan qinq 2 man
```

VLAN Ethernet Type

Description:

Set or show out layer VLAN tag ether type in Q-in-Q VLAN mode.

Syntax:

VLAN Ethtype [<port_list>] [man|dot1q]

Parameters:

<port_list>: Port list or 'all', default: All ports

man : Set out layer VLAN tag ether type : MAN

dot1q : Set out layer VLAN tag ether type : 802.1Q

(default: Show VLAN out layer VLAN tag ether type)

Default Setting:

N/A

Example:

Set out layer VLAN tag Ethernet type for port 10 in man Ethernet type

```
NS3502-8P-2T-2S-V2:/>vlan ethtype 10 man
```

VLAN untagVID

Description:

Set or show the port untagVLAN ID.

Syntax:

VLAN untagVID [<port_list>] [<untagvid>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<untagvid> : Port VLAN ID (0-4095) or 'none', default: Show port VLAN ID

If Untag VID = 0 ,then disable untag VID function.

Default Setting:

N/A

VLAN Add

Description:

Add or modify VLAN entry.

Syntax:

VLAN Add <vid>|<name> [<port_list>]

Parameters:

<vid>|<name>: VLAN ID (1-4095) or VLAN Name

<port_list> : Port list or 'all', default: All ports

Default Setting:

1

Example:

Add port1 to port4 in VLAN10

```
NS3502-8P-2T-2S-V2:/>vlan add 10 1-4
```

VLAN Forbidden Add

Description:

Add or modify VLAN entry in forbidden table.

Syntax:

VLAN Forbidden Add <vid>|<name> [<port_list>]

Parameters:

<vid>|<name>: VLAN ID (1-4095) or VLAN Name

<port_list> : Port list or 'all', default: All ports

Example:

Forbidden add port1 to port4 in VLAN10

```
NS3502-8P-2T-2S-V2:/>vlan forbidden add 10 1-4
```

VLAN Delete

Description:

Delete VLAN entry.

Syntax:

VLAN Delete <vid>|<name>

Parameters:

<vid>|<name>: VLAN ID (1-4095) or VLAN Name

Example:

Delete VLAN10

```
NS3502-8P-2T-2S-V2:/>vlan delete 10
```

VLAN Forbidden Delete

Description:

Delete VLAN entry.

Syntax:

LAN Forbidden Delete <vid>|<name>

Parameters:

<vid>|<name>: VLAN ID (1-4095) or VLAN Name

Example:

Forbidden delete VLAN10

```
NS3502-8P-2T-2S-V2:/>vlan forbidden delete 10
```

VLAN Forbidden Lookup

Description:

Lookup VLAN Forbidden port entry.

Syntax:

VLAN Forbidden Lookup [<vid>] [(name <name>)]

Parameters:

<vid> : VLAN ID (1-4095), default: Show all VLANs

name : VLAN name string

<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alpha characters or numbers.

VLAN name should contain at least one alpha character.

VLAN Lookup

Description:

Lookup VLAN entry.

Syntax:

VLAN Lookup [<vid>] [(name <name>)] [combined|static|nas|mvr|voice_vlan|all]

Parameters:

<vid> : VLAN ID (1-4095), default: Show all VLANs

name : VLAN name string

<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alpha characters or numbers.

VLAN name should contain at least one alpha character.

combined : Shows All the Combined VLAN database

static : Shows the VLAN entries configured by the administrator

nas : Shows the VLANs configured by NAS

mvr : Shows the VLANs configured by MVR

voice_vlan : Shows the VLANs configured by Voice VLAN

all : Shows all VLANs configuration

(default: combined VLAN Users configuration)

Example:

Show VLAN status

```
NS3502-8P-2T-2S-V2:/>vlan lookup

VID   VLAN Name                       Ports
----  -------------------------------  -----
1     default                          1-10
```

VLAN Name Add

Description:

Add VLAN Name to a VLAN ID Mapping.

Syntax:

VLAN Name Add <name> <vid>

Parameters:

<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alpha characters or numbers.

VLAN name should contain at least one alpha character.

<vid> : VLAN ID (1-4095)

Example:

Add VLAN name for VLAN 1

```
NS3502-8P-2T-2S-V2:/>vlan name add test 1
```

VLAN Name Delete

Description:

Delete VLAN Name to VLAN ID Mapping.

Syntax:

VLAN Name Delete <name>

Parameters:

<name>: VLAN name - Maximum of 32 characters. VLAN Name can only

contain alphas or numbers. VLAN name should contain at least one alpha character.

Example:

Delete VLAN name

```
NS3502-8P-2T-2S-V2:/>vlan name delete test
```

VLAN Name Lookup

Description:

Show VLAN Name table.

Syntax:

VLAN Name Lookup [<name>]

Parameters:

<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alpha characters or numbers. VLAN name should contain at least one alpha character.

Example:

To show VLAN Name table

```
NS3502-8P-2T-2S-V2:/>vlan name lookup
VLAN NAME                       vid
------------------------------  ---
test                            1
```

VLAN Status

Description:

VLAN Port Configuration Status.

Syntax:

VLAN Status [<port_list>] [combined|static|nas|mvr|voice_vlan|mstp|all|conflicts]

Parameters:

<port_list>: Port list or 'all', default: All ports
combined : combined VLAN Users configuration
static : static port configuration
nas : NAS port configuration
mvr : MVR port configuration
voice_vlan : Voice VLAN port configuration
mstp : MSTP port configuration
all : All VLAN Users configuration
(default: combined VLAN Users configuration)

Default Setting:

Promiscous

Example:

Show VLAN configuration of port10

```
NS3502-8P-2T-2S-V2:/>status 1

Port  VLAN User    PortType      PVID  Frame Type  Ing Filter   Tx Tag
UVID   Conflicts
----  ------------  -------------  ----  ----------  -----------  -----------  -----  ---------
1     Static      Unaware       1     All         Disabled     Untag This   1
```

```
    NAS                                                    No
    MVR                                                    No
    Voice VLAN                                               No
    MSTP                                                   No
    Combined    Unaware      1    All       Disabled    Untag This   1
No
```

Private VLAN Configuration Command

PVLAN Configuration

Description:

Show Private VLAN configuration.

Syntax:

PVLAN Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show private VLAN configuration

```
NS3502-8P-2T-2S-V2:/> pvlan configuration

Private VLAN Configuration:
===========================


Port  Isolation
----  ---------
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
9     Disabled
10    Disabled

PVLAN ID  Ports
--------  -----
1         1-10
```

PVLAN Add

Description:

Add or modify Private VLAN entry.

Syntax:

PVLAN Add <pvlan_id> [<port_list>]

Parameters:

<pvlan_id> : Private VLAN ID. The allowed range for a Private VLAN ID is the same as the switch port number range.

<port_list>: Port list or 'all', default: All ports

Example:

Add port1 to port4 in PVLAN10

```
NS3502-8P-2T-2S-V2:/>pvlan add 10 1-4
```

PVLAN Delete

Description:

Delete Private VLAN entry.

Syntax:

PVLAN Delete <pvlan_id>

Parameters:

<pvlan_id>: Private VLAN ID. The allowed range for a Private VLAN ID is the same as the switch port number range.

Example:

Delete PVLAN10

```
NS3502-8P-2T-2S-V2:/>pvlan delete 10
```

PVLAN Lookup

Description:

Lookup Private VLAN entry.

Syntax:

PVLAN Lookup [<pvlan_id>]

Parameters:

<pvlan_id>: Private VLAN ID, default: Show all PVLANs. The allowed range for a Private VLAN ID is the same as the switch port number range.

Example:

Lookup PVLAN

```
NS3502-8P-2T-2S-V2:/>pvlan lookup

PVLAN ID  Ports
--------  -----
1         1-10
```

PVLAN Isolate

Description:

Set or show the port isolation mode.

Syntax:

PVLAN Isolate [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port isolation

disable : Disable port isolation

(default: Show port isolation port list)

Default Setting:

disable

Example:

Enable isolate for port10

```
NS3502-8P-2T-2S-V2:/>pvlan isolate 10 enable
```

Security Command

Security Switch User Configuration

Description:

Show users configuration.

Syntax:

Security Switch Users Configuration

Default Setting:

User Name	Privilege
admin	15

Example:

Show users configuration

```
NS3502-8P-2T-2S-V2:/>security switch user configuration

Users Configuration:
====================

User Name                       Privilege Level
------------------------------  ---------------
admin                           15
```

Security Switch User Add

Description:

Add or modify users entry.

Syntax:

Security Switch Users Add <user_name> <password> <privilege_level>

Parameters:

<user_name> : A string identifying the user name that this entry should belong to. The allowed string length is (1-32). The valid user name is a combination of letters, numbers, and underscores

<password> : The password for this user name. The allowed string length is (0-32). Use 'clear' or "" as null string

<privilege_level>: User privilege level (1-15)

Example:

Add new user: username: test, password: test & privilege: 10

```
NS3502-8P-2T-2S-V2:/>security switch users add test test 10
```

Security Switch User Delete

Description:

Delete users entry.

Syntax:

Security Switch Users Delete <user_name>

Parameters:

<user_name>: A string identifying the user name that this entry should belong to. The allowed string length is (1-32). The valid user name is a combination of letters, numbers, and underscores

Example:

Delete test account.

```
NS3502-8P-2T-2S-V2:/>security switch users delete user
```

Security Switch Privilege Level Configuration

Description:

Show privilege configuration.

Syntax:

Security Switch Privilege Level Configuration

Security Switch Privilege Level Group

Description:

Configure a privilege level group.

Syntax:

Security Switch Privilege Level Group <group_name> [<cro>] [<crw>] [<sro>] [<srw>]

Parameters:

<group_name>: Privilege group name
<cro> : Configuration read-only privilege level (1-15)
<crw> : Configuration/Execute read-write privilege level (1-15)
<sro> : Status/Statistics read-only privilege level (1-15)
<srw> : Status/Statistics read-write privilege level (1-15)

Example:

Change privilege level of MVR group.

```
NS3502-8P-2T-2S-V2:/>security switch privilege level group mvr 15 15 15 15
```

Security Switch Privilege Level Current

Description:

Show the current privilege level.

Syntax:

Security Switch Privilege Level Current

Default Setting:
15

Security Switch Auth Configuration

Description:
Show Auth configuration.
Syntax:
Security Switch Auth Configuration
Example:
Show authentication configuration.

```
NS3502-8P-2T-2S-V2:/>security switch auth configuration

Auth Configuration:
===================

Client   Authentication Method   Local Authentication Fallback
-------  ---------------------  -----------------------------
console  local                  Disabled
telnet   local                  Disabled
ssh      local                  Disabled
web      local                  Disabled
```

Security Switch Auth Method

Description:
Set or show Auth method. (default: Show Auth method).
Syntax:
Security Switch Auth Method [console|telnet|ssh|web] [none|local|radius|tacacs+] [enable|disable]
Parameters:
console : Settings for console
telnet : Settings for telnet
ssh : Settings for ssh
web : Settings for web
(default: Set or show the specific client authentication method)
none : Authentication disabled
local : Use local authentication
radius : Use remote RADIUS authentication
tacacs+ : Use remote TACACS+ authentication
(default: Show client authentication method)
enable : Enable local authentication if remote authentication fails
disable : Disable local authentication if remote authentication fails
(The parameter is effective when it is typed)
Default Setting:
disable
Example:
Use RADIUS authentication method for telnet.

```
NS3502-8P-2T-2S-V2:/>security switch auth method telnet radius enable
```

Security Switch SSH Configuration

Description:

Show SSH configuration.

Syntax:

Security Switch SSH Configuration

Example:

Show SSH configuration.

```
NS3502-8P-2T-2S-V2:/>security switch ssh configuration

SSH Configuration:
==================

SSH Mode : Enable
```

Security Switch SSH Mode

Description:

Set or show the SSH mode.

Syntax:

Security Switch SSH Mode [enable|disable]

Parameters:

enable : Enable SSH
disable: Disable SSH
(default: Show SSH mode)

Default Setting:

enable

Example:

Enable SSH function.

```
NS3502-8P-2T-2S-V2:/>security switch ssh mode enable
```

Security Switch HTTPs Configuration

Description:

Show HTTPS configuration.

Syntax:

Security Switch HTTPS Configuration

Example:

Show HTTPs configuration.

```
NS3502-8P-2T-2S-V2:/>security switch https configuration

HTTPS Configuration:
====================

HTTPS Mode         : Enable
HTTPS Redirect Mode : Disabled
```

Security Switch HTTPs Mode

Description:

Set or show the HTTPS mode.

Syntax:

Security Switch HTTPS Mode [enable|disable]

Parameters:

enable : Enable HTTPs
disable: Disable HTTPs
(default: Show HTTPs mode)

Default Setting:

Enable

Example:

Enable HTTPs function.

```
NS3502-8P-2T-2S-V2:/>security switch https mode enable
```

Security Switch HTTPs Redirect

Description:

Set or show the HTTPS redirect mode.
Automatic redirect web browser to HTTPS during HTTPS mode enabled.

Syntax:

Security Switch HTTPS Redirect [enable|disable]

Parameters:

enable : Enable HTTPs redirect
disable: Disable HTTPs redirect
(default: Show HTTPs redirect mode)

Default Setting:

disable

Example:

Enable HTTPs redirect function.

```
NS3502-8P-2T-2S-V2:/>security switch https redirect enable
```

Security Switch Access Configuration

Description:

Show access management configuration.

Syntax:

Security Switch Access Configuration

Example:

Show access management configuration.

```
NS3502-8P-2T-2S-V2:/>security switch access configuration

Access Mgmt Configuration:
==========================

System Access Mode : Disabled
System Access number of entries: 0
```

Security Switch Access Mode

Description:

Set or show the access management mode.

Syntax:

Security Switch Access Mode [enable|disable]

Parameters:

enable : Enable access management
disable: Disable access management
(default: Show access management mode)

Default Setting:

disable

Example:

Enable access management function.

```
NS3502-8P-2T-2S-V2:/>security switch access mode enable
```

Security Switch Access Add

Description:

Add access management entry, default: Add all supported protocols.

Syntax:

Security Switch Access Add <access_id> <start_ip_addr> <end_ip_addr> [web] [snmp] [telnet]

Parameters:

<access_id> : entry index (1-16)
<start_ip_addr>: Start IP address (a.b.c.d)
<end_ip_addr> : End IP address (a.b.c.d)
web : Indicates that the host can access the switch from HTTP/HTTPS
snmp : Indicates that the host can access the switch from SNMP
telnet : Indicates that the host can access the switch from TELNET/SSH

Example:

Add access management list from 192.168.0.1 to 192.168.0.200 via web interface.

```
NS3502-8P-2T-2S-V2:/>security switch access add 1 192.168.0.1
192.168.0.200 web
```

Security Switch Access IPv6 Add

Description:

Add access management IPv6 entry, default: Add all supported protocols.

Syntax:

Security Switch Access Ipv6 Add <access_id> <start_ipv6_addr> <end_ipv6_addr> [web] [snmp] [telnet]

Parameters:

<access_id> : entry index (1-16)
<start_ipv6_addr>: Start 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 only appear

once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

<end_ipv6_addr> : End 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 only appear once. It also uses a following legally IPv4 address. For example,'::192.1.2.34'.

web : Indicates that the host can access the switch from HTTP/HTTPS
snmp : Indicates that the host can access the switch from SNMP
telnet : Indicates that the host can access the switch from TELNET/SSH

Example:
Add access management list from 2001::0001 to 2001::0100 via web interface.

```
NS3502-8P-2T-2S-V2:/> security switch access add 2001::0001 2001::0100 web
```

Security Switch Access Delete

Description:
Delete access management entry.
Syntax:
Security Switch Access Delete <access_id>
Parameters:
<access_id>: entry index (1-16)
Example:
Delete access management ID 1

```
NS3502-8P-2T-2S-V2:/>security switch access delete 1
```

Security Switch Access Lookup

Description:
Lookup access management entry.
Syntax:
Security Switch Access Lookup [<access_id>]
Parameters:
<access_id> : entry index (1-16)
Example:
Lookup access management entry.

```
NS3502-8P-2T-2S-V2:/>security switch access lookup 1
```

Security Switch Access Clear

Description:
Clear access management entry.
Syntax:
Security Switch Access Clear

Example:

Clear access management entry.

```
NS3502-8P-2T-2S-V2:/>security switch access clear
```

Security Switch Access Statistics

Description:

Show or clear access management statistics.

Syntax:

Security Switch Access Statistics [clear]

Parameters:

clear: Clear access management statistics

Example:

Show access management statistics.

```
NS3502-8P-2T-2S-V2:/>security switch access statistics

Access Management Statistics:
-----------------------------
HTTP     Receive:        0    Allow:        0    Discard:        0
HTTPS    Receive:        0    Allow:        0    Discard:        0
SNMP     Receive:        0    Allow:        0    Discard:        0
TELNET   Receive:        0    Allow:        0    Discard:        0
SSH      Receive:        0    Allow:        0    Discard:        0
```

Security Switch SNMP Configuration

Description:

Show SNMP configuration.

Syntax:

Security Switch SNMP Configuration

Security Switch SNMP Mode

Description:

Set or show the SNMP mode.

Syntax:

Security Switch SNMP Mode [enable|disable]

Parameters:

enable : Enable SNMP

disable: Disable SNMP

(default: Show SNMP mode)

Default Setting:

enable

Example:

Disable SNMP mode.

```
NS3502-8P-2T-2S-V2:/>security switch snmp mode disable
```

Security Switch SNMP Version

Description:

Set or show the SNMP protocol version.

Syntax:

Security Switch SNMP Version [1|2c|3]

Parameters:

1 : SNMP version 1
2c: SNMP version 2c
3 : SNMP version 3
(default: Show SNMP version)

Default Setting:

2c

Example:

Set SNMP in version 3.

```
NS3502-8P-2T-2S-V2:/>security switch snmp version 3
```

Security Switch SNMP Read Community

Description:

Set or show the community string for SNMP read access.

Syntax:

Security Switch SNMP Read Community [<community>]

Parameters:

<community>: Community string. Use 'clear' or "" to clear the string
(default: Show SNMP read community)

Default Setting:

public

Example:

Set SNMP read community private.

```
NS3502-8P-2T-2S-V2:/>security switch snmp read community private
```

Security Switch SNMP Write Community

Description:

Set or show the community string for SNMP write access.

Syntax:

Security Switch SNMP Write Community [<community>]

Parameters:

<community>: Community string. Use 'clear' or "" to clear the string
(default: Show SNMP write community)

Default Setting:

private

Example:

Set public value in SNMP write community.

```
NS3502-8P-2T-2S-V2:/>security switch snmp write community public
```

Security Switch SNMP Trap Mode

Description:

Set or show the SNMP trap mode.

Syntax:

Security Switch SNMP Trap Mode [enable|disable]

Parameters:

enable : Enable SNMP traps
disable: Disable SNMP traps
(default: Show SNMP trap mode)

Default Setting:

disable

Example:

Enable SNMP trap mode.

```
NS3502-8P-2T-2S-V2:/>security switch snmp trap mode enable
```

Security Switch SNMP Trap Version

Description:

Set or show the SNMP trap protocol version.

Syntax:

Security Switch SNMP Trap Version [1|2c|3]

Parameters:

1 : SNMP version 1
2c: SNMP version 2c
3 : SNMP version 3
(default: Show SNMP trap version)

Default Setting:

1

Example:

Set SNMP trap version in version 2c.

```
NS3502-8P-2T-2S-V2:/>security switch snmp trap version 2c
```

Security Switch SNMP Trap Community

Description:

Set or show the community string for SNMP traps.

Syntax:

Security Switch SNMP Trap Community [<community>]

Parameters:

<community>: Community string. Use 'clear' or "" to clear the string
(default: Show SNMP trap community)

Default Setting:

public

Example:

Set private value for SNMP trap community.

```
NS3502-8P-2T-2S-V2:/>security switch snmp trap community private
```

Security Switch SNMP Trap Destination

Description:

Set or Show the SNMP trap destination address.

Syntax:

Security Switch SNMP Trap Destination [<ip_addr_string>]

Parameters:

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

Example:

Set SNMP trap destination address for 192.168.0.20

```
NS3502-8P-2T-2S-V2:/>security switch snmp trap destination 192.168.0.20
```

Security Switch SNMP Trap IPv6 Destination

Description:

Set or Show the SNMP trap destination IPv6 address.

Syntax:

Security Switch SNMP Trap IPv6 Destination [<ipv6_addr>]

Parameters:

<ipv6_addr>: 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, 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 only appear once. It also uses a following legally IPv4 address. For example,'::192.1.2.34'.

Example:

Set SNMP trap IPv6 destination address for 2001::0001

```
NS3502-8P-2T-2S-V2:/>security switch snmp trap ipv6 destination
2001::0001
```

Security Switch SNMP Trap Authentication Failure

Description:

Set or show the SNMP authentication failure trap mode.

Syntax:

Security Switch SNMP Trap Authentication Failure [enable|disable]

Parameters:

enable : Enable SNMP trap authentication failure

disable: Disable SNMP trap authentication failure

(default: Show SNMP trap authentication failure mode)

Default Setting:

enable

Example:

Disable SNMP trap authentication failure

```
NS3502-8P-2T-2S-V2:/>security switch snmp trap authentication failure
disable
```

Security Switch SNMP Trap Link-up

Description:

Set or show the port link-up and link-down trap mode.

Syntax:

Security Switch SNMP Trap Link-up [enable|disable]

Parameters:

enable : Enable SNMP trap link-up and link-down

disable: Disable SNMP trap link-up and link-down

(default: Show SNMP trap link-up and link-down mode)

Default Setting:

enable

Example:

Disable SNMP trap link-up

```
NS3502-8P-2T-2S-V2:/>security switch snmp trap link-up disable
```

Security Switch SNMP Trap Inform Mode

Description:

Set or show the SNMP trap inform mode.

Syntax:

Security Switch SNMP Trap Inform Mode [enable|disable]

Parameters:

enable : Enable SNMP trap inform

disable: Disable SNMP trap inform

(default: Show SNMP inform mode)

Default Setting:

enable

Example:

Disable SNMP trap inform mode.

```
NS3502-8P-2T-2S-V2:/>security switch snmp trap inform mode disable
```

Security Switch SNMP Trap Inform Timeout

Description:

Set or show the SNMP trap inform timeout (usecs).

Syntax:

Security Switch SNMP Trap Inform Timeout [<timeout>]

Parameters:

<timeout>: SNMP trap inform timeout (0-2147 seconds)

(default: Show SNMP trap inform timeout)

Default Setting:

1

Example:

Set SNMP trap inform timeout in 20sec.

```
NS3502-8P-2T-2S-V2:/>security switch snmp trap inform timeout 20
```

Security Switch SNMP Trap Inform Retry Times

Description:

Set or show the SNMP trap inform retry times.

Syntax:

Security Switch SNMP Trap Inform Retry Times [<retries>]

Parameters:

<retries>: SNMP trap inform retransmited times (0-255)
(default: Show SNMP trap inform retry times)

Default Setting:

5

Example:

Set SNMP trap inform retry times in 10.

```
NS3502-8P-2T-2S-V2:/>security switch snmp trap inform retry times 10
```

Security Switch SNMP Trap Probe Security Engine ID

Description:

Show SNMP trap security engine ID probe mode.

Syntax:

Security Switch SNMP Trap Probe Security Engine ID [enable|disable]

Parameters:

enable : Enable SNMP trap security engine ID probe
disable: Disable SNMP trap security engine ID probe
(default: Show SNMP trap security engine ID probe mode)

Default Setting:

enable

Example:

Disable SNMP trap probe security engine ID

```
NS3502-8P-2T-2S-V2:/>security switch snmp trap probe security engine id disable
```

Security Switch SNMP Trap Security Engine ID

Description:

Set or show SNMP trap security engine ID.

Syntax:

Security Switch SNMP Trap Security Engine ID [<engineid>]

Parameters:

<engineid>: Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

Example:

Set the SNMP trap security engine ID

```
NS3502-8P-2T-2S-V2:/>security switch snmp trap security engine id 800007e5017f000011
```

Security Switch SNMP Trap Security Name

Description:

Set or show SNMP trap security name.

Syntax:

Security Switch SNMP Trap Security Name [<security_name>]

Parameters:

<security_name>: A string representing the security name for a principal (default: Show SNMP trap security name). The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

Example:

Set the SNMP trap security name

```
NS3502-8P-2T-2S-V2:/>security switch snmp trap security name 12345678
```

Security Switch SNMP Engine ID

Description:

Set or show SNMPv3 local engine ID.

Syntax:

Security Switch SNMP Engine ID [<engineid>]

Parameters:

<engineid>: Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

Default Setting:

800007e5017f000001

Example:

Set 800007e5017f000002 for SNMPv3 local engine ID

```
NS3502-8P-2T-2S-V2:/>security switch snmp engine id
800007e5017f000002
```

Security Switch SNMP Community Add

Description:

Add or modify SNMPv3 community entry.

The entry index key is <community>.

Syntax:

Security Switch SNMP Community Add <community> [<ip_addr>] [<ip_mask>]

Parameters:

<community>: Community string

<ip_addr> : IP address (a.b.c.d), default: Show IP address

<ip_mask> : IP subnet mask (a.b.c.d), default: Show IP mask

Example:

Add SNMPv3 community entry.

```
NS3502-8P-2T-2S-V2:/>security switch snmp community add public
192.168.0.20 255.255.255.0
```

Security Switch SNMP Community Delete

Description:

Delete SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 community entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp community delete 3
```

Security Switch SNMP Community Lookup

Description:

Lookup SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 community entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp community lookup
Idx Community                    Source IP       Source Mask
--- ------------------------------          ---------------       ---------------
1   public                       192.168.0.20     255.255.255.0
2   private                       0.0.0.0          0.0.0.0

Number of entries: 2
```

Security Switch SNMP User Add

Description:

Add SNMPv3 user entry.

The entry index key are <engineid> and <user_name> and it doesn't allow modify.

Syntax:

Security Switch SNMP User Add <engineid> <user_name> [MD5|SHA] [<auth_password>] [DES] [<priv_password>]

Parameters:

<engineid> : Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

<user_name> : A string identifying the user name that this entry should belong to. The name of "None" is reserved.

The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

md5 : An optional flag to indicate that this user using MD5 authentication protocol. The allowed length is (8-32), and the allowed content is ASCII characters from 33 to 126

sha : An optional flag to indicate that this user using SHA authentication protocol. The allowed length is (8-40), and the allowed content is ASCII characters from 33 to 126

<auth_password>: A string identifying the authentication pass phrase

des : An optional flag to indicate that this user using DES privacy protocol privacy protocol should belong to.

The allowed string length is (8-32), and the allowed content is ASCII characters from 33 to 126

<priv_password>: A string identifying the privacy pass phrase.

The allowed string length is (8-40), and the allowed content is ASCII characters from 33 to 126

Example:

Add SNMPv3 user entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp user add 800007e5017f000003
admin_snmpv3 md5 12345678 des abcdefgh
```

Security Switch SNMP User Delete

Description:

Delete SNMPv3 user entry.

Syntax:

Security Switch SNMP User Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 user entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp user delete 1
```

Security Switch SNMP User Changekey

Description:

Change SNMPv3 user password.

Syntax:

Security Switch SNMP User Changekey <engineid> <user_name> <auth_password> [<priv_password>]

Parameters:

<engineid> : Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

<user_name> : A string identifying the user name that this entry should belong to. The name of "None" is reserved. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

<auth_password>: A string identifying the authentication pass phrase

<priv_password>: A string identifying the privacy pass phrase.

The allowed string length is (8-40), and the allowed content is ASCII characters from 33 to 126

Example:

Delete SNMPv3 user entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp user changekey
800007e5017f000003 admin_snmpv3 87654321 12345678
```

Security Switch SNMP User Lookup

Description:

Lookup SNMPv3 user entry.

Syntax:

Security Switch SNMP User Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 user entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp user lookup
Idx Engine ID   User Name                       Level         Auth  Priv
--- ---------   ------------------------------  ------------  ----  ----
1   Remote      admin_snmpv3                    Auth, Priv    MD5   DES

Number of entries: 1
```

Security Switch SNMP Group Add

Description:

Add or modify SNMPv3 group entry.

The entry index key are <security_model> and <security_name>.

Syntax:

Security Switch SNMP Group Add <security_model> <security_name> <group_name>

Parameters:

<security_model>: 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 (1-32), 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 (1-32), and the allowed content is ASCII characters from 33 to 126

Example:

Add SNMPv3 group entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp group add usm
admin_snmpv3 group_snmpv3
```

Security Switch SNMP Group Delete

Description:

Delete SNMPv3 group entry.

Syntax:

Security Switch SNMP Group Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 group entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp group delete 1
```

Security Switch SNMP Group Lookup

Description:

Lookup SNMPv3 group entry.

Syntax:

Security Switch SNMP Group Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 group entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp group lookup
Idx Model Security Name                 Group Name
--- ----- -------------------------------- --------------------------------
1   v1    public                        default_ro_group
2   v1    private                       default_rw_group
3   v2c   public                        default_ro_group
4   v2c   private                       default_rw_group
5   usm   default_user                      default_rw_group

Number of entries: 5
```

Security Switch SNMP View Add

Description:

Add or modify SNMPv3 view entry.

The entry index key are <view_name> and <oid_subtree>.

Syntax:

Security Switch SNMP View Add <view_name> [included|excluded] <oid_subtree>

Parameters:

<view_name> : A string identifying the view name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

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

excluded : An optional flag to indicate that this view subtree should excluded

<oid_subtree>: The OID defining the root of the subtree to add to the named view

Example:

Add SNMPv3 view entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp view add snmpv3_view
include .1
```

Security Switch SNMP View Delete

Description:

Delete SNMPv3 view entry.

Syntax:

Security Switch SNMP View Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 view entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp view delete 3
```

Security Switch SNMP View Lookup

Description:

Lookup SNMPv3 view entry.

Syntax:

Security Switch SNMP View Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 view entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp view lookup
Idx  View Name                      View Type  OID Subtree
---  -------------------------------  ---------  --------------------------------
1   default_view                    included    .1
2   snmpv3_viwe                     included    .1

Number of entries: 2
```

Security Switch SNMP Access Add

Description:

Add or modify SNMPv3 access entry.

The entry index key are <group_name>, <security_model> and <security_level>.

Syntax:

Security Switch SNMP Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>]

Parameters:

<group_name> : A string identifying the group name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

<security_model> : any - Accepted any security model (v1|v2c|usm)
v1 - Reserved for SNMPv1
v2c - Reserved for SNMPv2c
usm - User-based Security Model (USM)

<security_level> : noAuthNoPriv - None authentication and none privacy
AuthNoPriv - Authentication and none privacy
AuthPriv - 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 name of "None" is reserved.
The allowed string length is (1-32), 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 name of "None" is reserved.
The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

Example:

Add SNMPv3 access entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp access add group_snmpv3
usm authpriv snmpv3_view snmpv3_view
```

Security Switch SNMP Access Delete

Description:

Delete SNMPv3 access entry.

Syntax:

Security Switch SNMP Access Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 access entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp access delete 3
```

Security Switch SNMP Access Lookup

Description:

Lookup SNMPv3 access entry.

Syntax:

Security Switch SNMP Access Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 access entry

```
NS3502-8P-2T-2S-V2:/>security switch snmp access lookup
Idx Group Name                      Model Level
--- ------------------------------- ----- --------------
1   default_ro_group                any   NoAuth, NoPriv
2   default_rw_group                any   NoAuth, NoPriv

Number of entries: 2
```

Security Switch RMON Statistics Add

Description:

Add or modify RMON Statistics entry. The entry index key is <stats_id>.

Syntax:

Security Switch RMON Statistics Add <stats_id> <data_source>

Parameters:

<stats_id> : Statistics ID (1-65535).

<data_source>: The OID that indicates that the ifIndex in ifEntry.
The value should be like .1.3.6.1.2.1.2.2.1.1.xxx.

Security Switch RMON Statistics Delete

Description:

Delete RMON Statistics entry. The entry index key is <stats_id>.

Syntax:

Security Switch RMON Statistics Delete <stats_id>

Parameters:

<stats_id>: Statistics ID (1-65535).

Security Switch RMON Statistics Lookup

Description:

Show RMON Statistics entries.

Syntax:

Security Switch RMON Statistics Lookup [<stats_id>]

Parameters:

<stats_id>: Statistics ID (1-65535).

Security Switch RMON History Add

Description:

Add or modify RMON Hisotry entry. The entry index key is <history_id>.

Syntax:

Security Switch RMON History Add <history_id> <data_source> [<interval>] [<buckets>]

Parameters:

<history_id> : History ID (1-65535).

<data_source>: The OID that indicates that the ifIndex in ifEntry.

The value should be like .1.3.6.1.2.1.2.2.1.1.xxx.

<interval> : Sampling interval (1-3600) (default: 1800).

<buckets> : The maximum data entries associated this History control entry stored in RMON(1-65535) (default: 50).

Security Switch RMON History Delete

Description:

Delete RMON Hisotry entry. The entry index key is <history_id>.

Syntax:

Security Switch RMON History Delete <history_id>

Parameters:

<history_id> : History ID (1-65535).

Security Switch RMON History Lookup

Description:

Show RMON History entries.

Syntax:

Security Switch RMON History Lookup [<history_id>]

Parameters:

<history_id> : History ID (1-65535).

Security Switch RMON Alarm Add

Description:

Add or modify RMON Alarm entry. The entry index key is <alarm_id>.

Syntax:

Security Switch RMON Alarm Add <alarm_id> <interval> <alarm_vairable> [absolute|delta] <rising_threshold> <rising_event_index> <falling_threshold> <falling_event_index> [rising|falling|both]

Parameters:

<alarm_id> : Alarm ID (1-65535).
<interval> : Sampling interval (1-2147483647) (default: 30).
<alarm_vairable> : The MIB OID that need to be referenced.
.1.3.6.1.2.1.2.2.1.10.xxx – ifInOctets
.1.3.6.1.2.1.2.2.1.11.xxx – ifInUcastPkts
.1.3.6.1.2.1.2.2.1.12.xxx – ifInNUcastPkts
.1.3.6.1.2.1.2.2.1.13.xxx – ifInDiscards
.1.3.6.1.2.1.2.2.1.14.xxx – ifInErrors
.1.3.6.1.2.1.2.2.1.15.xxx – ifInUnkownProtos
.1.3.6.1.2.1.2.2.1.16.xxx – ifOutOctets
.1.3.6.1.2.1.2.2.1.17.xxx – ifOutUcastPkts
.1.3.6.1.2.1.2.2.1.18.xxx – ifOutNUcastPkts
.1.3.6.1.2.1.2.2.1.19.xxx – ifOutDiscards
.1.3.6.1.2.1.2.2.1.20.xxx – ifOutErrors
.1.3.6.1.2.1.2.2.1.21.xxx – ifOutQLen
"xxx" means the interface identified by a particular value of this index is the same interface as identified by the same value of OID 'ifIndex'.
absolute : Get the sample directly.
delta : Calculate the difference between samples (default).
<rising_threshold> : Rising threshold value (-2147483648–2147483647).
<rising_event_index> : Rising event index (1-65535).
<falling_threshold> : Falling threshold value (-2147483648–2147483647).
<falling_event_index>: Falling event index (1-65535).
rising : Trigger alarm when the first value is larger than the rising threshold.
falling : Trigger alarm when the first value is less than the falling threshold.
both : Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default)

Security Switch RMON Alarm Delete

Description:
Delete RMON Alarm entry. The entry index key is <alarm_id>.
Syntax:
Security Switch RMON Alarm Delete <alarm_id>
Parameters:
<alarm_id>: Alarm ID (1-65535).

Security Switch RMON Alarm Lookup

Description:
Show RMON Alarm entries.
Syntax:
Security Switch RMON Alarm Lookup [<alarm_id>]
Parameters:
<alarm_id>: Alarm ID (1-65535).

Security Switch RMON Event Add

Description:

Add or modify RMON Event entry. The entry index key is <event_id>.

Syntax:

Security Switch RMON Event Add <event_id> [none|log|trap|log_trap] [<community>] [<description>]

Parameters:

<event_id> : Event ID (1-65535).

none : Get the sample directly.

log : Get the sample directly.

trap : Get the sample directly.

log_trap : Calculate the difference between samples (default).

<community> : Specify the community when trap is sent (the string lengh is 0~127) (default: public).

<description>: The string for describing this event (the string lengh is 0~127) (default: null string).

Security Switch RMON Event Delete

Description:

Delete RMON Event entry. The entry index key is <event_id>.

Syntax:

Security Switch RMON Event Delete <event_id>

Parameters:

<event_id> : Event ID (1-65535).

Security Switch RMON Event Lookup

Description:

Show RMON Event entries.

Syntax:

Security Switch RMON Event Lookup [<event_id>]

Parameters:

<event_id> : Event ID (1-65535).

Security Network Psec Switch

Description:

Show Port Security status.

Syntax:

Security Network Psec Switch [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show port security status.

```
NS3502-8P-2T-2S-V2:/>security network psec switch
Users:
L = Limit Control
8 = 802.1X
D = DHCP Snooping
```

```
V = Voice VLAN

Port  Users  State          MAC Cnt
----  -----  -------------  -------
1     ----   No users        0
2     ----   No users        0
3     ----   No users        0
4     ----   No users        0
5     ----   No users        0
6     ----   No users        0
7     ----   No users        0
8     ----   No users        0
9     ----   No users        0
10    ----   No users        0
```

Security Network Psec Port

Description:

Show MAC Addresses learned by Port Security.

Syntax:

Security Network Psec Port [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show MAC address learned on port 1

```
NS3502-8P-2T-2S-V2:/>security network psec port 1

Port 1:
-------

MAC Address       VID   State      Added                 Age/Hold Time
-----------------  ----  ----------  -------------------------  -------------
<none>
```

Security Network Limit Configuration

Description:

Show Limit Control configuration.

Syntax:

Security Network Limit Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show Limit Control configuration.

```
NS3502-8P-2T-2S-V2:/>security network limit configuration

Port Security Limit Control Configuration:
==========================================
```

```
Mode     : Disabled
Aging    : Disabled
Age Period: 3600

Port  Mode      Limit  Action
----  --------  -----  ---------------
1     Disabled    4    None
2     Disabled    4    None
3     Disabled    4    None
4     Disabled    4    None
5     Disabled    4    None
6     Disabled    4    None
7     Disabled    4    None
8     Disabled    4    None
9     Disabled    4    None
10    Disabled    4    None
```

Security Network Limit Mode

Description:

Set or show global enabledness.

Syntax:

Security Network Limit Mode [enable|disable]

Parameters:

enable : Globally enable port security

disable : Globally disable port security

(default: Show current global enabledness of port security limit control)

Default Setting:

disable

Example:

Enable the limit mode

```
NS3502-8P-2T-2S-V2:/>security network limit mode enable
```

Security Network Limit Aging

Description:

Set or show aging enabledness.

Syntax:

Security Network Limit Aging [enable|disable]

Parameters:

enable : Enable aging

disable : Disable aging

(default: Show current enabledness of aging)

Default Setting:

disable

Example:

Enable limit aging

```
NS3502-8P-2T-2S-V2:/>security network limit aging enable
```

Security Network Limit Agetime

Description:

Time in seconds between check for activity on learned MAC addresses.

Syntax:

Security Network Limit Agetime [<age_time>]

Parameters:

<age_time>: Time in seconds between checks for activity on a MAC address (10-10000000 seconds)

(default: Show current age time)

Default Setting:

3600

Example:

Set age time in 100sec.

```
NS3502-8P-2T-2S-V2:/>security network limit agetime 100
```

Security Network Limit Port

Description:

Set or show per-port enabledness.

Syntax:

Security Network Limit Port [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port security on this port

disable : Disable port security on this port

(default: Show current port enabledness of port security limit control)

Default Setting:

disable

Example:

Enable port limit for port 1

```
NS3502-8P-2T-2S-V2:/>security network limit port 1 enable
```

Security Network Limit Limit

Description:

Set or show the max. number of MAC addresses that can be learned on this set of ports.

Syntax:

Security Network Limit Limit [<port_list>] [<limit>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<limit> : Max. number of MAC addresses on this port

(default: Show current limit)

Default Setting:

4

Example:

Set limit in 5

```
NS3502-8P-2T-2S-V2:/>security network limit limit 1-10 5
```

Security Network Limit Action

Description:

Set or show the action involved with exceeding the limit.

Syntax:

Security Network Limit Action [<port_list>] [none|trap|shut|trap_shut]

Parameters:

<port_list> : Port list or 'all', default: All ports

none|trap|shut|trap_shut: Action to be taken in case the number of MAC addresses exceeds the limit

none : Don't do anything

trap : Send an SNMP trap

shut : Shutdown the port

trap_shut: Send an SNMP trap and shutdown the port

(default: Show current action)

Default Setting:

none

Example:

Set trap mode for limit action for port 1

```
NS3502-8P-2T-2S-V2:/>security network limit action 1 trap
```

Security Network Limit Reopen

Description:

Reopen one or more ports whose limit is exceeded and shut down.

Syntax:

Security Network Limit Reopen [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Reopen port 1

```
NS3502-8P-2T-2S-V2:/>security network limit reopen 1
```

Security Network NAS Configuration

Description:

Show 802.1X configuration.

Syntax:

Security Network NAS Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show 802.1X configuration of port 1

```
NS3502-8P-2T-2S-V2:/>security network nas configuration 1

802.1X Configuration:
=====================

Mode           : Disabled
Reauth.        : Disabled
```

```
Reauth. Period   : 3600
EAPOL Timeout    : 30
Age Period       : 300
Hold Time        : 10
RADIUS QoS       : Disabled
RADIUS VLAN      : Disabled
Guest VLAN       : Disabled
Guest VLAN ID    : 1
Max. Reauth Count: 2
Allow Guest VLAN if EAPOL Frame Seen: Disabled

Port  Admin State        Port State           Last Source       Last ID
----  -----------------  -------------------  ----------------  -----------------
1     Force Authorized   Globally Disabled    -                 -
```

Security Network NAS Mode

Description:

Set or show the global NAS enabledness.

Syntax:

Security Network NAS Mode [enable|disable]

Parameters:

enable : Globally enable 802.1X

disable: Globally disable 802.1X

(default: Show current 802.1X global enabledness)

Default Setting:

disable

Example:

Enable IEEE802.1X function

```
NS3502-8P-2T-2S-V2:/>security network nas mode enable
```

Security Network NAS State

Description:

Set or show the port security state.

Syntax:

Security Network NAS State [<port_list>] [auto|authorized|unauthorized|single|multi|macbased]

Parameters:

<port_list>: Port list or 'all', default: All ports

auto : Port-based 802.1X Authentication

authorized : Port access is allowed

unauthorized: Port access is not allowed

single : Single Host 802.1X Authentication

multi : Multiple Host 802.1X Authentication

macbased : Switch authenticates on behalf of the client

(default: Show 802.1X state)

Default Setting:

none

Example:

Show the port 1 security state.

```
NS3502-8P-2T-2S-V2:/>security network nas state 1

Port  Admin State        Port State           Last Source       Last ID
----  ------------------ -------------------- ----------------- ------------------
1     Force Authorized   Globally Disabled    -                 -
```

Security Network NAS Reauthentication

Description:

Set or show Reauthentication enabledness.

Syntax:

Security Network NAS Reauthentication [enable|disable]

Parameters:

enable : Enable reauthentication

disable: Disable reauthentication

(default: Show current reauthentication mode)

Default Setting:

disable

Example:

Enable reauthentication function.

```
NS3502-8P-2T-2S-V2:/>security network nas reauthentication enable
```

Security Network NAS ReauthPeriod

Description:

Set or show either global enabledness (use the global keyword) or per-port enabledness of RADIUS-assigned VLAN.

Syntax:

Security Network NAS RADIUS_VLAN [global|<port_list>] [enable|disable]

Parameters:

global : Select the global RADIUS-assigned VLAN setting

<port_list>: Select the per-port RADIUS-assigned VLAN setting

(default: Show current per-port RADIUS-assigned VLAN enabledness)

enable : Enable RADIUS-assigned VLAN either globally or on one or more ports

disable: Disable RADIUS-assigned VLAN either globally or on one or more ports

(default: Show current RADIUS-assigned VLAN enabledness)

Default Setting:

disable

Example:

Enable RADIUS-assigned VLAN.

```
NS3502-8P-2T-2S-V2:/>security network nas radius_vlan enable
```

Security Network NAS EapolTimeout

Description:

Set or show the time between EAPOL retransmissions.

Syntax:

Security Network NAS EapolTimeout [<eapol_timeout>]

Parameters:

<eapol_timeout>: Time between EAPOL retransmissions (1-65535 seconds)
(default: Show current EAPOL retransmission timeout)

Default Setting:

30

Example:

Set the time between EAPOL retransmissions for 100sec.

```
NS3502-8P-2T-2S-V2:/>security network nas eapoltimeout 100
```

Security Network NAS Agetime

Description:

Time in seconds between check for activity on successfully authenticated MAC addresses.

Syntax:

Security Network NAS Agetime [<age_time>]

Parameters:

<age_time>: Time between checks for activitiy on a MAC address that succeeded autentication
(default: Show current age time)

Default Setting:

300

Example:

Set NAS age time in 1000sec

```
NS3502-8P-2T-2S-V2:/>security network nas agetime 1000
```

Security Network NAS Holdtime

Description:

Time in seconds before a MAC-address that failed authentication gets a new authentication chance.

Syntax:

Security Network NAS Holdtime [<hold_time>]

Parameters:

<hold_time>: Hold time before MAC addresses that failed authentication expire
(default: Show current hold time)

Default Setting:

10

Example:

Set NAS hold time in 100sec

```
NS3502-8P-2T-2S-V2:/>security network nas holdtime 100
```

Security Network NAS RADIUS_QoS

Description:

Set or show either global enabledness (use the global keyword) or per-port enabledness of RADIUS-assigned QoS.

Syntax:

Security Network NAS RADIUS_QoS [global|<port_list>] [enable|disable]

Parameters:

global : Select the global RADIUS-assigned QoS setting

<port_list>: Select the per-port RADIUS-assigned QoS setting

(default: Show current per-port RADIUS-assigned QoS enabledness)

enable : Enable RADIUS-assigned QoS either globally or on one or more ports

disable: Disable RADIUS-assigned QoS either globally or on one or more ports

(default: Show current RADIUS-assigned QoS enabledness)

Default Setting:

disable

Example:

Enable NAS RADIUS QoS

```
NS3502-8P-2T-2S-V2:/>security network nas radius_qos enable
```

Security Network NAS RADIUS_VLAN

Description:

Set or show either global enabledness (use the global keyword) or per-port enabledness of RADIUS-assigned VLAN.

Syntax:

Security Network NAS RADIUS_VLAN [global|<port_list>] [enable|disable]

Parameters:

global : Select the global RADIUS-assigned VLAN setting

<port_list>: Select the per-port RADIUS-assigned VLAN setting

(default: Show current per-port RADIUS-assigned VLAN enabledness)

enable : Enable RADIUS-assigned VLAN either globally or on one or more ports

disable: Disable RADIUS-assigned VLAN either globally or on one or more ports

(default: Show current RADIUS-assigned VLAN enabledness)

Default Setting:

disable

Example:

Enable NAS RADIUS VLAN

```
NS3502-8P-2T-2S-V2:/>security network nas radius_vlan enable
```

Security Network NAS Guest_VLAN

Description:

Set or show either global enabledness and parameters (use the global keyword) or per-port enabledness of Guest VLAN

Unless the 'global' keyword is used, the <reauth_max> and <allow_if_eapol_seen> parameters will not be unused..

Syntax:

Security Network NAS Guest_VLAN [global|<port_list>] [enable|disable] [<vid>] [<reauth_max>] [<allow_if_eapol_seen>]

Parameters:

global: Select the global Guest VLAN setting

<port_list>: Select the per-port Guest VLAN setting

(default: Show current per-port Guest VLAN enabledness)

enable|disable: enable : Enable Guest VLAN either globally or on one or more

ports

disable: Disable Guest VLAN either globally or on one or more ports

(default: Show current Guest VLAN enabledness)

<vid>: Guest VLAN ID used when entering the Guest VLAN. Use the 'global' keyword to change it

(default: Show current Guest VLAN ID)

<reauth_max>: The value can only be set if you use the 'global' keyword in the beginning of the command. The number of times a Request Identity EAPOL frame is sent without reasponse before considering entering the Guest VLAN

(default: Show current Maximum Reauth Count value)

<allow_if_eapol_seen>: The value can only be set if you use the 'global' keyword in the beginning of the command.

disable:The Guest VLAN can only be entered if no EAPOL frames have been received on a port for the lifetime of the port

enable :The Guest VLAN can be entered even if an EAPOL frame has been received during the lifetime of the port

(default: Show current setting)

Default Setting:

Disable

Example:

Enable NAS guest VLAN

```
NS3502-8P-2T-2S-V2:/>security network nas guest_vlan enable
```

Security Network NAS Authenticate

Description:

Refresh (restart) 802.1X authentication process.

Syntax:

Security Network NAS Authenticate [<port_list>] [now]

Parameters:

<port_list>: Port list or 'all', default: All ports

now: Force reauthentication immediately

Example:

Start NAS authentication now for port 1.

```
NS3502-8P-2T-2S-V2:/>security network nas authenticate 1 now
```

Security Network NAS Statistics

Description:

Show or clear 802.1X statistics.

Syntax:

Security Network NAS Statistics [<port_list>] [clear|eapol|radius]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear : Clear statistics

eapol : Show EAPOL statistics

radius : Show Backend Server statistics

(default: Show all statistics)

Example:

Show 802.1X statistics in port 1

```
NS3502-8P-2T-2S-V2:/>security network nas statistics 1
Port 1 EAPOL Statistics:

Rx Total:                0   Tx Total:                0
Rx Response/Id:          0   Tx Request/Id:           0
Rx Response:             0   Tx Request:              0
Rx Start:                0
Rx Logoff:               0
Rx Invalid Type:         0
Rx Invalid Length:       0

Port 1 Backend Server Statistics:

Rx Access Challenges:    0   Tx Responses:            0
Rx Other Requests:       0
Rx Auth. Successes:      0
Rx Auth. Failures:       0
```

Security Network ACL Configuration

Description:

Show ACL Configuration.

Syntax:

Security Network ACL Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Security Network ACL Action

Description:

Set or show the ACL port default action.

Syntax:

Security Network ACL Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]

Parameters:

<port_list> : Port list or 'all', default: All ports
permit : Permit forwarding (default)
deny : Deny forwarding
<rate_limiter>: Rate limiter number (1-15) or 'disable'
<port_copy> : Port number for copy of frames or 'disable'
<logging> : System logging of frames: log|log_disable
<shutdown> : Shut down ingress port: shut|shut_disable

Example:

Show ACL action in port 1

```
NS3502-8P-2T-2S-V2:/>security network acl action 1

Port  Action  Rate Limiter  Port Copy  Mirror  Logging  Shutdown
Counter
```

```
---- ------ ------------ --------- -------- -------- -------- -------
1    Permit  Disabled     Disabled   Disabled  Disabled  Disabled  0
```

Security Network ACL Policy

Description:

Set or show the ACL port policy.

Syntax:

Security Network ACL Policy [<port_list>] [<policy>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<policy> : Policy number (1-8)

Default Setting:

1

Example:

Set ACL policy 2 for port 1

```
NS3502-8P-2T-2S-V2:/>security network acl policy 1 2
```

Security Network ACL Rate

Description:

Set or show the ACL rate limiter.

Syntax:

Security Network ACL Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]

Parameters:

<rate_limiter_list>: Rate limiter list (1-16), default: All rate limiters

<rate_unit> : IP flags: pps|kbps, default: pss

<rate> : Rate in pps (0-100) or kbps (0, 100, 2*100, 3*100, ..., 1000000)

Default Setting:

1

Example:

Set rate limit value in 100 for port 1

```
NS3502-8P-2T-2S-V2:/>security network acl rate 1 100
```

Security Network ACL Add

Description:

Add or modify Access Control Entry (ACE).

If the ACE ID parameter <ace_id> is specified and an entry with this ACE ID already exists, the ACE will be modified. Otherwise, a new ACE will be added. If the ACE ID is not specified, the next available ACE ID will be used.

If the next ACE ID parameter <ace_id_next> is specified, the ACE will be placed before this ACE in the list. If the next ACE ID is not specified, the ACE will be placed last in the list.

If the Switch keyword is used, the rule applies to all ports.

If the Port keyword is used, the rule applies to the specified port only. If the Policy keyword is used, the rule applies to all ports configured with the specified policy. The default is that the rule applies to all ports.

Syntax:

Security Network ACL Add [<ace_id>] [<ace_id_next>] [switch | (port <port_list>) | (policy <policy>)] [<tagged>] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit|deny] [<rate_limiter>] [<port_copy>] [<mirror>] [<logging>] [<shutdown>]

Parameters:

<ace_id> : ACE ID (1-256), default: Next available ID
<ace_id_next> : Next ACE ID (1-256), default: Add ACE last
switch : Switch ACE keyword
port : Port ACE keyword
<port_list> : Port list or 'all', default: All ports
policy : Policy ACE keyword
<policy> : Policy number (1-8)
<tagged> : Tagged of frames: any|enable|disable
<vid> : VLAN ID (1-4095) or 'any'
<tag_prio> : VLAN tag priority (0-7) or 'any'
<dmac_type> : DMAC type: any|unicast|multicast|broadcast
etype : Ethernet Type keyword
<etype> : Ethernet Type: 0x600 - 0xFFFF or 'any' but excluding, 0x800(IPv4) 0x806(ARP) and 0x86DD(IPv6)
<smac> : Source MAC address (xx-xx-xx-xx-xx-xx) or 'any'
<dmac> : Destination MAC address (xx-xx-xx-xx-xx-xx) or 'any'
arp : ARP keyword
<sip> : Source IP address (a.b.c.d/n) or 'any'
<dip> : Destination IP address (a.b.c.d/n) or 'any'
<arp_opcode> : ARP operation code: any|arp|rarp|other
<arp_flags> : ARP flags: request|smac|tmac|len|ip|ether [0|1|any]
ip : IP keyword
<protocol> : IP protocol number (0-255) or 'any'
<ip_flags> : IP flags: ttl|options|fragment [0|1|any]
icmp : ICMP keyword
<icmp_type> : ICMP type number (0-255) or 'any'
<icmp_code> : ICMP code number (0-255) or 'any'
udp : UDP keyword
<sport> : Source UDP/TCP port range (0-65535) or 'any'
<dport> : Destination UDP/TCP port range (0-65535) or 'any'
tcp : TCP keyword
<tcp_flags> : TCP flags: fin|syn|rst|psh|ack|urg [0|1|any]
permit : Permit forwarding (default)
deny : Deny forwarding
<rate_limiter>: Rate limiter number (1-15) or 'disable'
<port_copy> : Port list for copy of frames or 'disable'
<mirror> : Mirror of frames: enable|disable
<logging> : System logging of frames: log|log_disable
<shutdown> : Shut down ingress port: shut|shut_disable

Security Network ACL Delete

Description:

Delete ACE.

Syntax:

Security Network ACL Delete <ace_id>

Parameters:

<ace_id>: ACE ID (1-256)

Example:

Delete ACE 1

```
NS3502-8P-2T-2S-V2:/>security network acl delete 1
```

Security Network ACL Lookup

Description:

Show ACE, default: All ACEs.

Syntax:

Security Network ACL Lookup [<ace_id>]

Parameters:

<ace_id>: ACE ID (1-256)

Example:

Lookup ACE 1

```
NS3502-8P-2T-2S-V2:/>security network acl lookup 1
```

Security Network ACL Clear

Description:

Clear all ACL counters.

Syntax:

Security Network ACL Clear

Example:

Clear all ACL counters.

```
NS3502-8P-2T-2S-V2:/>security network acl clear
```

Security Network ACL Status

Description:

Show ACL status.

Syntax:

Security Network ACL Status [combined|static|dhcp|upnp|arp_inspection|ipmc|ip_source_guard|conflicts]

Parameters:

combined : Shows the combined status
static : Shows the static user configured status
dhcp : Shows the status by DHCP
upnp : Shows the status by UPnP
arp_inspection : Shows the status by ARP Inspection
ip_source_guard : Shows the status by IP Source Guard
conflicts : Shows all conflict status

(default : Shows the combined status)

Example:

Show ACL status.

```
NS3502-8P-2T-2S-V2:/>security network acl status
```

Security Network DHCP Relay Configuration

Description:

Show DHCP relay configuration.

Syntax:

Security Network DHCP Relay Configuration

Example:

Show DHCP relay configuration.

```
NS3502-8P-2T-2S-V2:/>security network dhcp relay configuration

DHCP Relay Configuration:
=========================

DHCP Relay Mode             : Disabled
DHCP Relay Server           : NULL
DHCP Relay Information Mode   : Disabled
DHCP Relay Information Policy : replace
```

Security Network DHCP Relay Mode

Description:

Set or show the DHCP relay mode.

Syntax:

Security Network DHCP Relay Mode [enable|disable]

Parameters:

enable : Enable DHCP relaly mode.

When enable DHCP relay mode operation, the agent forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain. And the DHCP broadcast message won't flood for security considered.

disable: Disable DHCP relaly mode

(default: Show flow DHCP relaly mode)

Default Setting:

disable

Example:

Enable DHCP relay mode

```
NS3502-8P-2T-2S-V2:/>security network dhcp relay mode enable
```

Security Network DHCP Relay Server

Description:

Show or set DHCP relay server.

Syntax:

Security Network DHCP Relay Server [<ip_addr>]

Parameters:

<ip_addr>: IP address (a.b.c.d), default: Show IP address

Default Setting:

null

Example:

Set DHCP relay server in 192.168.0.20

```
NS3502-8P-2T-2S-V2:/>security network dhcp relay server 192.168.0.20
```

Security Network DHCP Relay Information Mode

Description:

Set or show DHCP relay agent information option mode.
When enable DHCP relay information mode operation, the agent insert specific information (option 82) into a DHCP message when forwarding to DHCP server and remote it from a DHCP message when transferring to DHCP client. It only works under DHCP relay operation mode enabled.

Syntax:

Security Network DHCP Relay Information Mode [enable|disable]

Parameters:

enable : Enable DHCP relay agent information option mode
disable: Disable DHCP relay agent information option mode
(default: Show DHCP relay agent information option mode)

Default Setting:

disable

Example:

Enable DHCP relay agent information option mode.

```
NS3502-8P-2T-2S-V2:/>security network dhcp relay information mode enable
```

Security Network DHCP Relay Information Policy

Description:

Set or show the DHCP relay mode.
When DHCP relay information mode operation is enabled, if an agent receives a DHCP message that already contains relay agent information, it will enforce the policy.

Syntax:

Security Network DHCP Relay Information Policy [replace|keep|drop]

Parameters:

replace : Replace the original relay information when receiving a DHCP message that already contains it

keep : Keep the original relay information when receiving a DHCP message that already contains it

drop : Drop the package when receiving a DHCP message that already contains relay information

(default: Show DHCP relay information policy)

Default Setting:

replace

Example:

Keep the original relay information when receiving a DHCP message that already

contains it

```
NS3502-8P-2T-2S-V2:/>security network dhcp relay information policy keep
```

Security Network DHCP Relay Statistics

Description:

Show or clear DHCP relay statistics.

Syntax:

Security Network DHCP Relay Statistics [clear]

Parameters:

clear: Clear DHCP relay statistics

Example:

Show DHCP relay statistics.

```
NS3502-8P-2T-2S-V2:/>security network dhcp relay statistics
```

Security Network DHCP Snooping Configuration

Description:

Show DHCP snooping configuration.

Syntax:

Security Network DHCP Snooping Configuration

Security Network DHCP Snooping Mode

Description:

Set or show the DHCP snooping mode.

Syntax:

Security Network DHCP Snooping Mode [enable|disable]

Parameters:

enable : Enable DHCP snooping mode.

When DHCP snooping mode operation is enabled, the requested DHCP messages will be forwarded to trusted ports and only allows reply packets from trusted ports.

disable: Disable DHCP snooping mode

(default: Show flow DHCP snooping mode)

Default Setting:

disable

Example:

Enable DHCP snooping mode

```
NS3502-8P-2T-2S-V2:/>security network dhcp snooping mode enable
```

Security Network DHCP Snooping Port Mode

Description:

Set or show the DHCP snooping port mode.

Syntax:

Security Network DHCP Snooping Port Mode [<port_list>] [trusted|untrusted]

Parameters:

<port_list>: Port list or 'all', default: All ports
trusted : Configures the port as trusted sources of the DHCP message
untrusted: Configures the port as untrusted sources of the DHCP message
(default: Show flow DHCP snooping port mode)

Default Setting:

trusted

Example:

Set untrusted DHCP snooping port mode in port 1

```
NS3502-8P-2T-2S-V2:/>security network dhcp snooping port mode 1
untrusted
```

Security Network DHCP Snooping Statistics

Description:

Show or clear DHCP snooping statistics.

Syntax:

Security Network DHCP Snooping Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports
clear : Clear DHCP snooping statistics

Example:

Show DHCP snooping statistics of port 1.

```
NS3502-8P-2T-2S-V2:/>security network dhcp snooping statistics 1
Port 1 Statistics:
--------------------
Rx Discover:           0   Tx Discover:           0
Rx Offer:              0   Tx Offer:              0
Rx Request:            0   Tx Request:            0
Rx Decline:            0   Tx Decline:            0
Rx ACK:                0   Tx ACK:                0
Rx NAK:                0   Tx NAK:                0
Rx Release:            0   Tx Release:            0
Rx Inform:             0   Tx Inform:             0
Rx Lease Query:        0   Tx Lease Query:        0
Rx Lease Unassigned:   0   Tx Lease Unassigned:   0
Rx Lease Unknown:      0   Tx Lease Unknown:      0
Rx Lease Active:       0   Tx Lease Active:       0
```

Security Network IP Source Guard Configuration

Description:

Show IP source guard configuration.

Syntax:

Security Network IP Source Guard Configuration

Security Network IP Source Guard Mode

Description:

Set or show IP source guard mode.

Syntax:

Security Network IP Source Guard Mode [enable|disable]

Parameters:

enable : Enable IP Source Guard

disable: Disable IP Source Guard

Default Setting:

disable

Example:

Enable IP source guard mode

```
NS3502-8P-2T-2S-V2:/>security network ip source guard mode enable
```

Security Network IP Source Guard Port Mode

Description:

Set or show the IP Source Guard port mode.

Syntax:

Security Network IP Source Guard Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable IP Source Guard port

disable : Disable IP Source Guard port

(default: Show IP Source Guard port mode)

Default Setting:

disable

Example:

Enable IP source guard port mode for port1~4

```
NS3502-8P-2T-2S-V2:/>security network ip source guard port mode 1-4 enable
```

Security Network IP Source Guard Limit

Description:

Set or show the IP Source Guard port limitation for dynamic entries.

Syntax:

Security Network IP Source Guard limit [<port_list>] [<dynamic_entry_limit>|unlimited]

Parameters:

<port_list> : Port list or 'all', default: All ports

<dynamic_entry_limit>|unlimited: dynamic entry limit (0-2) or unlimited

Default Setting:

unlimited

Example:

Set IP source guard limit

```
NS3502-8P-2T-2S-V2:/>security network ip source guard 1 1
```

Security Network IP Source Guard Entry

Description:

Add or delete IP source guard static entry.

Syntax:

Security Network IP Source Guard Entry [<port_list>] add|delete <vid> <allowed_ip> <allowed_mac>

Parameters:

<port_list> : Port list or 'all', default: All ports

add : Add new port IP source guard static entry

delete : Delete existing port IP source guard static entry

<vid> : VLAN ID (1-4095)

<allowed_ip> : IP address (a.b.c.d), IP address allowed for doing IP source guard

<allowed_mac>: MAC address (xx-xx-xx-xx-xx-xx), MAC address allowed for doing IP source guard

Example:

Add IP source guard static entry.

```
NS3502-8P-2T-2S-V2:/>security network ip source guard entry 1 add 1 192.168.0.20
```

Security Network IP Source Guard Status

Description:

Show IP source guard static and dynamic entries.

Syntax:

Security Network IP Source Guard Status [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show IP source guard static and dynamic entries.

```
NS3502-8P-2T-2S-V2:/>security network ip source guard status
```

Security Network IP Source Guard Translation

Description:

Translate IP source guard dynamic entries into static entries.

Syntax:

Security Network IP Source Guard Translation

Security Network ARP Inspection Configuration

Description:

Show ARP inspection configuration.

Syntax:

Security Network ARP Inspection Configuration

Example:

Show ARP inspection configuration.

```
NS3502-8P-2T-2S-V2:/>security network arp inspection configuration
```

Security Network ARP Inspection Mode

Description:

Set or show ARP inspection mode.

Syntax:

Security Network ARP Inspection Mode [enable|disable]

Parameters:

enable : Enable ARP Inspection

disable: Disable ARP Inspection

Default Setting:

disable

Example:

Enable ARP inspection mode

```
NS3502-8P-2T-2S-V2:/>security network arp inspection mode enable
```

Security Network ARP Inspection Port Mode

Description:

Set or show the ARP Inspection port mode.

Syntax:

Security Network ARP Inspection Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable ARP Inspection port

disable : Disable ARP Inspection port

(default: Show ARP Inspection port mode)

Default Setting:

Disable

Example:

Enable the ARP inspection mode of port 1

```
NS3502-8P-2T-2S-V2:/>security network arp inspection port mode 1
```

Security Network ARP Inspection Entry

Description:

Add or delete ARP inspection static entry.

Syntax:

Security Network ARP Inspection Entry [<port_list>] add|delete <vid> <allowed_mac> <allowed_ip>

Parameters:

<port_list> : Port list or 'all', default: All ports

add : Add new port ARP inspection static entry

delete : Delete existing port ARP inspection static entry

<vid> : VLAN ID (1-4095)

<allowed_mac>: MAC address (xx-xx-xx-xx-xx-xx), MAC address allowed for doing ARP request

<allowed_ip> : IP address (a.b.c.d), IP address allowed for doing ARP request

Example:

Add ARP inspection static entry.

```
NS3502-8P-2T-2S-V2:/>security network arp inspection entry 1 add 1 00-30-4f-00-00-11 192.168.0.11
```

Security Network ARP Inspection Status

Description:

Show ARP inspection static and dynamic entries.

Syntax:

Security Network ARP Inspection Status [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show ARP inspection static and dynamic entries.

```
NS3502-8P-2T-2S-V2:/>security network arp inspection status
```

Security Network ARP Inspection Translation

Description:

Translate ARP inspection dynamic entries into static entries.

Syntax:

Security Network ARP Inspection Translation

Security AAA Configuration

Description:

Show Auth configuration.

Syntax:

Security AAA Configuration

Example:

Show Auth configuration.

```
NS3502-8P-2T-2S-V2:/>security aaa configuration

AAA Configuration:
==================


Server Timeout   : 15 seconds

Server Dead Time : 300 seconds

RADIUS Authentication Server Configuration:
=========================================
Server  Mode     IP Address      Secret                    Port
------  -------- --------------  ------------------------------  -----
1       Disabled                                           1812
2       Disabled                                           1812
3       Disabled                                           1812
4       Disabled                                           1812
5       Disabled                                           1812

RADIUS Accounting Server Configuration:
=====================================
Server  Mode     IP Address      Secret                    Port
```

```
------  --------  --------------  ------------------------------  -----
1       Disabled                                  1813
2       Disabled                                  1813
3       Disabled                                  1813
4       Disabled                                  1813
5       Disabled                                  1813

TACACS+ Authentication Server Configuration:
============================================
Server  Mode      IP Address      Secret                          Port
------  --------  --------------  ------------------------------  -----
1       Disabled                                  49
2       Disabled                                  49
3       Disabled                                  49
4       Disabled                                  49
5       Disabled                                  49
```

Security AAA Timeout

Description:

Set or show server timeout.

Syntax:

Security AAA Timeout [<timeout>]

Parameters:

<timeout>: Server response timeout (3-3600 seconds)

(default: Show server timeout configuration)

Default Setting:

15

Example:

Set 30sec for server timeout

```
NS3502-8P-2T-2S-V2:/>security aaa timeout 30
```

Security AAA Deadtime

Description:

Set or show server dead time.

Syntax:

Security AAA Deadtime [<dead_time>]

Parameters:

<dead_time>: Time that a server is considered dead if it doesn't answer a request (0-3600 seconds)

(default: Show server dead time configuration)

Default Setting:

300

Example:

Set 1000sec for server dead time

```
NS3502-8P-2T-2S-V2:/>security aaa deadtime 1000
```

Security AAA RADIUS

Description:

Set or show RADIUS authentication server setup.

Syntax:

Security AAA RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)
(default: Show RADIUS authentication server configuration)
enable : Enable RADIUS authentication server
disable : Disable RADIUS authentication server
(default: Show RADIUS server mode)
<ip_addr_string>: IP host address (a.b.c.d) or a host name string
<secret> : Secret shared with external authentication server.
To set an empty secret, use two quotes ("").
To use spaces in secret, enquote the secret.
Quotes in the secret are not allowed.
<server_port> : Server UDP port. Use 0 to use the default RADIUS port (1812)

Example:

Set RADIUS authentication server configuration.

```
NS3502-8P-2T-2S-V2:/>security aaa radius 1 enable 192.168.0.20 12345678
1812
```

Security AAA ACCT_RADIUS

Description:

Set or show RADIUS accounting server setup.

Syntax:

Security AAA ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)
(default: Show RADIUS accounting server configuration)
enable : Enable RADIUS accounting server
disable : Disable RADIUS accounting server
(default: Show RADIUS server mode)
<ip_addr_string>: IP host address (a.b.c.d) or a host name string
<secret> : Secret shared with external accounting server.
To set an empty secret, use two quotes ("").
To use spaces in secret, enquote the secret.
Quotes in the secret are not allowed.
<server_port> : Server UDP port. Use 0 to use the default RADIUS port (1813)

Example:

Set RADIUS accounting server configuration.

```
NS3502-8P-2T-2S-V2:/>security acct_radius 1 enable 192.168.0.20
12345678 1813
```

Security AAA TACACS+

Description:

Set or show TACACS+ authentication server setup.

Syntax:

Security AAA TACACS+ [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)
(default: Show TACACS+ authentication server configuration)
enable : Enable TACACS+ authentication server
disable : Disable TACACS+ authentication server
(default: Show TACACS+ server mode)
<ip_addr_string>: IP host address (a.b.c.d) or a host name string
<secret> : Secret shared with external authentication server.
To set an empty secret, use two quotes ("").
To use spaces in secret, enquote the secret.
Quotes in the secret are not allowed.
<server_port> : Server TCP port. Use 0 to use the default TACACS+ port (49)

Example:

Set TACACS+ authentication server configuration.

```
NS3502-8P-2T-2S-V2:/>security aaa tacacs+ 1 enable 192.168.0.20
12345678 49
```

Security AAA Statistics

Description:

Show RADIUS statistics.

Syntax:

Security AAA Statistics [<server_index>]

Parameters:

The server index (1-5)
(default: Show statistics for all servers)

Example:

Show RADIUS statistics.

```
NS3502-8P-2T-2S-V2:/>security aaa statistics
```

Spanning Tree Protocol Command

STP Configuration

Description:

Show STP configuration.

Syntax:

STP Configuration

Example:

Show STP configuration.

```
NS3502-8P-2T-2S-V2:/>stp cofiguration

STP Configuration:
==================

Protocol Version: MSTP
Max Age        : 20
Forward Delay  : 15
Tx Hold Count  : 6
Max Hop Count  : 20
BPDU Filtering : Disabled
BPDU Guard     : Disabled
Error Recovery : Disabled
```

STP Version

Description:

Set or show the STP Bridge protocol version.

Syntax:

STP Version [<stp_version>]

Parameters:

<stp_version>: mstp|rstp|stp

Default Setting:

MSTP

Example:

Set the STP Bridge protocol version.

```
NS3502-8P-2T-2S-V2:/> stp version rstp
```

STP Tx Hold

Description:

Set or show the STP Bridge Transmit Hold Count parameter.

Syntax:

STP Txhold [<holdcount>]

Parameters:

<holdcount>: STP Transmit Hold Count (1-10)

Default Setting:

6

Example:

Set STP Tx hold in 10

```
NS3502-8P-2T-2S-V2:/>stp txhold 10
```

STP MaxHops

Description:

Set or show the MSTP Bridge Max Hop Count parameter.

Syntax:

STP MaxHops [<maxhops>]

Parameters:

<maxhops>: STP BPDU MaxHops (6-40))

Default Setting:

20

Example:

Set STP maximum hops in 25

```
NS3502-8P-2T-2S-V2:/>stp maxhops 25
```

STP MaxAge

Description:

Set or show the bridge instance maximum age.

Syntax:

STP MaxAge [<max_age>]

Parameters:

<max_age>: STP maximum age time (6-40, and max_age <= (forward_delay-1)*2)

Default Setting:

20

Example:

Set STP maximum age time in 10

```
NS3502-8P-2T-2S-V2:/>stp maxage 10
```

STP FwdDelay

Description:

Set or show the CIST/MSTI bridge forward delay.

Syntax:

STP FwdDelay [<delay>]

Parameters:

<delay>: MSTP forward delay (4-30, and max_age <= (forward_delay-1)*2))

Default Setting:

15

Example:

Set STP forward delay value in 25

```
NS3502-8P-2T-2S-V2:/>stp fwddelay 25
```

STP CName

Description:

Set or Show MSTP configuration name and revision.

Syntax:

STP CName [<config-name>] [<integer>]

Parameters:

<config-name>: MSTP Configuration name. A text string up to 32 characters long. Use quotes (") to embed spaces in name.

<integer> : Integer value

Default Setting:

Configuration name: MAC address

Configuration rev.: 0

Example:

Set MSTP configuration name and revision.

```
NS3502-8P-2T-2S-V2:/>stp cname 9f_NS3502-8P-2T-2S-V2 1
```

STP BPDU Filter

Description:

Set or show edge port BPDU Filtering.

Syntax:

STP bpduFilter [enable|disable]

Parameters:

enable|disable: enable or disable BPDU Filtering for Edge ports

Default Setting:

Disable

Example:

Set edge port BPDU filtering

```
NS3502-8P-2T-2S-V2:/>stp bpdufilter enable
```

STP BPDU Guard

Description:

Set or show edge port BPDU Guard.

Syntax:

STP bpduGuard [enable|disable]

Parameters:

enable|disable: enable or disable BPDU Guard for Edge ports

Default Setting:

Disable

Example:

Set edge port BPDU guard

```
NS3502-8P-2T-2S-V2:/>stp bpduguard enable
```

STP Recovery

Description:

Set or show edge port error recovery timeout.

Syntax:

STP recovery [<timeout>]

Parameters:

<timeout>: Time before error-disabled ports are reenabled (30-86400 seconds, 0 disables)

(default: Show recovery timeout)

Default Setting:

Disable

Example:

Set STP recovery value in 30 sec.

```
NS3502-8P-2T-2S-V2:/>stp recovery 30
```

STP Status

Description:

Show STP Bridge status.

Syntax:

STP Status [<msti>] [<port_list>]

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<port_list>: Port list or 'all', default: All ports

Default Setting:

Disable

Example:

Show STP Bridge status.

```
NS3502-8P-2T-2S-V2:/>stp status
CIST Bridge STP Status
Bridge ID    : 80:00-00:30:4F:24:04:D1
Root ID      : 80:00-00:30:4F:24:04:D1
Root Port    : -
Root PathCost: 0
Regional Root: 80:00-00:30:4F:24:04:D1
Int. PathCost: 0
Max Hops     : 20
TC Flag      : Steady
TC Count     : 0
TC Last      : -
Port      Port Role      State      Pri  PathCost  Edge  P2P  Uptime
---------  --------------  ----------  ---  --------  ----  ---  -------------
10      DesignatedPort  Forwarding  128  20000    Yes   Yes  0d
00:10:32
```

STP MSTI Priority

Description:

Set or show the bridge instance priority.

Syntax:

STP Msti Priority [<msti>] [<priority>]

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<priority> : STP bridge priority (0/16/32/48/.../224/240)

Default:

128

Example:

Set MST1 priority value in 48.

```
NS3502-8P-2T-2S-V2:/>stp msti priority 1 48
```

STP MSTI Map

Description:

Show or clear MSTP MSTI VLAN mapping configuration.

Syntax:

STP Msti Map [<msti>] [clear]

Parameters:

<msti>: STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

Clear : Clear VID to MSTI mapping

Example:

Add MST1 priority value in 48.

```
NS3502-8P-2T-2S-V2:/>stp msti priority 1 48
```

STP MSTI Add

Description:

Add a VLAN to a MSTI.

Syntax:

STP Msti Add <msti> <vid>

Parameters:

<msti>: STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<vid> : VLAN ID (1-4095)

Example:

Add MST1 in vlan1.

```
NS3502-8P-2T-2S-V2:/>stp msti add 1 1
```

STP Port Configuration

Description:

Show STP Port configuration.

Syntax:

STP Port Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

Example:

Show STP status of Port1

```
NS3502-8P-2T-2S-V2:/>stp port configuration 1

Port  Mode     AdminEdge AutoEdge  restrRole restrTcn  Point2point
----  -------- ----------------- ----------------- -----------
1    Disabled  Disabled  Enabled   Disabled  Disabled  Auto
```

STP Port Mode

Description:

Set or show the STP enabling for a port.

Syntax:

STP Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

Enable : Enable MSTP protocol

Disable : Disable MSTP protocol

Default:

disable

Example:

Enable STP function on port1

```
NS3502-8P-2T-2S-V2:/>stp port mode 1 enable
```

STP Port Edge

Description:

Set or show the STP adminEdge port parameter.

Syntax:

STP Port Edge [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

Enable : Configure MSTP adminEdge to Edge

Disable : Configure MSTP adminEdge to Non-edge

Default:

disable

Example:

Enable STP edge function on port1

```
NS3502-8P-2T-2S-V2:/>stp port edge 1 enable
```

STP Port AutoEdge

Description:

Set or show the STP autoEdge port parameter.

Syntax:

STP Port AutoEdge [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

Enable : Enable MSTP autoEdge

Disable : Disable MSTP autoEdge

Default:

enable

Example:

Disable STP edge function on port1

```
NS3502-8P-2T-2S-V2:/>stp port autoedge 1 disable
```

STP Port P2P

Description:

Set or show the STP point2point port parameter.

Syntax:

STP Port P2P [<port_list>] [enable|disable|auto]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable MSTP point2point

disable : Disable MSTP point2point

auto : Automatic MSTP point2point detection

Default:

auto

Example:

Disable STP P2P function on port1

```
NS3502-8P-2T-2S-V2:/>stp port p2p 1 disable
```

STP Port RestrictedRole

Description:

Set or show the MSTP restrictedRole port parameter.

Syntax:

STP Port RestrictedRole [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable MSTP restricted role
disable : Disable MSTP restricted role

Default:

disable

Example:

Enable STP restricted role on port1

```
NS3502-8P-2T-2S-V2:/>stp port restrictedrole 1 enable
```

STP Port RestrictedTcn

Description:

Set or show the MSTP restrictedTcn port parameter.

Syntax:

STP Port RestrictedTcn [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable MSTP restricted TCN
disable : Disable MSTP restricted TCN

Default:

disable

Example:

Enable STP restricted TCN on port1

```
NS3502-8P-2T-2S-V2:/>stp port restrictedtcn 1 enable
```

STP Port bpduGuard

Description:

Set or show the bpduGuard port parameter.

Syntax:

STP Port bpduGuard [<port_list>] [enable|disable]

eters:

<port_list>: Port list or 'all', default: All ports
enable : Enable port BPDU Guard
disable : Disable port BPDU Guard

Default:

disable

Example:

Enable BPDU guard on port1

```
NS3502-8P-2T-2S-V2:/>stp port bpduguard 1 enable
```

STP Port Statistic

Description:

Show STP port statistics.

Syntax:

STP Port Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear : Clear the selected port statistics

Example:

Show STP port statistics.

```
NS3502-8P-2T-2S-V2:/>stp port statistics
Port      Rx MSTP   Tx MSTP   Rx RSTP   Tx RSTP   Rx STP   Tx STP
Rx TCN   Tx TCN   Rx Ill.  Rx Unk.
--------- --------- --------- --------- --------- -------- -------- -------- -------- -------- -----
--
```

STP Port Mcheck

Description:

Set the STP mCheck (Migration Check) variable for ports.

Syntax:

STP Port Mcheck [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Set the STP mCheck (Migration Check) variable for port 1.

```
NS3502-8P-2T-2S-V2:/>stp port mcheck 1
```

STP MSTI Port Configuration

Description:

Show the STP port instance configuration.

Syntax:

STP Msti Port Configuration [<msti>] [<port_list>]

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<port_list>: Port list or 'all', default: All ports

Default:

auto

STP MSTI Port Cost

Description:

Set or show the STP port instance path cost.

Syntax:
STP Msti Port Cost [<msti>] [<port_list>] [<path_cost>]
Parameters:
<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<port_list>: Port list or 'all'. Port zero means aggregations.
<path_cost>: STP port path cost (1-200000000) or 'auto'
Default:
auto
Example:
Set MSTI7 in port1

```
NS3502-8P-2T-2S-V2:/>stp msti port cost 7 1

MSTI  Port  Path Cost
----   ----   ----------
MST7  1    Auto
```

STP MSTI Port Priority

Description:
Set or show the STP port instance priority.
Syntax:
STP Msti Port Priority [<msti>] [<port_list>] [<priority>]
Parameters:
<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<port_list>: Port list or 'all'. Port zero means aggregations.
<priority> : STP port priority (0/16/32/48/.../224/240)
Default:
128

Link Aggregation Command

Aggregation Configuration

Description:
Show link aggregation configuration.
Syntax:
Aggr Configuration

Aggregation Add

Description:
Add or modify link aggregation.
Syntax:
Aggr Add <port_list> [<aggr_id>]
Parameters:
<port_list>: Port list or 'all', default: All ports
<aggr_id> : Aggregation ID
Example:

Add port 1~4 in Group1

```
NS3502-8P-2T-2S-V2:/>aggr add 1-4 1
```

Aggregation Delete

Description:

Delete link aggregation.

Syntax:

Aggr Delete <aggr_id>

Parameters:

<aggr_id>: Aggregation ID

Example:

Delete Group2

```
NS3502-8P-2T-2S-V2:/>aggr delete 2
```

Aggregation Lookup

Description:

Lookup link aggregation.

Syntax:

Aggr Lookup [<aggr_id>]

Parameters:

<aggr_id>: Aggregation ID

Aggregation Mode

Description:

Set or show the link aggregation traffic distribution mode.

Syntax:

Aggr Mode [smac|dmac|ip|port] [enable|disable]

Parameters:

smac : Source MAC address
dmac : Destination MAC address
ip : Source and destination IP address
port : Source and destination UDP/TCP port
enable : Enable field in traffic distribution
disable: Disable field in traffic distribution

Default Setting:

SMAC : Enabled
DMAC : Disabled
IP : Enabled
Port : Enabled

Example:

Disable SMAC mode

```
NS3502-8P-2T-2S-V2:/>Aggr mode smac disable
```

Link Aggregation Control Protocol Command

LACP Configuration

Description:

Show LACP configuration.

Syntax:

LACP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LACP configuration

```
NS3502-8P-2T-2S-V2:/>lacp configuration

Port  Mode     Key   Role
----  --------   ----   ------
1     Disabled  Auto  Active
2     Disabled  Auto  Active
3     Disabled  Auto  Active
4     Disabled  Auto  Active
5     Disabled  Auto  Active
6     Disabled  Auto  Active
7     Disabled  Auto  Active
8     Disabled  Auto  Active
9     Disabled  Auto  Active
10    Disabled  Auto  Active
```

LACP Mode

Description:

Set or show LACP mode.

Syntax:

LACP Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable LACP protocol

disable: Disable LACP protocol

(default: Show LACP mode)

Default Setting:

disable

Example:

Enable LACP for port1~4

```
NS3502-8P-2T-2S-V2:/>lacp mode 1-4 enable
```

LACP Key

Description:

Set or show the LACP key.

Syntax:

LACP Key [<port_list>] [<key>]

Parameters:

<port_list>: Port list or 'all', default: All ports
<key> : LACP key (1-65535) or 'auto'

Default Setting:

auto

Example:

Set key1 for port1~4

```
NS3502-8P-2T-2S-V2:/>lacp key 1-4 1
```

LACP Prio

Description:

Set or show the LACP prio.

Syntax:

LACP Prio [<port_list>] [<prio>]

Parameters:

<port_list>: Port list or 'all', default: All ports
<prio> : LACP Prio (0-65535)

Default Setting:

32768

LACP System Prio

Description:

Set or show the LACP System prio.

Syntax:

LACP System Prio [<sysprio>]

Parameters:

<sysprio>: LACP System Prio (0-65535)

Default Setting:

32768

LACP Role

Description:

Set or show the LACP role.

Syntax:

LACP Role [<port_list>] [active|passive]

Parameters:

<port_list>: Port list or 'all', default: All ports
active : Initiate LACP negotiation
passive: Listen for LACP packets
(default: Show LACP role)

Default Setting:

active

Example:

Set passive for port1~4

```
NS3502-8P-2T-2S-V2:/>lacp role 1-4 passive
```

LACP Status

Description:

Show LACP Status.

Syntax:

LACP Status [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LACP status of port1~4

```
NS3502-8P-2T-2S-V2:/>lacp status 1-4

Port  Mode      Key   Aggr ID  Partner System ID  Partner Port
----  --------  ----- -------  -----------------  ------------
1     Disabled  1     -        -                  -
2     Disabled  1     -        -                  -
3     Disabled  1     -        -                  -
4     Disabled  1     -        -                  -
```

LACP Statistics

Description:

Show LACP Statistics.

Syntax:

LACP Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear **:** Clear LACP statistics

Example:

Show LACP statistics of port1~4

```
NS3502-8P-2T-2S-V2:/>lacp statistics 1-4

Port  Rx Frames   Tx Frames   Rx Unknown  Rx Illegal
------ ---------- ---------- ---------- ----------
1     0          0          0          0
2     0          0          0          0
3     0          0          0          0
4     0          0          0          0
```

LACP Timeout

Description:

Set or show the LACP timeout.

Syntax:

LACP Timeout [<port_list>] [fast|slow]

Parameters:

<port_list>: Port list or 'all', default: All ports

fast : Fast PDU transmissions (fast timeout)

slow : Slow PDU transmissions (slow timeout)

(default: Show LACP timeout)

Default Setting:

fast

LLDP Command

LLDP Configuration

Description:

Show LLDP configuration.

Syntax:

LLDP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LLDP configuration of port1~4

```
NS3502-8P-2T-2S-V2:/>lldp configuration 1-4

LLDP Configuration:
===================

Interval    : 30
Hold        : 3
Tx Delay    : 2
Reinit Delay: 2

Port Mode     Port Descr System Name System Descr System Capa Mgmt
Addr CDP awareness
---- --------  ----------  -----------  ------------  -----------  ---------  -----------
--
1  Enabled  Enabled   Enabled     Enabled     Enabled    Enabled
Disabled
2  Enabled  Enabled   Enabled     Enabled     Enabled    Enabled
Disabled
3  Enabled  Enabled   Enabled     Enabled     Enabled    Enabled
Disabled
4  Enabled  Enabled   Enabled     Enabled     Enabled    Enabled
Disabled
```

LLDP Mode

Description:

Set or show LLDP mode.

Syntax:

LLDP Mode [<port_list>] [enable|disable|rx|tx]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable LLDP reception and transmission
disable: Disable LLDP
rx : Enable LLDP reception only
tx : Enable LLDP transmission only
(default: Show LLDP mode)

Default Setting:

disable

Example:

Enable port1 LLDP function.

```
NS3502-8P-2T-2S-V2:/>lldp mode 1 enable
```

LLDP Optional TLV

Description:

Show or Set LLDP Optional TLVs.

Syntax:

LLDP Optional_TLV [<port_list>] [port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
port_descr : Description of the port
sysm_name : System name
sys_descr : Description of the system
sys_capa : System capabilities
mgmt_addr : Master's IP address
(default: Show optional TLV's configuration)
enable : Enables TLV
disable : Disable TLV
(default: Show optional TLV's configuration)

Default Setting:

Description of the port: Enable
System name: Enable
Description of the system: Enable
System capabilities: Enable
Master's IP address: Enable

Example:

Disable description of the port for port1

```
NS3502-8P-2T-2S-V2:/>lldp optional_tlv 1 port_descr disable
```

LLDP Interval

Description:

Set or show LLDP Tx interval.

Syntax:

LLDP Interval [<interval>]

Parameters:

<interval>: LLDP transmission interval (5-32768)

Default Setting:

30

Example:

Set transmission interval in 10

```
NS3502-8P-2T-2S-V2:/>lldp interval 10
```

LLDP Hold

Description:

Set or show LLDP Tx hold value.

Syntax:

LLDP Hold [<hold>]

Parameters:

<hold>: LLDP hold value (2-10)

Default Setting:

3

Example:

Set LLDP hold value in 10

```
NS3502-8P-2T-2S-V2:/>lldp hold 10
```

LLDP Delay

Description:

Set or show LLDP Tx delay.

Syntax:

LLDP Delay [<delay>]

Parameters:

<delay>: LLDP transmission delay (1-8192)

Default Setting:

2

Example:

Set LLDP delay value in 1

```
NS3502-8P-2T-2S-V2:/>lldp delay 1
```

LLDP Reinit

Description:

Set or show LLDP reinit delay.

Syntax:

LLDP Reinit [<reinit>]

Parameters:

<reinit>: LLDP reinit delay (1-10)

Default Setting:

2

Example:

Set LLDP reinit delay value in 3

```
NS3502-8P-2T-2S-V2:/>lldp reinit 3
```

LLDP Statistics

Description:

Show LLDP Statistics.

Syntax:

LLDP Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear : Clear LLDP statistics

Example:

Show LLDP Statistics of port 1

```
NS3502-8P-2T-2S-V2:/>lldp statistics 1

LLDP global counters
Neighbor entries was last changed at - (18819 sec. ago).
Total Neighbors Entries Added    0.
Total Neighbors Entries Deleted  0.
Total Neighbors Entries Dropped  0.
Total Neighbors Entries Aged Out 0.

LLDP local counters
     Rx      Tx      Rx      Rx      Rx TLV   Rx TLV   Rx TLV
Port  Frames  Frames  Errors  Discards Errors  Unknown  Organz.
Aged
----  ------  ------  ------  --------  ------  -------  -------  -----
1     0       0       0       0       0       0       0       0
```

LLDP Info

Description:

Show LLDP neighbor device information.

Syntax:

LLDP Info [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

LLDP MED Command

LLDP MED Configuration

Description:

Show LLDP-MED configuration.

Syntax:

LLDPMED Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LLDP-MED configuration of port1~4

```
NS3502-8P-2T-2S-V2:/>lldpmed configuration 1-4

LLDP-MED Configuration:
=======================

Fast Start Repeast Count : 4
Location Coordinates    : Latitude              - 0.0000 North
                          Longitude             - 0.0000 East
                          Altitude              - 0.0000 meter(s)
                          Map datum             - WGS84
Civic Address Location  :


Port     Policies
1        none
2        none
3        none
4        none
```

LLDP MED Civic

Description:

Set or show LLDP-MED Civic Address Location.

Syntax:

LLDPMED Civic [country|state|county|city|district|block|street|leading_street_direction|trailing_street_suffix|str_suf|house_no|house_no_suffix|landmark|additional_info|name|zip_code|building|apartment|floor|room_number|place_type|postal_com_name|p_o_box|additional_code] [<civic_value>]

Parameters:

country : Country
state : National subdivisions (state, caton, region, province, prefecture)
county : County, parish,gun (JP), district(IN)
city : City, townchip, shi (JP)
district : City division,borough, city, district, ward,chou (JP)
block : Neighborhood, block
street : Street
leading_street_direction : Leading street direction

trailing_street_suffix : Trailing street suffix
str_suf : Street Suffix
house_no : House Number
house_no_suffix : House number suffix
landmark : Landmark or vanity address
additional_info : Additional location information
name : Bame(residence and office occupant)
zip_code : Postal/zip code
building : Building (structure)
apartment : Unit (apartment, suite)
floor : Floor
room_number : Room numbe**r**
place_type : Placetype
postal_com_name : Postal community name
p_o_box : Post office box (P.O. Box)
additional_code : Addtional code
(default: Show Civic Address Location configuration)
<civic_value>: lldpmed The value for the Civic Address Location entry.

LLDP MED ECS

Description:
Set or show LLDP-MED Emergency Call Service.
Syntax:
LLDPMED ecs [<ecs_value>]
Parameters:
<ecs_value>: lldpmed The value for the Emergency Call Service

LLDP MED Policy Delete

Description:
Delete the selected policy.
Syntax:
LLDPMED policy delete [<policy_list>]
Parameters:
<policy_list>: List of policies to delete
Example:
Delete the policy 1

```
NS3502-8P-2T-2S-V2:/>lldpmed policy delete 1
```

LLDP MED Policy Add

Description:
Adds a policy to the list of polices.
Syntax:
LLDPMED policy add
[voice|voice_signaling|guest_voice|guest_voice_signaling|softphone_voice|video_conferencing|streaming_video|video_signaling] [tagged|untagged] [<vlan_id>] [<l2_priority>] [<dscp>]
Parameters:

voice : 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

voice_signaling : Voice Signaling (conditional) for use in network topologies that require a different policy for the voice signaling than for the voice media.

guest_voice : 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.

guest_voice_signaling : 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.

softphone_voice : 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.

video_conferencing : Video Conferencing for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

streaming_video : 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.

video_signaling : Video Signaling (conditional) for use in network topologies that require a separate policy for the video signaling than for the video media.

tagged : The device is using tagged frames

unragged : The device is using untagged frames

<vlan_id> : VLAN id

<l2_priority>: This field may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004 [3].

<dscp> : This field shall contain the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474 [5]. This 6 bit field 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.

LLDP MED Port Policy

Description:

Set or show LLDP-MED port polcies.

Syntax:

LLDPMED port policies [<port_list>] [<policy_list>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<policy_list>: List of policies to delete

LLDP MED Coordinates

Description:

Set or show LLDP-MED Location.

Syntax:

LLDPMED Coordinates [latitude|longitude|altitude] [north|south|west|east|meters|floor] [coordinate_value]

Parameters:

latitude : Latitude, 0 to 90 degress with max. 4 digits (Positive numbers are north of the equator and negative numbers are south of the equator).

longitude : Longitude,0 to 180 degress with max. 4 digits (Positive values are East of the prime meridian and negative numbers are West of the prime meridian.

altitude : Altitude, Meters or floors with max. 4 digits.

(default: Show coordinate location configuration)

north|south|west|east|meters|floor:

North : North (Valid for latitude)

South : South (Valid for latitude)

West : West (Valid for longitude)

East : East (Valid for longitude)

Meters : Meters (Valid for altitude)

Floor : Floor (Valid for altitude)

lldpmed Coordinate value

coordinate_value : lldpmed Coordinate value

LLDP MED Datum

Description:

Set or show LLDP-MED Coordinates map datum.

Syntax:

LLDPMED Datum [wgs84|nad83_navd88|nad83_mllw]

Parameters:

wgs84|nad83_navd88|nad83_mllw:

wgs84 : WGS84

nad83_navd88 : NAD83_NAVD88

nad83_mllw : NAD83_MLLW

lldpmed Coordinate datum

LLDP MED Fast

Description:

Set or show LLDP-MED Fast Start Repeat Count.

Syntax:

LLDPMED Fast [<count>]

Parameters:

<count>: The number of times the fast start LLDPDU are being sent during the activation of the fast start mechanism defined by LLDP-MED (1-10).

LLDP MED Info

Description:

Show LLDP-MED neighbor device information.

Syntax:

LLDPMED Info [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Thermal Command

Thermal Prio_temp

Description:

Set or show the temperature at which the ports shall be shut down.

Syntax:

Thermal prio_temp [<prio_list>] [<shut_down_temp>]

Parameters:

<prio_list> : List of priorities (0-3)

<shut_down_temp>: Temperature at which ports shall be shut down (0-255°C)

Thermal Port_prio

Description:

Set or show the ports priority.

Syntax:

Thermal port_prio [<port_list>] [<prio>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<prio> : Priority (0-3)

Thermal Status

Description:

Shows the chip temperature.

Syntax:

Thermal status

Thermal Configuration

Description:

Show thermal_protect configuration.

Syntax:
Thermal configuration

PoE Command

PoE Configuration

Description:
Show PoE configuration.
Syntax:
PoE Configuration

PoE Mode

Description:
Set or show the PoE mode.
Syntax:
PoE Mode [<port_list>] [enable|disable] [af|at]
Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enables PoE
disable : Disable PoE
(default: Show PoE's mode)
af : PoE to af mode
at : PoE to at mode
(default: Show PoE's af/at mode)
Default Setting:
enable

PoE Priority

Description:
Show / Set PoE Priority.
Syntax:
PoE Priority [<port_list>] [low|high|critical]
Parameters:
<port_list>: Port list or 'all', default: All ports
low : Set priority to low
high : Set priority to high
critical: Set priority to critical
(default: Show PoE priority)
Default Setting:
high

PoE Mamagement Mode

Description:
Show / Set PoE management mode.
Syntax:

PoE Mgmt_mode [mgt_class|mgt_alloc|mgt_consumption|mgt_priority]

PoE Allocated Power

Description:

Set or show PoE maximum power allocated per port (0-30.8, with one digit).

Syntax:

PoE Alloc_Power [<port_list>] [<alloc_power>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<alloc_power>: PoE maiximum power allocated for the port (0-30.8)

Default Setting:

30.8

PoE Power Supply

Description:

Set or show the value of the power supply.

Syntax:

PoE Power_Supply [<supply_power>]

Parameters:

<supply_power>: PoE power for a power supply

PoE Status

Description:

Show PoE status.

Syntax:

PoE Status

Ethernet Virtual Connections Command

EVC Configuration

Description:

Show EVC configuration.

Syntax:

EVC Configuration [<port_list>] [<policer_id>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<policer_id>: Policer ID (1-128)

EVC Port DEI

Description:

Set or show port DEI mode.

Syntax:

EVC Port DEI [<port_list>] [<dei_mode>]

Parameters:

<port_list>: Port list or 'all', default: All ports
<dei_mode> : DEI mode: coloured|fixed

EVC Port Tag

Description:
Set or show port tag match mode.
Syntax:
EVC Port Tag [<port_list>] [<tag_mode>]
Parameters:
<port_list>: Port list or 'all', default: All ports
<tag_mode> : Tag mode: inner|outer

EVC Port Addr

Description:
Set or show port address match mode.
Syntax:
EVC Port Addr [<port_list>] [<addr_mode>]
Parameters:
<port_list>: Port list or 'all', default: All ports
<addr_mode>: IP/MAC address mode: source|destination

EVC Port L2CP

Description:
Set or show port L2CP mode
Syntax:
EVC Port L2CP [<port_list>] [<l2cp_list>] [<mode>]
Parameters:
<port_list>: Port list or 'all', default: All ports
<l2cp_list>: L2CP ID list (0-31). BPDU range: 0-15, GARP range: 16-31
<mode> : The mode takes the following values:
normal : Default forwarding
forward : Forward
redirect : Redirect to CPU

EVC Policer

Description:
Set or show EVC bandwidth profile.
Syntax:
EVC Policer [<policer_id>] [enable|disable] [<policer_mode>] [<cir>] [<cbs>] [<eir>] [<ebs>]
Parameters:
<policer_id> : Policer ID (1-128)
enable : Enable policer
disable : Disable policer
<policer_mode>: Policer_mode: coupled|aware
<cir> : Committed Information Rate [kbps]
<cbs> : Committed Burst Size [bytes]

<eir> : Excess Information Rate [kbps]
<ebs> : Excess Burst Size [bytes]

EVC Add

Description:
Add or modify EVC.
Syntax:
EVC Add <evc_id> [<vid>] [<ivid>] [<nni_list>] [<learning>] [inner] [<it_type>] [<it_vid_mode>] [<it_vid>] [<it_preserve>] [<it_pcp>] [<it_dei>] [outer] [<ot_vid>]
Parameters:
<evc_id> : EVC ID (1-128)
<vid> : EVC VLAN ID
<ivid> : Internal VLAN ID
<nni_list> : NNI port list (1-10) or 'none'
<learning> : Learning mode: enable|disable
inner : Inner tag action keyword
<it_type> : Inner tag type: none|c-tag|s-tag|s-custom-tag
<it_vid_mode>: Inner VID mode: normal|tunnel
<it_vid> : Inner tag VLAN ID (1-4095)
<it_preserve>: Inner tag preserved or fixed PCP/DEI: preserved|fixed
<it_pcp> : Inner tag PCP value (0-7)
<it_dei> : Inner tag DEI value (0-1)
outer : Outer tag action keyword
<ot_vid> : EVC outer tag VID for UNI ports

EVC Delete

Description:
Delete EVC.
Syntax:
EVC Delete <evc_id>
Parameters:
<evc_id>: EVC ID (1-128)

EVC Lookup

Description:
Lookup EVC.
Syntax:
EVC Lookup [<evc_id>]
Parameters:
<evc_id>: EVC ID (1-128)

EVC Status

Description:
Show EVC Status.
Syntax:
EVC Status [<evc_id>]
Parameters:

<evc_id>: EVC ID (1-128)

EVC Statistics

Description:

Show or clear EVC statistics.

Syntax:

EVC Statistics [<port_list>] [<class_list>] [<command>]

Parameters:

<port_list> : Port list or 'all', default: All ports
<class_list>: QoS class list, 0-7
<command> : Statistics command: clear|green|yellow|red|discard

EVC ECE Add

Description:

Add or modify EVC Control Entry (ECE):
- If <ece_id> is specified and the ECE exists, the ECE will be modified.
- If <ece_id> is omitted or the ECE does not exist, a new ECE will be added.
- If <ece_id_next> is specified, the ECE will be placed before this entry.
- If <ece_id_next> is 'last', the ECE will be placed at the end of the list.
- If <ece_id_next> is omitted and it is a new ECE, the ECE will be placed last.
- If <ece_id_next> is omitted and the ECE exists, the ECE will not be moved.

Syntax:

EVC ECE Add [<ece_id>] [<ece_id_next>] [uni] [<uni_list>] [<dmac_type>] [<smac>][tag] [<tag_type>] [<vid>] [<pcp>] [<dei>] [all | (ipv4 [<proto>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) | (ipv6 [<proto>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])] [direction] [<direction>] [evc] [<evc_id>] [pop] [<pop>] [policy] [<policy>] [class] [<class>] [outer] [<ot_mode>] [<ot_preserve>] [<ot_pcp>] [<ot_dei>]

Parameters:

<ece_id> : ECE ID (1-128)
<ece_id_next>: Next ECE ID (1-128) or 'last'
uni : UNI keyword
<uni_list> : UNI port list (1-10)
<dmac_type> : DMAC type: any|unicast|multicast|broadcast
<smac> : SMAC or 'any'
tag : Tag matching keyword
<tag_type> : Tag type: tagged|untagged|any
<vid> : VLAN ID value/range (0-4095) or 'any'
<pcp> : PCP value/range (0-7) or 'any'
<dei> : DEI value, 0, 1 or 'any'
all : Keyword for matching any frame type
ipv4 : Keyword for matching IPv4 frames
<proto> : IP protocol value (0-255) or 'any'
<sip> : IPv4 source address (a.b.c.d/n) or 'any'
<dscp> : DSCP value/range (0-63) or 'any'
<fragment> : IPv4 fragment: any|fragment|non-fragment
<sport> : UDP/TCP source port value/range (0-65535) or 'any'
<dport> : UDP/TCP destination port value/range (0-65535) or 'any'

ipv6 : Keyword for matching IPv6 frames
<sip_v6> : IPv6 source address (a.b.c.d/n) or 'any'
direction : Direction keyword
<direction> : ECE direction: both|uni-to-nni|nni-to-uni
evc : EVC keyword
<evc_id> : EVC ID (1-128) or 'none'
pop : Pop keyword
<pop> : Tag pop count: 0|1|2
policy : Policy keyword
<policy> : ACL policy number (0-255)
class : Class keyword
<class> : QoS class, 'disable' or 0-7
outer : Outer tag action keyword
<ot_mode> : Outer tag for nni-to-uni direction: enable|disable
<ot_preserve>: Outer tag preserved or fixed PCP/DEI: preserved|fixed
<ot_pcp> : Outer tag PCP value (0-7)
<ot_dei> : Outer tag DEI value (0-1)

EVC ECE Delete

Description:
Delete ECE.
Syntax:
EVC ECE Delete <ece_id>
Parameters:
<ece_id>: ECE ID (1-128)

EVC ECE Lookup

Description:
Lookup ECE.
Syntax:
EVC ECE Lookup [<ece_id>]
Parameters:
<ece_id>: ECE ID (1-128)

EVC ECE Status

Description:
Show ECE Status.
Syntax:
EVC ECE Status [<ece_id>]
Parameters:
<ece_id>: ECE ID (1-128)

Ethernet Protection Switching Command

EPS Create

Description:

EPS create.

Syntax:

EPS create [<inst>] [domport|dompath|domservice|dommpls] [1p1|1f1] [<flow_w>] [<flow_p>] [<mep_w>] [<mep_p>][<mep_aps>] [enable|disable]

Parameters:

<inst> : Instance number
domport|dompath|domservice|dommpls: Flow domain
1p1|1f1 : EPS architecture
<flow_w> : Working flow instance number
<flow_p> : Protecting flow instance number
<mep_w> : Working MEP instance number
<mep_p> : Protecting MEP instance number
<mep_aps> : APS MEP instance number
enable|disable : enable/disable protection

EPS Config

Description:

EPS config operation.

Syntax:

EPS config [<inst>] [aps|noaps] [revert|norevert] [unidir|bidir] [w0s|w10s|w30s|w1m|w5m|w12m][h0s|h100ms|h500ms|h1s|h2s|h5s|h10s]

Parameters:

<inst> : Instance number
aps|noaps : APS enable/disable
revert|norevert : Revertive enable/disable
unidir|bidir : Unidirectional or bidirectional switching
w0s|w10s|w30s|w1m|w5m|w12m : Wait to restore timer value
h0s|h100ms|h500ms|h1s|h2s|h5s|h10s: Hold off timer value

EPS Command

Description:

EPS command set operation.

Syntax:

EPS command [<inst>] [clear|lockout|forced|manualp|manualw|exercise|freeze|lockoutlocal]

Parameters:

<inst> : Instance number
clear|lockout|forced|manualp|manualw|exercise|freeze|lockoutlocal: EPS protection command type - clear is 'no command active'

EPS State

Description:

Get protection state.

Syntax:

EPS state [<inst>]

Parameters:

<inst>: Instance number

Maintainence entity End Point Command

MEP Config

Description:

MEP instance configuration

'mep|mip' this entity is either a MEP or a MIP - end point or intermediate point

'ingress|egress' this entity is either a Ingress (down) or Egress (up) type of MEP/MIP

'domport|domevc' the domain is either Port or EVC

'level' is the MEG level

'port' is the residence port

'flow' is the related flow instance number - Port number in Port domain - EVC number in EVC domain

'vid' is used for TAGGED OAM in port domain

'itu|ieee' is the MEG ID format

'meg' is the MEG ID - max. 8 char in case of 'ieee' - 6 or 7 char in case of 'itu'

'mep' is the MEP ID.

Syntax:

MEP config [<inst>] [mep|mip] [ingress|egress] [<port>] [domport|domevc] [<level>] [itu|ieee] [<meg>] [<mep>] [<vid>] [<flow>] [enable|disable]

Parameters:

<inst> : Instance number

mep|mip : Mode of the MEP instance

ingress|egress: Direction of the MEP instance

<port> : Port number.

domport|domevc: Flow domain

<level> : MEP level (0-7)

itu|ieee : MEG format

ITU: ICC format as defined in Y.1731 ANNEX A

IEEE: String format Domain Name and Short Name as defined in 802.1ag

<meg> : MEG ID (max. 8 chars)

<mep> : This MEP id (0-0x1FFF)

<vid> : C-TAG only applicable for Port MEP

<flow> : Flow instance number (Port/EVC)

enable|disable: enable/disable

MEP Peer MEP

Description:

MEP Peer MEP id configuration.

Syntax:

MEP peer MEP [<inst>] [<mep>] [<mac_addr>] [enable|disable]

Parameters:

<inst> : Instance number
<mep> : This MEP id (0-0x1FFF)
<mac_addr> : MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit)
enable|disable: enable/disable

MEP Continuity Check Configuration

Description:

MEP Continuity Check configuration
'prio' is the priority (PCP) of transmitted CCM frame
'300s|100s|10s|1s|6m|1m|6h' is the number of CCM frame pr. second.

Syntax:

MEP cc config [<inst>] [<prio>] [300s|100s|10s|1s|6m|1m|6h] [enable|disable]

Parameters:

<inst> : Instance number
<prio> : OAM PDU priority
300s|100s|10s|1s|6m|1m|6h: OAM period (100s -> 100 PDU pr. second)
enable|disable : enable/disable

MEP Loss Measurement Configuration

Description:

MEP Loss Measurement configuration
'prio' is the priority (PCP) of transmitted LM frame
'uni|multi' is selecting uni-cast or multi-cast transmission of LM frame
'single|dual' is selecting single-ended (LMM) or dual-ended (CCM) LM
'10s|1s|6m|1m|6h' is the number of LM frame pr. second
'flr' is the Frame Loss Ratio time interval.

Syntax:

MEP lm config [<inst>] [<prio>] [uni|multi] [single|dual] [10s|1s|6m|1m|6h] [<flr>] [enable|disable]

Parameters:

<inst> : Instance number
<prio> : OAM PDU priority
uni|multi : Destination address is unicast or multicast
single|dual : LM is single or dual ended
10s|1s|6m|1m|6h: LM period (10s -> 10 PDU pr. second)
<flr> : Frame loss ratio (in sec.)
enable|disable : enable/disable

MEP APS Configuration

Description:

MEP APS configuration
'prio' is the priority (PCP) of transmitted APS frame
'uni|multi' is selecting uni-cast or multi-cast transmission of APS frame
'laps|raps' is selecting ELPS or ERPS protocol
'octet' is the last octet in RAPS multicast MAC.

Syntax:

MEP aps config [<inst>] [<prio>] [uni|multi] [laps|raps] [<octet>] [enable|disable]

Parameters:

<inst> : Instance number
<prio> : OAM PDU priority
uni|multi : Destination address is unicast or multicast
laps|raps : Selection of Linear or Ring APS type
<octet> : The last octet in RAPS multicast MAC
enable|disable: enable/disable

MEP Client Configuration

Description:

MEP Client configuration
'domport|domevc' is the client domain - must be EVC
'level' is the client MEG level - the contained level in the AIS and LCK frames
'cflow' is the client flow instance - up to 10 possible client flows (EVC).

Syntax:

MEP client config [<inst>] [domport|domevc] [<level>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>]

Parameters:

<inst> : Instance number
domport|domevc: Flow domain
<level> : MEP level (0-7)
<cflow> : Client flow instance number (EVC)

MEP AIS Configuration

Description:

MEP AIS configuration
'prio' is the priority (PCP) of transmitted AIS frame
'1s|1m' is the number of AIS frame pr. second
'set|clear' is set or clear of protection usability. If set, the first three AIS frames are transmitted as fast as possible - this gives protection reliability in the path end-point.

Syntax:

MEP ais config [<inst>] [<prio>] [1s|1m] [set|clear] [enable|disable]

Parameters:

<inst> : Instance number
<prio> : OAM PDU priority
1s|1m : Transmit period for AIS
1s - to send OAM Frames in the rate of 1 per second
1m - to send OAM frames in the rate of 1 per minute
set|clear : Protection usability set/clear
enable|disable: enable/disable

MEP LCK Configuration

Description:

MEP LCK configuration
'prio' is the priority (PCP) of transmitted AIS frame
'1s|1m' is the number of AIS frame pr. second.

Syntax:

MEP lck config [<inst>] [<prio>] [1s|1m] [enable|disable]

Parameters:

<inst> : Instance number
<prio> : OAM PDU priority
1s|1m : Transmit period for LCK
1s - to send OAM Frames in the rate of 1 per second
1m - to send OAM frames in the rate of 1 per minute
enable|disable: enable/disable

MEP Link Trace Configuration

Description:

MEP Link Trace configuration
'prio' is the priority (PCP) of transmitted LTM frame
'mac_addr' is the unicast MAC of target MEP/MIP
'mep' is the peer MEP-ID of target MEP - only used if 'mac_addr is 'all zero'
'tll' is the TLL in the transmitted LTM.

Syntax:

MEP lt config [<inst>] [<prio>] [<mac_addr>] [<mep>] [<ttl>] [enable|disable]

Parameters:

<inst> : Instance number
<prio> : OAM PDU priority
<mac_addr> : MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit)
<mep> : This MEP id (0-0x1FFF)
<ttl> : LT - Time To Live
enable|disable: enable/disable

MEP Loop Back Configuration

Description:

MEP Loop Back configuration
'set|clear' is set or clear of DEI of transmitted LBM frame
'prio' is the priority (PCP) of transmitted LBM frame
'uni|multi' is selecting uni-cast or multi-cast transmission of LBM frame
'mac_addr' is the unicast MAC of target MEP/MIP
'mep' is the peer MEP-ID of target MEP - only used if 'mac_addr is 'all zero'
'tosend' is the number of LBM to send
'size' is the size of the LBM data field
'gap' is the gap between LBM.

Syntax:

MEP lb config [<inst>] [set|clear] [<prio>] [uni|multi] [<mac_addr>] [<mep>] [<tosend>] [<size>] [<gap>] [enable|disable]

Parameters:

<inst> : Instance number
set|clear : OAM DEI set/clear
<prio> : OAM PDU priority
uni|multi : Destination address is unicast or multicast
<mac_addr> : MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or

'xxxxxxxxxxxx', x is a hexadecimal digit)
<mep> : This MEP id (0-0x1FFF)
<tosend> : Number of LBM to send
<size> : Size of LBM data field in bytes (max 1400)
<gap> : Gap between LBM to send in 10ms. (max 100 - '0' is as fast as possible)
enable|disable: enable/disable

MEP Delay Measurement Configuration

Description:
MEP Delay Measurement configuration
'prio' is the priority (PCP) of transmitted DM frame
'uni|multi' is selecting uni-cast or multi-cast transmission of DM frame
'mep' is the peer MEP-ID of target MEP - only used if 'uni'
'oneway|twoway' is selecting one-way (1DM) or two-way (DMM) DM
'std|prop' is selecting standadized or proprietary DM. the latest is using off-standard follow-up message carrying the exact HW transmit timestamp
'rdtrp|flow' is selecting round-trip or flow delay calculation. Round-trip is not using the far-end timestamps to calculate the far-end residence time
'gap' Gap between transmitting 1DM/DMM PDU - in 10 ms.
'count' number of frames used for average calculation on the latest 'count' frames received
'us|ns' calculation results are shown in micro or nano seconds
'keep|reset' the action in case of total delay counter overflow - either 'keep' all results or 'reset' all results
'd2ford1' this is selecting to used two-way DMM for calculate one-way delay.

Syntax:
MEP dm config [<inst>] [<prio>] [uni|multi] [<mep>] [oneway|twoway] [std|prop] [rdtrp|flow] [<gap>] [<count>] [us|ns] [keep|reset] [d2ford1] [enable|disable]

Parameters:
<inst> : Instance number
<prio> : OAM PDU priority
uni|multi : Destination address is unicast or multicast
<mep> : This MEP id (0-0x1FFF)
oneway|twoway : DM is one-way or two-way
std|prop : Standard or Vitesse proprietary way(w/ follow-up packets) to send DM
rdtrp|flow : 2/4 timestamps selection
<gap> : Gap between 1DM/DMM to send in 10ms(10-65535).
<count> : The number of last records to calculate(10 - 2000)
us|ns : Time resolution
keep|reset : The action to counter when overflow happens
d2ford1 : Enable to use DMM/DMR packets to calculate one-way DM
enable|disable: enable/disable

MEP Test Signal Configuration

Description:
MEP Test Signal configuration
'set|clear' is set or clear of DEI of transmitted LBM frame

'prio' is the priority (PCP) of transmitted TST frame
'mep' is the peer MEP-ID of target MEP - only used if 'mac_addr is 'all zero'
'no_seq|seq' is without and with transmitted sequence numbers
'rate' is the TST frame transmission bit rate in Mbps'
'size' is the size of the un-tagged TST frame - four bytes will be added for each tag
'allzero|allone|onezero' is pattern contained in the TST frame data TLV.

Syntax:

MEP tst config [<inst>] [set|clear] [<prio>] [<mep>] [no_seq|seq] [<rate>] [<size>] [allzero|allone|onezero] [enable|disable]

Parameters:

<inst> : Instance number
set|clear : OAM DEI set/clear
<prio> : OAM PDU priority
<mep> : This MEP id (0-0x1FFF)
no_seq|seq : TST sequence number transmission
<rate> : Transmission bit rate of TST frames - in Mbps
<size> : Size of TST data field in bytes (max 1518)
allzero|allone|onezero: Data pattern to be filled in TST PDU
enable|disable : enable/disable

MEP State

Description:

MEP state get.

Syntax:

MEP state [<inst>]

Parameters:

<inst> : Instance number

MEP Loss Measurement State

Description:

MEP Loss Measurement state get.

Syntax:

MEP lm state [<inst>]

Parameters:

<inst> : Instance number

MEP Loss Measurement State Clear

Description:

MEP Loss Measurement state clear

Syntax:

MEP lm clear <inst>

Parameters:

<inst> : Instance number

MEP Link Trace State

Description:

MEP Link Trace state get.

Syntax:
MEP lt state [<inst>]
Parameters:
<inst> : Instance number

MEP Loop Back State

Description:
MEP Loop Back state get.
Syntax:
MEP lb state [<inst>]
Parameters:
<inst> : Instance number

MEP Delay Measurement State

Description:
MEP Delay Measurement state get.
Syntax:
MEP dm state [<inst>]
Parameters:
<inst> : Instance number

MEP Delay Measurement State Clear

Description:
MEP Delay Measurement state clear
Syntax:
MEP dm clear <inst>
Parameters:
<inst> : Instance number

MEP Test Signal State

Description:
MEP Test Signal state get
RX rate is shown in 100 Kbps.
Syntax:
MEP tst state [<inst>]
Parameters:
<inst> : Instance number

MEP Test Signal State Clear

Description:
MEP Test Signal state clear
Syntax:
MEP tst clear <inst>
Parameters:
<inst> : Instance number

Quality of Service Command

QoS Configuration

Description:

Show QoS Configuration.

Syntax:

QoS Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

QoS Port Classification Class

Description:

Set or show the default QoS class.

Syntax:

QoS Port Classification Class [<port_list>] [<class>]

Parameters:

<port_list>: Port list or 'all', default: All ports
<class> : QoS class (0-7)

Default Setting:

0

Example:

Set default QoS class in 1 for port 1

```
NS3502-8P-2T-2S-V2:/>qos Port Classification Class 1 1
```

QoS Port Classification DPL

Description:

Set or show the default Drop Precedence Level.

Syntax:

QoS Port Classification DPL [<port_list>] [<dpl>]

Parameters:

<port_list>: Port list or 'all', default: All ports
<dpl> : Drop Precedence Level (0-1)

Default Setting:

0

Example:

Set the default Drop Precedence Level in 1 for port1

```
NS3502-8P-2T-2S-V2:/>qos Port Classification dpl 1 1
```

QoS Port Classification PCP

Description:

Set or show the default PCP for an untagged frame.

Syntax:

QoS Port Classification PCP [<port_list>] [<pcp>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<pcp> : Priority Code Point (0-7)

Default Setting:

0

Example:

Set the default PCP for an untagged frame in 1 for port1

```
NS3502-8P-2T-2S-V2:/>qos Port Classification pcp 1 1
```

QoS Port Classification DEI

Description:

Set or show the default DEI for an untagged frame.

Syntax:

QoS Port Classification DEI [<port_list>] [<dei>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<dei> : Drop Eligible Indicator (0-1)

Default Setting:

0

Example:

Set the default DEI for an untagged frame in 1 for port1.

```
NS3502-8P-2T-2S-V2:/>qos Port Classification dei 1 1
```

QoS Port Classification Tag

Description:

Set or show if the classification is based on the PCP and DEI values in tagged frames.

Syntax:

QoS Port Classification Tag [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable tag classification

disable : Disable tag classification

(default: Show tag classification mode)

Default Setting:

disable

Example:

Enable QoS port classification Tag.

```
NS3502-8P-2T-2S-V2:/>qos Port Classification tag 1-10 enable
```

QoS Port Classification Map

Description:

Set or show the port classification map.

This map is used when port classification tag is enabled,and the purpose is to translate the Priority Code Point (PCP) and Drop Eligible Indicator (DEI) from a tagged frame to QoS class and DP level.

Syntax:
QoS Port Classification Map [<port_list>] [<pcp_list>] [<dei_list>] [<class>] [<dpl>]
Parameters:
<port_list>: Port list or 'all', default: All ports
<pcp_list> : PCP list or 'all', default: All PCPs (0-7)
<dei_list> : DEI list or 'all', default: All DEIs (0-1)
<class> : QoS class (0-7)
<dpl> : Drop Precedence Level (0-1)

QoS Port Classification DSCP

Description:
Set or show if the classification is based on DSCP value in IP frames.
Syntax:
QoS Port Classification DSCP [<port_list>] [enable|disable]
Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable DSCP based classification
disable : Disable DSCP based classification
(default: Show DSCP based classification mode)
Default Setting:
disable
Example:
Enable QoS port classification DSCP.

```
NS3502-8P-2T-2S-V2:/>qos Port Classification dscp 1-10 enable
```

QoS Port Policer Mode

Description:
Set or show the port policer mode
Syntax:
QoS Port Policer Mode [<port_list>] [enable|disable]
Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable port policer
disable : Disable port policer
(default: Show port policer mode)
Default Setting:
disable
Example:
Enable QoS port policer

```
NS3502-8P-2T-2S-V2:/>qos Port Policer Mode 1-10 enable
```

QoS Port Policer Rate

Description:
Set or show the port policer rate.
Syntax:
QoS Port Policer Rate [<port_list>] [<rate>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<rate> : Rate in kbps or fps (100-15000000)

Default Setting:

500

Example:

Set the port policer rate in 1000

```
NS3502-8P-2T-2S-V2:/>qos Port Policer Rate 1-10 1000
```

QoS Port Policer Unit

Description:

Set or show the port policer unit.

Syntax:

QoS Port Policer Unit [<port_list>] [kbps|fps]

Parameters:

<port_list>: Port list or 'all', default: All ports

kbps : Unit is kilo bits per second

fps : Unit is frames per second

(default: Show port policer unit)

Default Setting:

kbps

Example:

Set the port policer unit in fps

```
NS3502-8P-2T-2S-V2:/>qos Port Policer unit 1-10 fps
```

QoS Port Policer Flow Control

Description:

Set or show the port policer flow control.

If policer flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Syntax:

QoS Port Policer FlowControl [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port policer flow control

disable : Disable port policer flow control

(default: Show port policer flow control mode)

Default Setting:

disable

QoS Port QueuePolicer Mode

Description:

Set or show the port queue policer mode.

Syntax:

QoS Port QueuePolicer Mode [<port_list>] [<queue_list>] [enable|disable]

Parameters:

<port_list> : Port list or 'all', default: All ports
<queue_list>: Queue list or 'all', default: All queues (0-7)
enable : Enable port queue policer
disable : Disable port queue policer
(default: Show port queue policer mode)

Default Setting:
Disable

QoS Port QueuePolicer Rate

Description:
Set or show the port queue policer rate.

Syntax:
QoS Port QueuePolicer Rate [<port_list>] [<queue_list>] [<bit_rate>]

Parameters:
<port_list> : Port list or 'all', default: All ports
<queue_list>: Queue list or 'all', default: All queues (0-7)
<bit_rate> : Rate in kilo bits per second (100-3300000)

Default Setting:
500

QoS Port Scheduler Mode

Description:
Set or show the port scheduler mode.

Syntax:
QoS Port Scheduler Mode [<port_list>] [strict|weighted]

Parameters:
<port_list>: Port list or 'all', default: All ports
strict : Strict mode
weighted: Weighted mode
(default: Show port scheduler mode)

Default Setting:
strict

Example:
Set the port schedule mode in weighted mode

```
NS3502-8P-2T-2S-V2:/>qos Port Scheduler Mode 1-10 weighted
```

QoS Port Scheduler Weight

Description:
Set or show the port scheduler weight.

Syntax:
QoS Port Scheduler Weight [<port_list>] [<queue_list>] [<weight>]

Parameters:
<port_list> : Port list or 'all', default: All ports
<queue_list>: Weighted queue list or 'all', default: All weighted queues (0-5)
<weight> : Scheduler weight (1-100)

QoS Port QueueShaper Mode

Description:

Set or show the port queue shaper mode.

Syntax:

QoS Port QueueShaper Mode [<port_list>] [<queue_list>] [enable|disable]

Parameters:

<port_list> : Port list or 'all', default: All ports
<queue_list>: Queue list or 'all', default: All queues (0-7)
enable : Enable port queue shaper
disable : Disable port queue shaper
(default: Show port queue shaper mode)

Default Setting:

disable

Example:

Enable port queue shaper for all port & queue

```
NS3502-8P-2T-2S-V2:/>qos Port QueueShaper Mode 1-10 0-7 enable
```

QoS Port QueueShaper Rate

Description:

Set or show the port queue shaper rate.

Syntax:

QoS Port QueueShaper Rate [<port_list>] [<queue_list>] [<bit_rate>]

Parameters:

<port_list> : Port list or 'all', default: All ports
<queue_list>: Queue list or 'all', default: All queues (0-7)
<bit_rate> : Rate in kilo bits per second (100-3300000)

Default Setting:

500kbps

Example:

Set the port queue shaper rate in 1000

```
NS3502-8P-2T-2S-V2:/>qos Port QueueShaper rate 1-10 0-7 1000
```

QoS Port QueueShaper Excess

Description:

Set or show the port queue excess bandwidth mode.

Syntax:

QoS Port QueueShaper Excess [<port_list>] [<queue_list>] [enable|disable]

Parameters:

<port_list> : Port list or 'all', default: All ports
<queue_list>: Queue list or 'all', default: All queues (0-7)
enable : Enable use of excess bandwidth
disable : Disable use of excess bandwidth
(default: Show port queue excess bandwidth mode)

Default Setting:

disable

Example:

Enable the port queue excess bandwidth mode.

```
NS3502-8P-2T-2S-V2:/>qos Port QueueShaper Excess 1-10 0-7 enable
```

QoS Port TagRemarking Mode

Description:

Set or show the port tag remarking mode.

Syntax:

QoS Port TagRemarking Mode [<port_list>] [classified|default|mapped]

Parameters:

<port_list>: Port list or 'all', default: All ports
classified: Use classified PCP/DEI values
default : Use default PCP/DEI values
mapped : Use mapped versions of QoS class and DP level
(default: Show port tag remarking mode)

Default Setting:

classified

Example:

Set the port tag remarking mode in mapped.

```
NS3502-8P-2T-2S-V2:/>qos Port TagRemarking Mode 1-10 mapped
```

QoS Port TagRemarking PCP

Description:

Set or show the default PCP. This value is used when port tag remarking mode is set to 'default'.

Syntax:

QoS Port TagRemarking PCP [<port_list>] [<pcp>]

Parameters:

<port_list>: Port list or 'all', default: All ports
<pcp> : Priority Code Point (0-7)

Default Setting:

0

Example:

Set the default PCP in 1.

```
NS3502-8P-2T-2S-V2:/>qos Port TagRemarking PCP 1-10 1
```

QoS Port TagRemarking DEI

Description:

Set or show the default DEI. This value is used when port tag remarking mode is set to 'default'.

Syntax:

QoS Port TagRemarking DEI [<port_list>] [<dei>]

Parameters:

<port_list>: Port list or 'all', default: All ports
<dei> : Drop Eligible Indicator (0-1)

Default Setting:

0

Example:

Set the default EDI in 1.

```
NS3502-8P-2T-2S-V2:/>qos Port TagRemarking EDI 1-10 1
```

QoS Port TagRemarking Map

Description:

Set or show the port tag remarking map. This map is used when port tag remarking mode is set to 'mapped', and the purpose is to translate the classified QoS class (0-7) and DP level (0-1) to PCP and DEI.

Syntax:

QoS Port TagRemarking Map [<port_list>] [<class_list>] [<dpl_list>] [<pcp>] [<dei>]

Parameters:

<port_list> : Port list or 'all', default: All ports
<class_list>: QoS class list or 'all', default: All QoS classes (0-7)
<dpl_list> : DP level list or 'all', default: All DP levels (0-1)
<pcp> : Priority Code Point (0-7)
<dei> : Drop Eligible Indicator (0-1)

QoS Port DSCP Translation

Description:

Set or show DSCP ingress translation mode.
If translation is enabled for a port, incoming frame DSCP value is translated and translated value is used for QoS classification.

Syntax:

QoS Port DSCP Translation [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable DSCP ingress translation
disable : Disable DSCP ingress translation
(default: Show DSCP ingress translation mode)

Default Setting:

disable

Example:

Enable DSCP ingress translation on all port.

```
NS3502-8P-2T-2S-V2:/>qos Port DSCP Translation 1-10 enable
```

QoS Port DSCP Classification

Description:

Set or show DSCP classification based on QoS class and DP level.
This enables per port to map new DSCP value based on QoS class and DP level.

Syntax:

QoS Port DSCP Classification [<port_list>] [none|zero|selected|all]

Parameters:

<port_list>: Port list or 'all', default: All ports
none : No DSCP ingress classification
zero : Classify DSCP if DSCP = 0

selected : Classify DSCP for which class. mode is 'enable'
all : Classify all DSCP
(default: Show port DSCP ingress classification mode)

Default Setting:
none

Example:
Set DSCP classification based on QoS class and DP level in zero

```
NS3502-8P-2T-2S-V2:/> QoS Port DSCP Classification 1-10 zero
```

QoS Port DSCP EgressRemark

Description:
Set or show the port DSCP remarking mode.

Syntax:
QoS Port DSCP EgressRemark [<port_list>] [disable|enable|remap_dp_unaware|remap_dp_aware]

Parameters:
<port_list>: Port list or 'all', default: All ports
disable : Disable DSCP egress rewrite
enable : Enable DSCP egress rewrite with the value received from analyzer
remap_dp_unaware : Rewrite DSCP in egress frame with remapped DSCP where remap is DP unaware or DP = 0
remap_dp_aware : Rewrite DSCP in egress frame with remapped DSCP where remap is DP aware and DP = 1
(default: Show port DSCP egress remarking mode)

Default Setting:
disable

Example:
Enable DSCP egress rewrite

```
NS3502-8P-2T-2S-V2:/> QoS Port DSCP EgressRemark 1-10 enable
```

QoS DSCP Map

Description:
Set or show DSCP mapping table.
This table is used to map QoS class and DP level based on DSCP value.
DSCP value used to map QoS class and DPL is either translated DSCP value or incoming frame DSCP value.

Syntax:
QoS DSCP Map [<dscp_list>] [<class>] [<dpl>]

Parameters:
<dscp_list>: DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'
(default: Show DSCP ingress map table i.e. DSCP->(class, DPL))
<class> : QoS class (0-7)
<dpl> : Drop Precedence Level (0-1)

QoS DSCP Translation

Description:

Set or show global ingress DSCP translation table.
If port DSCP translation is enabled, translation table is used to translate incoming frames DSCP value and translated value is used to map QoS class and DP level.

Syntax:

QoS DSCP Translation [<dscp_list>] [<trans_dscp>]

Parameters:

<dscp_list> : DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'
(default: Show DSCP translation table)
<trans_dscp>: Translated DSCP: 0-63, BE, CS1-CS7, EF or AF11-AF43

QoS DSCP Trust

Description:

Set or show trusted DSCP value which is used for QoS classification.
The DSCP value to be checked for trust is either translated value ifDSCP translation is enabled for the ingress port or incoming frame DSCPvalue if translation is disabled for the port. Trusted DSCP value is onlyused for QoS classification.

Syntax:

QoS DSCP Trust [<dscp_list>] [enable|disable]

Parameters:

<dscp_list>: DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'
enable : Set DSCP as trusted DSCP
disable : Set DSCP as un-trusted DSCP
(default: Show DSCP Trust status)

Default Setting:

disable

QoS DSCP Classification Mode

Description:

Set or show DSCP ingress classification mode.
If port DSCP classification is 'selected', DSCP will be classified based on QoS class and DP level only for DSCP value with classification mode 'enabled'. DSCP may be translated DSCP if translation is enabled for the port.

Syntax:

QoS DSCP Classification Mode [<dscp_list>] [enable|disable]

Parameters:

<dscp_list>: DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'
enable : Enable DSCP ingress classification
disable : Disable DSCP ingress classification
(default: Show DSCP classification mode)

Default Setting:

disable

QoS DSCP EgressRemap

Description:

Set or show DSCP egress remap table. This table is used if the port egress

remarking mode is 'remap' and the purpose is to map the DSCP and DP level to a new DSCP value.

Syntax:

QoS DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]

Parameters:

<dscp_list>: DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'
<dpl_list> : DP level list or 'all', default: All DP levels (0-1)
<dscp> : Egress remapped DSCP: 0-63, BE, CS1-CS7, EF or AF11-AF43

QoS Storm Unicast

Description:

Set or show the unicast storm rate limiter.

Syntax:

QoS Storm Unicast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable unicast storm control
disable : Disable unicast storm control
<packet_rate>: Rate in fps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 32768k)

Default Setting:

disable

Example:

Enable unicast storm control in 2fps

```
NS3502-8P-2T-2S-V2:/> QoS Storm Unicast enable 2
```

QoS Storm Multicast

Description:

Set or show the multicast storm rate limiter.

Syntax:

QoS Storm Multicast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable multicast storm control
disable : Disable multicast storm control
<packet_rate>: Rate in fps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 32768k)

Default Setting:

disable

Example:

Enable multicast storm control in 2fps

```
NS3502-8P-2T-2S-V2:/> QoS Storm multicast enable 2
```

QoS Storm Broadcast

Description:

Set or show the broadcast storm rate limiter. The limiter will only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

Syntax:

QoS Storm Broadcast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable broadcast storm control
disable : Disable broadcast storm control
<packet_rate>: Rate in fps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

disable

QoS QCL Add

Description:

Add or modify QoS Control Entry (QCE).
If the QCE ID parameter <qce_id> is specified and an entry with this QCE ID already exists, the QCE will be modified. Otherwise, a new QCE will be added. If the QCE ID is not specified, the next available QCE ID will be used. If the next QCE ID parameter <qce_id_next> is specified, the QCE will be placed before this QCE in the list. If the next QCE ID is not specified and if it is a new entry added, the QCE will be placed last in the list. Otherwise if the next QCE ID is not specified and if existing QCE is modified, QCE will be in the same location in the list. To modify and move the entry to last in the list, use the word 'last' for <qce_id_next>.

Syntax:

QoS QCL Add [<qce_id>] [<qce_id_next>] [<port_list>] [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>] [(etype [<etype>]) | (LLC [<DSAP>] [<SSAP>] [<control>]) | (SNAP [<PID>]) | (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) | (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])] [<class>] [<dp>] [<classified_dscp>]

Parameters:

<qce_id> : QCE ID (1-256), default: Next available ID
<qce_id_next> : Next QCE ID: "next_id (1-256) or 'last'"
<port_list> : Port List: "port <port_list> or 'all'", default: All ports
<tag> : Frame tag: untag|tag|any
<vid> : VID: 1-4095 or 'any', either a specific VID or range of VIDs
<pcp> : Priority Code Point: 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: 0-1 or 'any'
<smac> : Source MAC address: (xx-xx-xx) or 'any', 24 MS bits (OUI)
<dmac_type> : Destination MAC type: unicast|multicast|broadcast|any
etype : Ethernet Type keyword
<etype> : Ethernet Type: 0x600-0xFFFF or 'any' but excluding 0x800(IPv4) and 0x86DD(IPv6)
llc : LLC keyword
<dsap> : Destination Service Access Point: 0x00-0xFF or 'any'
<ssap> : Source Service Access Point: 0x00-0xFF or 'any'
<control> : LLC control: 0x00-0xFF or 'any'
snap : SNAP keyword
<pid> : Protocol ID (EtherType) or 'any'
ipv4 : IPv4 keyowrd
<protocol> : IP protocol number: (0-255, TCP or UDP) or 'any'
<sip> : Source IP address: (a.b.c.d/n) or 'any'
<dscp> : DSCP:(0-63,BE,CS1-CS7,EF or AF11-AF43)or'any',specific/range
<fragment> : IPv4 frame fragmented: yes|no|any
<sport> : Source TCP/UDP port:(0-65535) or 'any',specific or port range

<dport> : Dest. TCP/UDP port:(0-65535) or 'any', specific or port range
ipv6 : IPv6 keyowrd
<sip_v6> : IPv6 source address: (a.b.c.d/n) or 'any', 32 LS bits
<class> : QoS Class: "class (0-7)", default: basic classification
<dp> : DP Level: "dp (0-1)", default: basic classification
<classified_dscp>: DSCP: "dscp (0-63, BE, CS1-CS7, EF or AF11-AF43)"

QoS QCL Delete

Description:
Delete QCE entry from QoS Control list.
Syntax:
QoS QCL Delete <qce_id>
Parameters:
<qce_id>: QCE ID (1-256), default: Next available ID
Default Setting:
disable
Example:
Enable multicast storm control in 2fps

NS3502-8P-2T-2S-V2:/> **QoS Storm multicast enable 2**

QoS QCL Lookup

Description:
Lookup QoS Control List.
Syntax:
QoS QCL Lookup [<qce_id>]
Parameters:
<qce_id>: QCE ID (1-256), default: Next available ID
Default Setting:
disable
Example:
Enable multicast storm control in 2fps

NS3502-8P-2T-2S-V2:/> **QoS Storm multicast enable 2**

QoS QCL Status

Description:
Show QCL status. This can be used to display if there is any conflict in QCE for differnet user types.
Syntax:
QoS QCL status [combined|static|voice_vlan|conflicts]
Parameters:
combined|static|voice_vlan|conflicts: combined **:** Shows the combined status
static : Shows the static user configured status
voice_vlan : Shows the status by Voice VLAN
conflicts : Shows all conflict status
(default : Shows the combined status)

QoS QCL Refresh

Description:

Resolve QCE conflict status. Same H/W resource is shared by multiple applications and it may not be available even before MAX QCE entry. So user can release the resource in use by other applications and use this command to acquire the resource.

Syntax:

QoS QCL refresh

Parameters:

combined|static|voice_vlan|conflicts: combined **:** Shows the combined status

static : Shows the static user configured status

voice_vlan : Shows the status by Voice VLAN

conflicts : Shows all conflict status

(default : Shows the combined status)

Default Setting:

disable

Example:

Enable multicast storm control in 2fps

```
NS3502-8P-2T-2S-V2:/> QoS Storm multicast enable 2
```

Mirror Command

Mirror Configuration

Description:

Show mirror configuration.

Syntax:

Mirror Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show mirror configuration.

```
NS3502-8P-2T-2S-V2:/>mirror configuration
```

Mirror Port

Description:

Set or show the mirror port.

Syntax:

Mirror Port [<port>|disable]

Parameters:

<port>|disable: Mirror port or 'disable', default: Show port

Default Setting:

disable

Example:

Set port 2 for the mirror port.

```
NS3502-8P-2T-2S-V2:/>mirror port 2
```

Mirror Mode

Description:

Set or show the mirror mode.

Syntax:

Mirror Mode [<port_list>] [enable|disable|rx|tx]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable Rx and Tx mirroring
disable: Disable Mirroring
rx : Enable Rx mirroring
tx : Enable Tx mirroring
(default: Show mirror mode)

Default Setting:

disable

Example:

Enable the mirror mode for port 1-4.

```
NS3502-8P-2T-2S-V2:/>mirror mode 1-4 enable
```

Configuration Command

Configuration Save

Description:

Save configuration to TFTP server.

Syntax:

Config Save <ip_server> <file_name>

Parameters:

<ip_server>: TFTP server IP address (a.b.c.d)
<file_name>: Configuration file name

Configuration Load

Description:

Load configuration from TFTP server.

Syntax:

Config Load <ip_server> <file_name> [check]

Parameters:

<ip_server>: TFTP server IP address (a.b.c.d)
<file_name>: Configuration file name
check : Check configuration file only, default: Check and apply file

Firmware Command

Firmware Load

Description:

Load new firmware from TFTP server.

Syntax:

Firmware Load <ip_addr_string> <file_name>

Parameters:

<ip_addr_string>: IP host address (a.b.c.d) or a host name string
<file_name> : Firmware file name

Firmware IPv6 Load

Description:

Load new firmware from IPv6 TFTP server.

Syntax:

Firmware IPv6 Load <ipv6_server> <file_name>

Parameters:

<ipv6_server>: TFTP server IPv6 address
<file_name> : Firmware file name

Firmware Information

Description:

Display information about active and alternate firmware images.

Syntax:

Firmware Information

Firmware Swap

Description:

Activate the alternate firmware image..

Syntax:

Firmware Swap

UPnP Command

UPnP Configuration

Description:

Show UPnP configuration.

Syntax:

UPnP Configuration

Example:

Show UPnP configuration.

```
NS3502-8P-2T-2S-V2:/>upnp configuration
```

```
UPnP Configuration:
===================

UPnP Mode              : Disabled
UPnP TTL               : 4
UPnP Advertising Duration : 100
```

UPnP Mode

Description:

Set or show the UPnP mode.

Syntax:

UPnP Mode [enable|disable]

Parameters:

enable : Enable UPnP

disable: Disable UPnP

(default: Show UPnP mode)

Default Setting:

disable

Example:

Enable the UPnP mode.

```
NS3502-8P-2T-2S-V2:/>upnp mode enable
```

UPnP TTL

Description:

Set or show the TTL value of the IP header in SSDP messages.

Syntax:

UPnP TTL [<ttl>]

Parameters:

<ttl>: ttl range (1..255), default: Show UPnP TTL

Default Setting:

4

Example:

Set the value 10 for TTL value of the IP header in SSDP messages.

```
NS3502-8P-2T-2S-V2:/>upnp ttl 10
```

UPnP Advertising Duration

Description:

Set or show UPnP Advertising Duration.

Syntax:

UPnP Advertising Duration [<duration>]

Parameters:

<duration>: duration range (100..86400), default: Show UPnP duration range

Default Setting:

100

Example:

Set value 1000 for UPnP Advertising Duration.

```
NS3502-8P-2T-2S-V2:/>upnp advertising duration 1000
```

MVR Command

MVR Configuration

Description:

Show the MVR configuration.

Syntax:

MVR Configuration

Example:

Show the MVR configuration.

```
NS3502-8P-2T-2S-V2:/>mvr configuration

MVR Configuration:
==================

MVR Mode: Disabled
Muticast VLAN ID: 100

Port  Port Mode    Port Type    Immediate Leave
----  ----------  ----------  ---------------
1     Disabled    Receive     Disabled
2     Disabled    Receive     Disabled
3     Disabled    Receive     Disabled
4     Disabled    Receive     Disabled
5     Disabled    Receive     Disabled
6     Disabled    Receive     Disabled
7     Disabled    Receive     Disabled
8     Disabled    Receive     Disabled
9     Disabled    Receive     Disabled
10    Disabled    Receive     Disabled
```

MVR Mode

Description:

Set or show the MVR mode.

Syntax:

MVR Mode [enable|disable]

Parameters:

enable : Enable MVR mode

disable : Disable MVR mode

(default: Show MVR mode)

Default Setting:

disable

Example:

Enable MVR mode.

```
NS3502-8P-2T-2S-V2:/>mvr mode enable
```

MVR VLAN Setup

Description:

Set or show per MVR VLAN configuration.

Syntax:

MVR VLAN Setup [<mvid>] [add|del|upd] [(Name <mvr_name>)]

Parameters:

<mvid> : MVR VLAN ID (1-4095)
add : Add operation
del : Delete operation
upd : Update operation
name : MVR Name keyword
<mvr_name>: MVR VLAN name (Maximum of 32 characters)

MVR VLAN Mode

Description:

Set or show per MVR VLAN mode.

Syntax:

MVR VLAN Mode [<vid>|<mvr_name>] [dynamic|compatible]

Parameters:

<vid>|<mvr_name>: MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)
dynamic : Dynamic MVR mode
compatible: Compatible MVR mode
(default: Show MVR VLAN mode)

MVR VLAN Port

Description:

Set or show per MVR VLAN port role.

Syntax:

MVR VLAN Port [<vid>|<mvr_name>] [<port_list>] [source|receiver|inactive]

Parameters:

<vid>|<mvr_name>: MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)
<port_list> : Port list or 'all', default: All ports
source : MVR source port
receiver : MVR receiver port
inactive : Disable MVR
(default: Show MVR port role)

MVR VLAN LLQI

Description:

Set or show per MVR VLAN LLQI (Last Listener Query Interval).

Syntax:
MVR VLAN LLQI [<vid>|<mvr_name>] [mvr_param_llqi]
Parameters:
<vid>|<mvr_name>: MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)
mvr_param_llqi :
-1 : Default Value (5)
0~31744 : Last Listener Query Interval in tenths of seconds
(default: Show MVR Interface Last Listener Query Interval

MVR VLAN Channel

Description:
Set or show per MVR VLAN channel.
Syntax:
MVR VLAN Channel [<vid>|<mvr_name>] [add|del|upd] [channel] [channel_bound] [(Name <grp_name>)]
Parameters:
<vid>|<mvr_name>: MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)
add : Add operation
del : Delete operation
upd : Update operation
channel : IPv4/IPv6 multicast group address
channel_bound : The boundary IPv4/IPv6 multicast group address for the channel
name : MVR Name keyword
<grp_name> : MVR Channel name. (Maximum of 32 characters)

MVR VLAN Priority

Description:
Set or show per MVR VLAN priority and VLAN tag.
Syntax:
MVR VLAN Priority [<vid>|<mvr_name>] [priority] [tagged|untagged]
Parameters:
<vid>|<mvr_name>: MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)
priority : CoS priority value ranges from 0 ~ 7
tagged : Tagged IGMP/MLD frames will be sent
untagged : Untagged IGMP/MLD frames will be sent

MVR Immediate Leave

Description:
Set or show MVR immediate leave per port.
Syntax:
MVR Immediate Leave [<port_list>] [enable|disable]
Parameters:
<<port_list>: Port list or 'all', default: All ports
enable : Enable Immediate Leave

disable : Disable Immediate Leave
(default: Show MVR Immediate Leave)

MVR Status

Description:
Show/Clear MVR operational status.
Syntax:
MVR Status [<vid>] [clear]
Parameters:
<vid>: VLAN ID (1-4095)
clear : Clear log

MVR Groups

Description:
Show MVR group addresses.
Syntax:
MVR Groups [<vid>]
Parameters:
<vid>: VLAN ID (1-4095)

MVR SFM

Description:
Show SFM (including SSM) related information for MVR.
Syntax:
MVR SFM [<vid>] [<port_list>]
Parameters:
<vid> : VLAN ID (1-4095)
<port_list>: Port list or 'all', default: All ports

Voice VLAN Command

Voice VLAN Configuration

Description:
Show Voice VLAN configuration.
Syntax:
Voice VLAN Configuration
Example:
Show Voice VLAN configuration.

```
NS3502-8P-2T-2S-V2:/>voice vlan configuration

V oice VLAN Configuration:
==========================

Voice VLAN Mode              : Disabled
```

```
Voice VLAN VLAN ID          : 1000
Voice VLAN Age Time(seconds)  : 86400
Voice VLAN Traffic Class      : 7

Voice VLAN OUI Table:
=====================

Telephony OUI Description
------------ -----------
00-03-6B     Cisco phones
00-0F-E2     H3C phones
00-60-B9     Philips and NEC AG phones
00-D0-1E     Pingtel phones
00-E0-75     Polycom phones
00-E0-BB     3Com phones
00-01-E3     Siemens AG phones

Voice VLAN Port Configuration:
==============================


Port  Mode     Security  Discovery Protocol
----  -------- --------  ------------------
1     Disabled  Disabled    OUI
2     Disabled  Disabled    OUI
3     Disabled  Disabled    OUI
4     Disabled  Disabled    OUI
5     Disabled  Disabled    OUI
6     Disabled  Disabled    OUI
7     Disabled  Disabled    OUI
8     Disabled  Disabled    OUI
9     Disabled  Disabled    OUI
10    Disabled  Disabled    OUI
```

Voice VLAN Mode

Description:

Set or show the Voice VLAN mode.
We must disable MSTP feature before we enable Voice VLAN.
It can avoid the conflict of ingress filter.

Syntax:

Voice VLAN Mode [enable|disable]

Parameters:

enable : Enable Voice VLAN mode.
disable: Disable Voice VLAN mode
(default: Show flow Voice VLAN mode)

Default Setting:

disable

Example:

Enable the Voice VLAN mode.

```
NS3502-8P-2T-2S-V2:/>voice vlan mode enable
```

Voice VLAN ID

Description:

Set or show Voice VLAN ID.

Syntax:

Voice VLAN ID [<vid>]

Parameters:

<vid>: VLAN ID (1-4095)

Default Setting:

1000

Example:

Set ID 2 for Voice VLAN ID.

```
NS3502-8P-2T-2S-V2:/>voice vlan id 2
```

Voice VLAN Agetime

Description:

Set or show Voice VLAN age time.

Syntax:

Voice VLAN Agetime [<age_time>]

Parameters:

<age_time>: MAC address age time (10-10000000) default: Show age time

Default Setting:

86400sec

Example:

Set Voice VLAN age time in 100sec.

```
NS3502-8P-2T-2S-V2:/>voice valn agetime 100
```

Voice VLAN Traffic Class

Description:

Set or show Voice VLAN ID.

Syntax:

Voice VLAN Traffic Class [<class>]

Parameters:

<class>: Traffic class (0-7)

Default Setting:

7

Example:

Set 4 traffic class for voice VLAN

```
NS3502-8P-2T-2S-V2:/>voice vlan traffic class4
```

Voice VLAN OUI Add

Description:

Add Voice VLAN OUI entry.

Modify OUI table will restart auto detect OUI process. The maximum entry number is (16).

Syntax:

Voice VLAN OUI Add <oui_addr> [<description>]

Parameters:

<oui_addr> : OUI address (xx-xx-xx). The null OUI address isn't allowed

<description>: Entry description. Use 'clear' or "" to clear the string

No blank or space characters are permitted as part of a contact. (only in CLI)

Example:

Add Voice VLAN OUI entry.

```
NS3502-8P-2T-2S-V2:/>voice vlan oui add 00-11-22 test
```

Voice VLAN OUI Delete

Description:

Delete Voice VLAN OUI entry.

Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Delete <oui_addr>

Parameters:

<oui_addr>: OUI address (xx-xx-xx). The null OUI address isn't allowed

Example:

Delete Voice VLAN OUI entry.

```
NS3502-8P-2T-2S-V2:/>voice vlan oui delete 00-11-22
```

Voice VLAN OUI Clear

Description:

Clear Voice VLAN OUI entry.

Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Clear

Example:

Clear Voice VLAN OUI entry.

```
NS3502-8P-2T-2S-V2:/>voice vlan oui clear
```

Voice VLAN OUI Lookup

Description:

Clear Voice VLAN OUI entry. Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Clear

Example:

Lookup Voice VLAN OUI entry.

```
NS3502-8P-2T-2S-V2:/>voice vlan oui lookup
```

Voice VLAN Port Mode

Description:

Set or show the Voice VLAN port mode.
When the port mode isn't disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter.

Syntax:

Voice VLAN Port Mode [<port_list>] [disable|auto|force]

Parameters:

<port_list>: Port list or 'all', default: All ports
disable : Disjoin from Voice VLAN.
auto : Enable auto detect mode. It detects whether there is VoIP phone attached on the specific port and configures the Voice VLAN members automatically.
force : Forced join to Voice VLAN.
(default: Show Voice VLAN port mode)

Default Setting:

disable

Example:

Set auto mode for port 1-4 of Voice VLAN port mode.

```
NS3502-8P-2T-2S-V2:/>voice vlan port mode 1-4 auto
```

Voice VLAN Security

Description:

Set or show the Voice VLAN port security mode. When the function is enabled, all non-telephone MAC address in Voice VLAN will be blocked 10 seconds.

Syntax:

Voice VLAN Security [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports
enable : Enable Voice VLAN security mode.
disable: Disable Voice VLAN security mode
(default: Show flow Voice VLAN security mode)

Default Setting:

disable

Example:

Enable the Voice VLAN port security mode for port 1-4.

```
NS3502-8P-2T-2S-V2:/>voice vlan security 1-4 enable
```

Voice VLAN Discovery Protocol

Description:

Set or show the Voice VLAN port discovery protocol mode. It only works when auto detect mode is enabled. The LLDP feature should be enabled before configuring discovery protocol to 'LLDP' or 'Both'. Change the discovery protocol to 'OUI' or 'LLDP' to restart the auto detect process.

Syntax:
Voice VLAN Discovery Protocol [<port_list>] [oui|lldp|both]
Parameters:
<port_list>: Port list or 'all', default: All ports
OUI : Detect telephony device by OUI address.
LLDP : Detect telephony device by LLDP.
Both : Both OUI and LLDP.
(default: Show Voice VLAN discovery protocol)
Default Setting:
OUI

Ethernet Ring Protection Switching Command

ERPS Command

Description:
Invoking an administrative command for a given protection group
[fs|ms|clear] : setting or clearing an administrative command for a given group
<port> : forced a block on the ring port where this command is issued
<group_id> : protection group id
Syntax:
Erps command [fs|ms|clear] <port> <group-id>
Parameters:
fs|ms|clear: administrative commands
<port> : Port number
<group-id> : protection group id 1 - 64

ERPS Version

Description:
Specifying protocol version for a given protection group
[v1|v2] : specifying protocol version for a given protection group
<group_id> : protection group id
Syntax:
Erps version [v1|v2] <group-id>
Parameters:
v1|v2 : ERPS protocol version to be supported
<group-id>: protection group id 1 - 64

ERPS Add

Description:
create a new ethernet ring protection group
<group-id> : protection group id
<east_port> : protection group Port 0
<west_port> : protection group Port 1, Port 1 can be 0 for sub-rings
[major|sub] : ring type i.e major-ring or sub-ring
[interconnected] : interconnection node or not
[[virtual_channel] : Virtual channel present or not

[<major-ring-id>] : major ring group Id for interconnected sub-ring

Syntax:

Erps add <group-id> <east_port> <west_port> [major|sub] [interconnected] [virtual_channel] [<major-ring-id>]

Parameters:

<group-id> : protection group id 1 - 64
<east_port> : Port 0 of a protection group
<west_port> : Port 1 of a protection group
major|sub : ring type
interconnected : Set for interconnected node
virtual_channel: Set for virtual channel
<major-ring-id>: major ring of a sub-ring, when configuring as an interconnected node

ERPS Reversion

Description:

Configuring reversion characteristics for a given node
[revertive|nonrevertive] : enabling or disabling reversion for a given group
<group_id> : protection group id

Syntax:

Erps reversion [revertive|nonrevertive] <group-id>

Parameters:

revertive|nonrevertive: specifying reversion parameters
<group-id> : protection group id 1 - 64

ERPS VLAN Add

Description:

Associating a given vlan to a protection group
<vid> : vlan to be protected
<group-id> : protection group-id for which vid belongs to.

Syntax:

Erps vlan add <vid> <group-id>

Parameters:

<vid> : VLAN ID (1-4095)
<group-id>: protection group id 1 - 64

ERPS VLAN Delete

Description:

Disassociating a given vlan to a protection group
<vid> : protected vlan to be deleted
<group-id> : protection group-id for which vid belongs to.

Syntax:

Erps vlan delete <vid> <group-id>

Parameters:

<vid> : VLAN ID (1-4095)
<group-id>: protection group id 1 - 64

ERPS MEP

Description:

Associating Port 0/1 MEP to a protection group
<east_sf_mep> : Mep_ID for finding out Continuity Check errors on Port 0
<west_sf_mep> : Mep_ID for finding out Continuity Check errors on Port 1
<east_raps_mep> : Mep_ID for transmitting R-APS frames on Port 0
<west_raps_mep> : Mep_ID for transmitting R-APS frames on Port 1
<group_id> : protection group id for which mep is associating.

Syntax:

Erps mep <east_sf_mep> <west_sf_mep> <east_raps_mep> <west_raps_mep> <group-id>

Parameters:

<east_sf_mep> : SF mep id for Port 0
<west_sf_mep> : SF mep id for Port 1
<east_raps_mep>: CC/RAPS mep id for Port 0
<west_raps_mep>: CC/RAPS mep id for Port 1
<group-id> : protection group id 1 - 64

ERPS RPL Neighbour

Description:

Selection of RPL neighbour for a protection group
(east|west) : selected east(Port 0) or west(Port 1) as RPL neighbour
<group-id> : protection group id for selecting RPL Block.

Syntax:

Erps rpl neighbour <rpl_port> <group-id>

Parameters:

<rpl_port>: RPL Block
<group-id>: protection group id 1 - 64

ERPS RPL Owner

Description:

Selection of RPL Block for a protection group
by default this node is considered as RPL Owner
(east|west) : select east(Port 0) or west(Port 1) as RPL Block
<group-id> : protection group id for selecting RPL Block.

Syntax:

Erps rpl owner <rpl_port> <group-id>

Parameters:

<rpl_port>: RPL Block
<group-id>: protection group id 1 - 64

ERPS RPL Neighbour Clear

Description:

make this node as non-neighbour for a protection group
<group-id> : protection group id for selecting RPL Block.

Syntax:

Erps rpl neighbour clear <group-id>

Parameters:

<group-id>: protection group id 1 - 64

ERPS RPL Owner Clear

Description:

making a node as Non-RPL Block for a protection group
After clear, this node is nore an rpl owner for the given group
(east|west) : selected east(Port 0) or west(Port 1) as RPL Block
<group-id> : protection group id for selecting RPL Block.

Syntax:

Erps rpl owner clear <group-id>

Parameters:

<group-id>: protection group id 1 - 64

ERPS Hold Off Timeout

Description:

configuring hold off timeout for a protection group
in milliseconds 0-10000 in the increments of 100ms
<hold_timeout> : hold-off timeout
<group-id> : protection group id for configuring hold-off time.

Syntax:

Erps hold off timeout <hold_timeout> <group-id>

Parameters:

<hold_timeout>: timer timeout values
<group-id> : protection group id 1 - 64

ERPS Guard-timeout

Description:

configuring guard timeout for a protection group
guard timeout should be configured in the increments of 10 milliseconds
minimum guard timeout 10 ms and maximum 2 seconds
<guard_timeout> : guard timeout
<group-id> : protection group id for configuring guard time.

Syntax:

Erps guard-timeout <guard_timeout> <group-id>

Parameters:

<guard_timeout>: timer timeout values
<group-id> : protection group id 1 - 64

ERPS WRT-timeout

Description:

configuring wait to restore timeout for a protection group
in minutes in the range of 1 to 12 minutes
<wtr_timeout> : configuring wtr timeout
<group-id> : protection group id for configuring wtr time.

Syntax:

Erps wtr-timeout <wtr_timeout> <group-id>

Parameters:

<wtr_timeout>: timer timeout values
<group-id> : protection group id 1 - 64

ERPS Delete

Description:
deletion of a protection group
<group-id> : protection group id for deletion .
Syntax:
Erps delete <group-id>
Parameters:
<group-id>: protection group id 1 - 64

ERPS Topologychange

Description:
specifying topology change propagation parameters for a given protection group
[propagate|nopropagate] : enabling or disabling topology change propagation for a given group
<group_id> : protection group id
Syntax:
Erps topologychange [propagate|nopropagate] <group-id>
Parameters:
propagate|nopropagate: topology change propagation configuration
<group-id> : protection group id 1 - 64

ERPS Configurationt

Description:
deletion of a protection group
<group-id> : protection group id
[statistics] : for displaying R-APS statistics
[clear] : for clearing R-APS statistics.
Syntax:
Erps configuration [<group-id>] [statistics|clear]
Parameters:
<group-id> : protection group id 1 - 64
statistics|clear: ERPS statistics

Loop Protect Command

Loop Protect Configuration

Description:
Show Loop Protection configuration.
Syntax:
Loop Protect Configuration

Loop Protect Mode

Description:

Set or show the Loop Protection mode.

Syntax:

Loop Protect Mode [enable|disable]

Parameters:

enable : Enable Loop Protection

disable: Disable Loop Protection

Default Setting:

enable

Loop Protect Transmit

Description:

Set or show the Loop Protection transmit interval.

Syntax:

Loop Protect Transmit [<transmit-time>]

Parameters:

Transmit time interval (1-10 seconds)

Default Setting:

5

Loop Protect Shutdown

Description:

Set or show the Loop Protection shutdown time.

Syntax:

Loop Protect Shutdown [<shutdown-time>]

Parameters:

Shutdown time interval (0-604800 seconds)

A value of zero disables re-enabling the port

Default Setting:

10

Loop Protect Port Configuration

Description:

Show Loop Protection port configuration.

Syntax:

Loop Protect Port Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Loop Protect Port Mode

Description:

Set or show the Loop Protection port mode.

Syntax:

Loop Protect Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable Loop Protection
disable: Disable Loop Protection

Loop Protect Port Action

Description:
Set or show the Loop Protection port action.
Syntax:
Loop Protect Port Action [<port_list>] [shutdown|shut_log|log]
Parameters:
<port_list>: Port list or 'all', default: All ports
shutdown : Shutdown the port
shut_log : Shutdown the port and Log event
log : (Only) Log the event

Loop Protect Port Transmit

Description:
Set or show the Loop Protection port transmit mode.
Syntax:
Loop Protect Port Transmit [<port_list>] [enable|disable]
Parameters:
<port_list>: Port list or 'all', default: All ports
enable : Enable Loop Protection
disable: Disable Loop Protection

Loop Protect Status

Description:
Show the Loop Protection status.
Syntax:
Loop Protect Status [<port_list>]
Parameters:
<port_list>: Port list or 'all', default: All ports

IPMC Command

IPMC Configuration

Description:
Show IPMC snooping configuration.
Syntax:
IPMC Configuration [mld|igmp]
Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP

IPMC Mode

Description:

Set or show the IPMC snooping mode.

Syntax:

IPMC Mode [mld|igmp] [enable|disable]

Parameters:

mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
enable : Enable IPMC snooping
disable: Disable IPMC snooping
(default: Show global IPMC snooping mode)

Default Setting:

disable

Example:

Enable IGMP snooping

```
NS3502-8P-2T-2S-V2:/>ipmc mode igmp enable
```

IPMC Flooding

Description:

Set or show the IPMC unregistered addresses flooding operation.

Syntax:

IPMC Flooding [mld|igmp] [enable|disable]

Parameters:

mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
enable : Enable IPMC flooding
disable: Disable IPMC flooding
(default: Show global IPMC flooding mode)

Default Setting:

enable

Example:

Enable IGMP flooding

```
NS3502-8P-2T-2S-V2:/>ipmc flooding igmp enable
```

IPMC Leave Proxy

Description:

Set or show the mode of IPMC Leave Proxy.

Syntax:

IPMC Leave Proxy [mld|igmp] [enable|disable]

Parameters:

mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
enable : Enable IPMC Leave Proxy
disable: Disable IPMC Leave Proxy

(default: Show global IPMC Leave Proxy mode)

Default Setting:

disable

Example:

Enable IGMP Leave Proxy

```
NS3502-8P-2T-2S-V2:/>ipmc leave proxy igmp enable
```

IPMC Proxy

Description:

Set or show the mode of IPMC Proxy.

Syntax:

IPMC Proxy [mld|igmp] [enable|disable]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

enable : Enable IPMC Proxy

disable: Disable IPMC Proxy

(default: Show global IPMC Proxy mode)

Default Setting:

disable

Example:

Enable IGMP Proxy

```
NS3502-8P-2T-2S-V2:/>ipmc proxy igmp enable
```

IPMC SSM

Description:

Set or show the IPMC SSM Range.

Syntax:

IPMC SSM [mld|igmp] [(Range <prefix> <mask_len>)]

Parameters:

mld|igmp :

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

range : SSM Range keyword

<prefix> : IPv4/IPv6 multicast group address, accordingly

<mask_len>: Mask length for IPv4(4 ~ 32)/IPv6(8 ~ 128) ssm range, accordingly

IPMC VLAN Add

Description:

Add the IPMC snooping VLAN interface.

Syntax:

IPMC VLAN Add [mld|igmp] <vid>

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095)

IPMC VLAN Delete

Description:
Delete the IPMC snooping VLAN interface.
Syntax:
IPMC VLAN Delete [mld|igmp] <vid>
Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095)

IPMC State

Description:
Set or show the IPMC snooping state for VLAN.
Syntax:
IPMC State [mld|igmp] [<vid>] [enable|disable]
Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
enable : Enable MLD snooping
disable: Disable MLD snooping
Default Setting:
disable
Example:
Enable IGMP snooping state for VLAN 1

```
NS3502-8P-2T-2S-V2:/>ipmc state igmp 1 enable
```

IPMC Querier

Description:
Set or show the IPMC snooping querier mode for VLAN.
Syntax:
IPMC Querier [mld|igmp] [<vid>] [enable|disable]
Parameters:
mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
enable : Enable MLD querier
disable: Disable MLD querier
Default Setting:
disable

Example:

Enable IGMP querier for VLAN 1

```
NS3502-8P-2T-2S-V2:/>ipmc querier igmp 1 enable
```

IPMC Compatibility

Description:

Set or show the IPMC Compatibility.

Syntax:

IPMC Compatibility [mld|igmp] [<vid>] [auto|v1|v2|v3]

Parameters:

mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
auto|v1|v2|v3:
auto : Auto Compatibility (Default Value)
v1 : Forced Compatibility of IGMPv1 or MLDv1
v2 : Forced Compatibility of IGMPv2 or MLDv2
v3 : Forced Compatibility of IGMPv3
(default: Show IPMC Interface Compatibility

IPMC Fastleave

Description:

Set or show the IPMC snooping fast leave port mode.

Syntax:

IPMC Fastleave [mld|igmp] [<port_list>] [enable|disable]

Parameters:

mld|igmp:
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<port_list>: Port list or 'all', default: All ports
enable : Enable MLD fast leave
disable: Disable MLD fast leave
(default: Show IPMC fast leave mode)

Default Setting:

disable

Example:

Enable IGMP fast leave for all port

```
NS3502-8P-2T-2S-V2:/>ipmc fastleave igmp 1-10 enable
```

IPMC Throttling

Description:

Set or show the IPMC port throttling status.

Syntax:

IPMC Throttling [mld|igmp] [<port_list>] [limit_group_number]

Parameters:

mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<port_list>: Port list or 'all', default: All ports
0 : No limit
1~10 : Group learn limit
(default: Show IPMC Port Throttling)

Default Setting:

Unlimited

Example:

Set the max. learn 10 groups for ICMP port throttling

```
NS3502-8P-2T-2S-V2:/>ipmc throttling igmp 1-10 10
```

IPMC Filtering

Description:

Set or show the IPMC port group filtering list.

Syntax:

IPMC Filtering [mld|igmp] [<port_list>] [add|del] [group_addr]

Parameters:

mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<port_list>: Port list or 'all', default: All ports
add : Add new port group filtering entry
del : Del existing port group filtering entry
(default: Show IPMC port group filtering list)
group_addr : IPv4/IPv6 multicast group address, accordingly

IPMC Router

Description:

Set or show the IPMC snooping router port mode.

Syntax:

IPMC Router [mld|igmp] [<port_list>] [enable|disable]

Parameters:

mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<port_list>: Port list or 'all', default: All ports
enable : Enable IPMC router port
disable : Disable IPMC router port
(default: Show IPMC router port mode)

Example:

Enable port 1 in IPMC router port

```
NS3502-8P-2T-2S-V2:/>ipmc riuter igmp 1 enable
```

IPMC Status

Description:

Show IPMC operational status, accordingly.

Syntax:

IPMC Status [mld|igmp] [<vid>]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

Example:

Show VLAN 1 IPMC operational status

```
NS3502-8P-2T-2S-V2:/>ipmc status igmp 1
```

IPMC Group

Description:

Show IPMC group addresses, accordingly.

Syntax:

IPMC Groups [mld|igmp] [<vid>]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

Example:

Show VLAN 1 IPMC group addresses, accordingly.

```
NS3502-8P-2T-2S-V2:/>ipmc groups igmp 1
```

IPMC Version

Description:

Show IPMC Versions.

Syntax:

IPMC Version [mld|igmp] [<vid>]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

Example:

Show VLAN 1 IPMC Versions.

```
NS3502-8P-2T-2S-V2:/>ipmc version igmp 1
```

IPMC SFM

Description:

Show SFM (including SSM) related information for IPMC.

Syntax:
IPMC SFM [mld|igmp] [<vid>] [<port_list>]
Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
<port_list>: Port list or 'all', default: All ports

IPMC Parameter RV

Description:
Set or show the IPMC Robustness Variable.
Syntax:
IPMC Parameter RV [mld|igmp] [<vid>] [ipmc_param_rv]
Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
ipmc_param_rv:
-1 : Default Value (2)
1~255 : Robustness Variable
(default: Show IPMC Interface Robustness Variable

IPMC Parameter QI

Description:
Set or show the IPMC Query Interval.
Syntax:
IPMC Parameter QI [mld|igmp] [<vid>] [ipmc_param_qi]
Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
ipmc_param_qi:
-1 : Default Value (125)
1~31744 : Query Interval in seconds
(default: Show IPMC Interface Query Interval

IPMC Parameter QRI

Description:
Set or show the IPMC Query Response Interval.
Syntax:
IPMC Parameter QRI [mld|igmp] [<vid>] [ipmc_param_qri]
Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
ipmc_param_qri:
-1 : Default Value (100)
0~31744 : Query Response Interval in tenths of seconds
(default: Show IPMC Interface Query Response Interval

IPMC Parameter LLQI

Description:
Set or show the IPMC Last Listener Query Interval.
Syntax:
IPMC Parameter LLQI [mld|igmp] [<vid>] [ipmc_param_llqi]
Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
ipmc_param_llqi:
-1 : Default Value (10)
0~31744 : Last Listener Query Interval in tenths of seconds
(default: Show IPMC Interface Last Listener Query Interval

IPMC Parameter URI

Description:
Set or show the IPMC Unsolicited Report Interval.
Syntax:
IPMC Parameter URI [mld|igmp] [<vid>] [ipmc_param_uri]
Parameters:
mld|igmp :
mld : IPMC for IPv6 MLD
igmp: IPMC for IPv4 IGMP
<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs
ipmc_param_uri:
-1 : Default Value (1)
0~31744 : Unsolicited Report Interval in seconds
(default: Show IPMC Interface Unsolicited Report Interval)

VLAN Control List Command

VCL MAC-based VLAN Configuration

Description:
Show VCL MAC-based VLAN configuration.
Syntax:
VCL Macvlan Configuration

VCL MAC-based VLAN Add

Description:

Add or modify VCL MAC-based VLAN entry.

Syntax:

VCL Macvlan Add <mac_addr> <vid> [<port_list>]

Parameters:

<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)
<vid> : VLAN ID (1-4095)
<port_list>: Port list or 'all', default: All ports

Example:

Add 00-11-22-33-44-55-66 in VLAN 20 for all port

```
NS3502-8P-2T-2S-V2:/>vcl macvlan add 00-11-22-33-44-55-66 20 1-10
```

VCL MAC-based VLAN Delete

Description:

Delete VCL MAC-based VLAN entry.

Syntax:

VCL Macvlan Del <mac_addr>

Parameters:

<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)

Example:

Delete 00-11-22-33-44-55-66 in MAC-based VLAN list

```
NS3502-8P-2T-2S-V2:/> vcl macvlan del 00-11-22-33-44-55-66
```

VCL Stasus

Description:

Show VCL MAC-based VLAN users configuration.

Syntax:

VCL Status [combined|static|nas|all]

Parameters:

combined|static|nas|all: VCL User

VCL Protocol-based VLAN Add Ethernet II

Description:

Add VCL protocol-based VLAN Ethernet-II protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Add Eth2 <ether_type>|arp|ip|ipx|at <group_id>

Parameters:

<ether_type>|arp|ip|ipx|at: Ether Type (0x0600 - 0xFFFF)
<group_id> : Protocol group ID

VCL Protocol-based VLAN Add SNAP

Description:

Add VCL protocol-based VLAN SNAP protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Add Snap <oui>|rfc_1042|snap_8021h <pid> <group_id>

Parameters:

<oui>|rfc_1042|snap_8021h: OUI value (Hexadecimal 00-00-00 to FF-FF-FF).

<pid> : PID value (0x0-0xFFFF). If OUI is 00-00-00, valid range of PID is from 0x0600-0xFFFF.

<group_id> : Protocol group ID

VCL Protocol-based VLAN Add LLC

Description:

Add VCL protocol-based VLAN LLC protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Add Llc <dsap> <ssap> <group_id>

Parameters:

<dsap> : DSAP value (0x00-0xFF)

<ssap> : SSAP value (0x00-0xFF)

<group_id>: Protocol group ID

VCL Protocol-based VLAN Delete Ethernet II

Description:

Delete VCL protocol-based VLAN Ethernet-II protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Delete Eth2 <ether_type>|arp|ip|ipx|at

Parameters:

<ether_type>|arp|ip|ipx|at: Ether Type (0x0600 - 0xFFFF)

VCL Protocol-based VLAN Delete SNAP

Description:

Delete VCL protocol-based VLAN SNAP protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Delete Snap <oui>|rfc_1042|snap_8021h <pid>

Parameters:

<oui>|rfc_1042|snap_8021h: OUI value (Hexadecimal 00-00-00 to FF-FF-FF).

<pid> : PID value (0x0-0xFFFF). If OUI is 00-00-00, valid range of PID is from 0x0600-0xFFFF.

VCL Protocol-based VLAN Delete LLC

Description:

Delete VCL protocol-based VLAN LLC protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Delete Llc <dsap> <ssap>

Parameters:

<dsap>: DSAP value (0x00-0xFF)

<ssap>: SSAP value (0x00-0xFF)

VCL Protocol-based VLAN Add

Description:

Add VCL protocol-based VLAN group to VLAN mapping.

Syntax:

VCL ProtoVlan Vlan Add [<port_list>] <group_id> <vid>

Parameters:

<port_list>: Port list or 'all', default: All ports
<group_id> : Protocol group ID
<vid> : VLAN ID (1-4095)

VCL Protocol-based VLAN Delete

Description:

Delete VCL protocol-based VLAN group to VLAN mapping.

Syntax:

VCL ProtoVlan Vlan Delete [<port_list>] <group_id>

Parameters:

<port_list>: Port list or 'all', default: All ports
<group_id> : Protocol group ID

VCL Protocol-based VLAN Configuration

Description:

Show VCL protocol-based VLAN entries.

Syntax:

VCL ProtoVlan Conf

VCL IP Subnet-based Vlan Configuration

Description:

Show VCL IP Subnet-based VLAN configuration.

Syntax:

VCL IPVlan Configuration [<vce_id>]

Parameters:

<vce_id>: Unique VCE ID (1-128) for each VCL entry

VCL IP Subnet-based Vlan Add

Description:

Add or modify VCL IP Subnet-based VLAN entry. The maximum IPVlan entries are limited to 128.

Syntax:

VCL IPVlan Add [<vce_id>] <ip_addr_mask> <vid> [<port_list>]

Parameters:

<vce_id> : Unique VCE ID (1-128) for each VCL entry
<ip_addr_mask>: Source IP address and mask (Format: a.b.c.d/n).
<vid> : VLAN ID (1-4095)
<port_list> : Port list or 'all', default: All ports

VCL IP Subnet-based Vlan Delete

Description:

Delete VCL IP Subnet-based VLAN entry.

Syntax:

VCL IPVlan Delete <vce_id>

Parameters:

<vce_id>: Unique VCE ID (1-128) for each VCL entry

SMTP Command

SMTP Configuration

Description:

Show SMTP configure.

Syntax:

SMTP Configuration

Default Setting:

disable

SMTP Mode

Description:

Enable or disable SMTP configure.

Syntax:

SMTP Mode [enable|disable]

Parameters:

enable : Enable SMTP mode

disable : Disable SMTP mode

(default: Show SMTP mode)

Default Setting:

Disable

SMTP Server

Description:

Set or show SMTP server configure.

Syntax:

SMTP Server [<server>] [<port>]

Parameters:

<server>: SMTP server address

<port> : SMTP server port

Default Setting:

disable

SMTP Auth

Description:

Enable or disable SMTP authentication configure.

Syntax:
SMTP Auth [enable|disable]
Parameters:
enable : Enable SMTP Authentication
disable : Disable SMTP Authentication
(default: Show SMTP Authentication)
Default Setting:
disable

SMTP Auth_user

Description:
Set or show SMTP authentication user name configure.
Syntax:
SMTP Auth_user [<auth_user_text>]
Parameters:
<auth_user_text>: SMTP Authentication User Name
Default Setting:
disable

SMTP Auth_pass

Description:
Set or to show SMTP authentication password configure.
Syntax:
SMTP Auth_pass [<auth_pass_text>]
Parameters:
<auth_pass_text>: SMTP Authentication Password
Default Setting:
disable

SMTP Mail from

Description:
Set or show SMTP e-mail from configure.
Syntax:
SMTP Mailfrom [<mailfrom_text>]
Parameters:
<mailfrom_text>: SMTP E-mail From address
Default Setting:
Disable

SMTP Mail Subject

Description:
Set or to show SMTP e-mail subject configure.
Syntax:
SMTP Mailsubject [<mailsubject_text>]
Parameters:
<mailsubject_text>: SMTP E-mail Subject

Default Setting:
Disable

SMTP Mail to 1

Description:
Set or show SMTP e-mail 1 to configure.
Syntax:
SMTP Mailto1 [<mailto1_text>]
Parameters:
<mailto1_text>: SMTP e-mail 1 to address
Default Setting:
Disable

SMTP Mail to 2

Description:
Set or show SMTP e-mail 2 to configure.
Syntax:
SMTP Mailto2 [<mailto2_text>]
Parameters:
<mailto1_text>: SMTP e-mail 2 to address
Default Setting:
Disable

SMTP Test

Description:
Test the status for linking to SMTP server
Syntax:
SMTP Test

Show Command

Show Access

Description:
Show access management configuration.
Syntax:
Show access

Show ACL

Description:
Show ACL Configuration.
Syntax:
Show acl

Show Aggregation

Description:

Show link aggregation configuration.

Syntax:

Show aggr

Show ARP

Description:

Show ARP inspection configuration.

Syntax:

Show arp

Show Auth

Description:

Show Auth configuration.

Syntax:

Show auth

Show DHCP Relay

Description:

Show DHCP relay configuration.

Syntax:

Show DHCP relay

Show EEE

Description:

Show EEE configuration.

Syntax:

Show EEE

Show HTTPs

Description:

Show HTTPS configuration.

Syntax:

Show https

Show IGMP

Description:

Show IPMC snooping configuration.

Syntax:

Show igmp

Show IP

Description:

Show IP configuration.

Syntax:

Show ip

Show LACP

Description:

Show LACP configuration.

Syntax:

Show lacp

Show Limit Control

Description:

Show Limit Control configuration.

Syntax:

Show limit control

Show LLDP

Description:

Show LLDP configuration.

Syntax:

Show lldp

Show LLDP-MED

Description:

Show LLDP-MED configuration.

Syntax:

Show LLDPMED

Show Loop Protect

Description:

Show Loop Protection configuration.

Syntax:

Show Loop Protect

Show MAC

Description:

Show MAC address table configuration.

Syntax:

Show MAC

Show Mirror

Description:

Show mirror configuration.

Syntax:

Show mirror

Show MVR

Description:

Show MVR configuration.

Syntax:

Show MVR

Show PoE

Description:

Show PoE configuration.

Syntax:

Show PoE

Show Port

Description:

Show port configuration.

Syntax:

Show port

Show Privilege

Description:

Show privilege configuration.

Syntax:

Show privilege

Show Private VLAN

Description:

Show Private VLAN configuration.

Syntax:

Show pvlan

Show QoS

Description:

Show QoS Configuration.

Syntax:

Show QoS

Show SNMP

Description:

Show SNMP configuration.

Syntax:

Show SNMP

Show SSH

Description:

Show SSH configuration.

Syntax:

Show ssh

Show System

Description:

Show system configuration.

Syntax:

Show system

Show Timezone

Description:

Show System Timezone configuration.

Syntax:

Show timezone

Show UPnP

Description:

Show UPnP configuration.

Syntax:

Show upnp

Show Users

Description:

Show users configuration.

Syntax:

Show users

Show VLAN

Description:

Show VLAN configuration.

Syntax:

Show vlan

Show Voice VLAN

Description:

Show Voice VLAN configuration.

Syntax:

Show voice vlan

Show Firmware

Description:

Display information about active and alternate firmware images.

Syntax:

Show firmware

Show STP

Description:

Show STP Port configuration.

Syntax:

Show STP

Chapter 7
Switch operation

Address table

The managed switch is implemented with an address table. This address table is composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port number, etc. This information comes from the learning process of the managed switch.

Learning

When one packet comes in from any port, the managed switch records the source address, port number, and the other related information in the address table. This information will be used to decide either forwarding or filtering for future packets.

Forwarding and filtering

When one packet comes from a port of the managed switch, it checks the destination address as well as the source address learning. The managed switch will look up the address table for the destination address. If not found, this packet will be forwarded to all the other ports except the port that this packet comes from. These ports will transmit this packet to the network it is connected to. If found, and the destination address is located at a different port from the one this packet comes from, the managed switch will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port that this packet comes in, then this packet will be filtered, thereby increasing the network throughput and availability.

Store-and-forward

Store-and-Forward is a packet-forwarding technique. A Store-and-Forward switch stores the incoming frame in an internal buffer and completes error checking before

transmission. Therefore, no erroneous packets will occur, making it the best choice when a network needs efficiency and stability.

The managed switch scans the destination address from the packet header and searches the routing table provided for the incoming port and forwards the packet if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment existing hubs, which nearly always improves the overall performance. Ethernet switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using conventional cabling and adapters.

Owing to the learning function of the managed switch, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduces the overall load on the network.

The managed switch performs Store-and-Forward, preventing errorneous packets and reducing the re-transmission rate. No packet loss will occur.

Auto-negotiation

The STP ports on the managed switch have built-in auto-negotiation. This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detecting the modes and speeds of both devices that are connected. Both the 10BASE-T and 100BASE-TX devices can connect with the port in either half- or full-duplex mode. 1000BASE-T can be only connected in full-duplex mode.

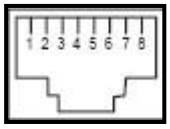
Chapter 8
Troubleshooting

This chapter contains information to help you solve issues. If the managed switch is not functioning properly, ensure that it was set up according to the instructions in this manual.

Issue	Solution
The per port LED does not illuminate	Check the cable connection of the managed switch.
Poor performance	Check the full duplex status of the managed switch. If the managed switch is set to auto negotiation mode and the partner is set to half duplex, then the performance will be poor.
The managed switch doesn't connect to the network	1. Check the per port LED on the managed switch. 2. Try another port on the managed switch. 3. Make sure the cable is installed properly. 4. Make sure the cable is the right type. 5. Turn off the power. After a while, turn on power again.
The per port LED illuminates, but the traffic is irregular	Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.
The managed switch does not power up.	1. Check to ensure that the AC power cord is not faulty and that it is inserted properly. 2. If the cord is inserted correctly, replace the power cord. 3. Check that the AC power source is working by connecting a different device in place of the switch. 4. If that device does not work, check the AC power

Appendix A
Networking connection

PoE RJ45 port pin assignments



Pin Number	RJ45 Power Assignment
1	Power +
2	Power +
3	Power -
6	Power -

RJ45 port pin assignments – 1000Mbps, 1000BASE-T

Pin number	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

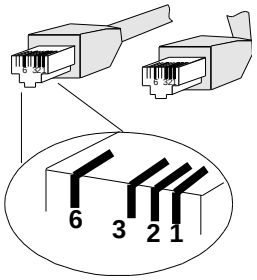
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

10/100Mbps, 10/100BASE-TX

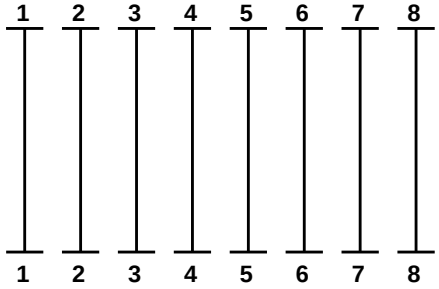
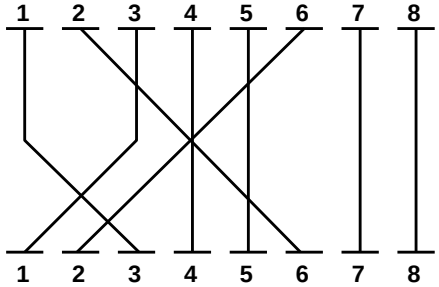
When connecting the managed switch to another Fast Ethernet switch, a bridge, or a hub, a straight or crossover cable is necessary. Each port of the managed switch supports auto-MDI (Media Dependent Interface)/MDI-X (Media Dependent Interface Cross) detection. This makes it possible to directly connect the managed switch to any Ethernet device without making a crossover cable. The following table and diagram show the standard RJ45 receptacle/ connector and their pin assignments.

Pin number	MDI	MDI-X
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx + (receive)	Tx + (transmit)
7, 8	Not used	

The standard RJ45 receptacle/connector:



There are eight wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and the color of the straight cable and crossover cable connection:

Straight Cable		SIDE 1	SIDE 2
	SIDE 1 SIDE 2	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown
Crossover Cable		**SIDE 1**	**SIDE 2**
	SIDE 1 SIDE 2	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Green 2 = Green 3 = White / Orange 4 = Blue 5 = White / Blue 6 = Orange 7 = White / Brown 8 = Brown

Ensure that connected cables are with the same pin assignment and color as the above diagram before deploying the cables into the network.

Glossary

A

ACE	Access Control Entry. It describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). ACE also contains many detailed, different parameter options that are available for individual application.
ACL	Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine if there are specific traffic object access rights. 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 three web pages associated with the manual ACL configuration: **Access Control List (ACL)**: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). The table is empty by default. 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, one 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 obtain further information for each of them. The maximum number of ACEs is 64. **ACL Port Configuration**: 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 only apply if the frame gets past the ACE matching without getting matched, however. 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**: This page can be used to configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per second. The "Ports" and "Access Control List" web pages can be used to assign a Rate Limiter ID to the ACE(s) or ingress port(s).
AES	Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.
AMS	Auto Media Select. AMS is used for dual media ports (ports supporting both copper (CU) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and CU cables are inserted, the port will select the prefered media.
APS	Automatic Protection Switching. This protocol is used to secure that switching is done bidirectionally in the two ends of a protection group, as defined in G.8031
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	Address Resolution Protocol. It is a protocol 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

CC	Continuity Check. This is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.
CCM	Continuity Check Message. This is an OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.
CDP	Cisco Discovery Protocol

D

DEI	Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.
DES	Data Encryption Standard. 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	Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network. DHCP is 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 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 DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from 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 is 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 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 to the DHCP relay agent’s MAC address.
DHCP Snooping	DHCP snooping is used to block an intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet into a legitimate conversation between the DHCP client and server.
DNS	Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.
DoS	Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting network sites or a network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.
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.
DSCP	Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

E

EEE	Energy Efficient Ethernet as defined in IEEE 802.3az.
EPS	Ethernet Protection Switching as 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

FTP	File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.
Fast Leave	IGMP 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.

H

HTTP	Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW). HTTP defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands. For example, entering a URL in a browser 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	Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection. HTTPS provides 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 the use of 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	Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic, or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.
IEEE 802.1X	IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.
IGMP	Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.
IGMP Querier	A router sends IGMP query messages onto a particular link. This router is called the Querier.
IMAP	Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server. IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server. The current version of the IMAP 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 email messages on the server rather than downloading them to a computer. To remove your messages from the server, use the mail client to generate local folders, copy messages to the local hard drive, and then delete and expunge the messages from the server.

IP	Internet Protocol. It is a protocol used for communicating data across a internet network. IP is a "best effort" system, which means that no packet of information sent over it 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 IP address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network. The most widely used version of the Internet protocol is IPv4, which has 32-bit IP addresses allowing for over four billion unique addresses. There is a substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bit IP 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	IP MultiCast
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 Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.
LLDP	Link Layer Discovery Protocol is an IEEE 802.1ab standard protocol. The 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 station’s 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 extendsion of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).
LOC	LOC is an acronym for Loss Of Connectivity and is detected by a MEP and indicates 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), that shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.
MEP	MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).
MD5	Message-Digest algorithm 5. MD5 is a message digest algorithm using a cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 – The MD5 Message-Digest Algorithm.
Mirroring	For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. In this context, mirroring a frame is the same as copying the frame. Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port
MLD	Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.
MVR	Multicast VLAN Registration. It 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.

N

NAS	Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS	Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN). The NetBIOS provides each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, as well as the session and transport services described in the Open Systems Interconnection (OSI) model.
NFS	Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems. NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.
NTP	Network Time Protocol. A network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as the transport layer.

O

OAM	Operation Administration and Maintenance. It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.
Optional TLVs	A LLDP frame contains multiple TLVs For some TLVs it is configurable if the switch includes 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	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 that forms the first 24 bits of a MAC address.

P

PCP	Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.
PD	Powered Device. In a PoE> system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.
PHY	Physical Interface Transceiver. It is the device that implements 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.
Policer	A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.
POP3	POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server. POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service. An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining email on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server. POP and IMAP deal with the receiving of email and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send email with SMTP, and a mail handler receives it on the recipient's behalf. Then, the mail is read using POP or IMAP.
PPPoE	Point-to-Point Protocol over Ethernet. It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames (Wikipedia). It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.
Private VLAN	In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.
PTP	Precision Time Protocol. A network protocol for synchronizing the clocks of computer systems.

Q

QCE	QoS Control Entry. It describes the 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 four different QoS classes: "Low", "Normal," "Medium," and "High" for individual application.

QCL	QoS Control List. It is the list table of QCEs, containing QoS control entries that classify 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 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	Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services, and QoS can help to provide this.
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	Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.
RADIUS	Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization, and accounting management for people or computers to connect to and use a network service.
RDI	Remote Defect Indication. It is a OAM functionallity that is used by a MEP to indicate defect detected to the remote peer MEP.
Router Port	A router port is a port on the Ethernet switch that connects it to the Layer 3 multicast device.
RSTP	In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SAMBA	Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking. Samba can be installed on a variety of operating system platforms, including Linux and most common Unix platforms. Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".
SHA	SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.
Shaper	A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.
SMTP	Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.
SNAP	SubNetwork Access Protocol (SNAP). It 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 identifiers.
SNMP	Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allows 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	Simple Network Time Protocol. A network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as a transport layer.
SPROUT	Stack Protocol using Routing Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform the shortest path forwarding within the stack.

SSID	Service Set Identifier. It is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one.
SSH	Secure Shell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality.
SSM	SSM In SyncE is an abbreviation for Synchronization Status Message and contains a QL indication.
STP	Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsoleted by RSTP.
SyncE	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+	Terminal Acess Controller Access Control System Plus. It is a networking protocol that 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	Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange 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 email 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), email, and File Transfer Protocol (FTP).

TELNET	TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client. TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.
TFTP	Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provides directory service and security features.
ToS	Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant six 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	Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as a TLV.
TKIP	Temporal Key Integrity Protocol. It is used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

U

UDP	User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers. UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP. UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact. Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP	Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components
User Priority	User Priority is a 3-bit field that stores the priority level for the 802.1Q frame.

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, QoS-related configuration for voice data can be performed, ensuring the transmission priority of voice traffic and voice quality.

W

WEP	Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks. When introduced, WEP was intended to provide data confidentiality comparable to that of a traditional wired network (Wikipedia).
Wi-Fi	Wireless Fidelity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA	Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system , Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).
WPA-PSK	Wi-Fi Protected Access - Pre Shared Key. WPA was designed to enhance the security of wireless networks. There are two types of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes a less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard.
WPA-Radius	Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard.
WPS	Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network.
WRED	Weighted Random Early Detection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.
WTR	Wait To Restore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource.