



NS4750-24S-4T-4X User Manual



Copyright	© 2014 United Technologies Corporation Interlogix is part of UTC Building & Industrial Systems, Inc. a unit of United Technologies Corporation. All rights reserved.
Trademarks and patents	The NS4750-24S-4T-4X name and logo are trademarks of United Technologies. Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.
Manufacturer	Interlogix 3211 Progress Drive, Lincolnton, NC 28092 USA Authorized EU manufacturing representative: UTC Climate Controls & Security B.V., Kelvinstraat 7, 6003 DH Weert, Netherlands
Intended use	Use this product only for the purpose it was designed for; refer to the data sheet and user documentation for details. For the latest product information, contact your local supplier or visit us online at www.interlogix.com .
Certification	  N4131
FCC compliance	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. You are cautioned that any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
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.
Canada	This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.
European Union directives	2004/108/EC (EMC Directive): Hereby, UTC Building & Industrial Systems, Inc. declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2004/108/EC.
Contact Information	For contact information, see www.interlogix.com or www.utcssecurityproducts.eu .

TABLE OF CONTENTS

- 1. INTRODUCTION..... 10
 - 1.1 Packet Contents 10
 - 1.2 Product Descriptions 11
 - 1.3 How to Use This Manual..... 14
 - 1.4 Product Features..... 15
 - 1.5 Product Specifications 18
- 2. INSTALLATION 21
 - 2.1 Hardware Descriptions 21
 - 2.1.1 Front Panel..... 21
 - 2.1.2 LED Indications 23
 - 2.1.3 Wiring the AC Power Input 25
 - 2.1.4 Wiring the DC Power Input 25
 - 2.1.5 Wiring the Faulty Alarm Contact 26
 - 2.1.6 Wiring the Digital Input / Output..... 27
 - 2.2 Installing the Managed Switch 30
 - 2.2.1 Desktop Installation 30
 - 2.2.2 Rack Mounting 31
 - 2.3 Cabling 33
 - 2.3.1 Installing the SFP Transceiver 34
 - 2.3.2 Removing the Module..... 37
- 3. SWITCH MANAGEMENT 38
 - 3.1 Requirements 38
 - 3.2 Management Access Overview..... 39
 - 3.3 CLI Mode Management 40
 - 3.4 Web Management..... 41
 - 3.5 SNMP-based Network Management 42
- 4. WEB CONFIGURATION 43
 - 4.1 Main Web Page..... 46

4.2 System.....	48
4.2.1 System Information.....	48
4.2.2 IP Configuration.....	49
4.2.3 IP Status	52
4.2.4 Users Configuration.....	53
4.2.5 Privilege Levels	55
4.2.6 NTP Configuration	58
4.2.7 Time Configuration	59
4.2.8 UPnP	60
4.2.9 DHCP Relay	62
4.2.10 DHCP Relay Statistics	64
4.2.11 CPU Load	65
4.2.12 System Log	67
4.2.13 Detailed Log	68
4.2.14 Remote Syslog	69
4.2.15 SMTP Configuration	71
4.2.16 Digital Input/Output.....	72
4.2.17 Faulty Alarm	75
4.2.18 Web Firmware Upgrade	76
4.2.19 TFTP Firmware Upgrade	77
4.2.20 Save Startup Config.....	78
4.2.21 Configuration Download	79
4.2.22 80	
4.2.23 Configuration Activate.....	81
4.2.24 Configuration Delete.....	82
4.2.25Image Select	82
4.2.26 Factory Default	84
4.2.27 System Reboot.....	85
4.3 Simple Network Management Protocol	86
4.3.1 SNMP Overview	86
4.3.2 SNMP System Configuration.....	87
4.3.3 TRAP Configuration.....	88
4.3.4 SNMP System Information	92
4.3.5 SNMPv3 Configuration.....	93
4.3.5.1 SNMPv3 Communities	93
4.3.5.2 SNMPv3 Users.....	94
4.3.5.3 SNMPv3 Groups	95
4.3.5.4 SNMPv3 Views.....	96

4.3.5.5 SNMPv3 Access.....	98
4.4 Port Management	100
4.4.1 Port Configuration.....	100
4.4.2 Port Statistics Overview.....	103
4.4.3 Detailed Port Statistics.....	104
4.4.4 SFP Information.....	106
4.4.5 Port Mirror	108
4.5 Link Aggregation	111
4.5.1 Static Aggregation.....	114
4.5.2 LACP Configuration.....	116
4.5.3 LACP System Status	118
4.5.4 LACP Port Status.....	119
4.5.5 LACP Port Statistics	121
4.6 VLAN.....	123
4.6.1 VLAN Overview	123
4.6.2 IEEE 802.1Q VLAN	124
4.6.3 VLAN Port Configuration	127
4.6.4 VLAN Membership Status.....	133
4.6.5 VLAN Port Status.....	135
4.6.6 Private VLAN	138
4.6.7 Port Isolation	139
4.6.8 VLAN Setting Example:	140
4.6.8.1 Two separate 802.1Q VLANs	141
4.6.8.2 VLAN Trunking between two 802.1Q aware Switches	146
4.6.10.3 Port Isolate	148
4.6.11 MAC-based VLAN	150
4.6.12 MAC-based VLAN Status	151
4.6.13 Protocol-based VLAN	151
4.6.14 Protocol-based VLAN Membership	153
4.7 Spanning Tree Protocol	155
4.7.1 Theory	155
4.7.2 STP System Configuration	162
4.7.3 Bridge Status	165
4.7.4 CIST Port Configuration	166
4.7.5 MSTI Priorities	170
4.7.6 MSTI Configuration.....	171
4.7.7 MSTI Ports Configuration	173

4.7.8 Port Status	176
4.7.9 Port Statistics	178
4.8 Multicast	179
4.8.1 IGMP Snooping	179
4.8.2 Profile Table	184
4.8.3 Address Entry	185
4.8.4 IGMP Snooping Configuration	187
4.8.5 IGMP Snooping VLAN Configuration	189
4.8.6 IGMP Group Port Group Filtering	192
4.8.7 IGMP Snooping Status	194
4.8.8 IGMP Group Information	196
4.8.9 IGMPv3 Information	197
4.8.10 MLD Snooping Configuration	199
4.8.11 MLD Snooping VLAN Configuration	201
4.8.12 MLD Snooping Port Group Filtering	203
4.8.13 MLD Snooping Status	205
4.8.14 MLD Group Information	207
4.8.15 MLDv2 Information	208
4.8.16 MVR (Multicastset VLAN Registration)	209
4.8.17 MVR Status	213
4.8.18 MVR Groups Information	214
4.8.19 MVR SFM Information	215
4.9 Quality of Service	216
4.9.1 Understand QOS	216
4.9.2 Port Policing	217
4.9.3 Port Shaping	219
4.9.3.1 QoS Egress Port Schedule and Shapers	220
4.9.4 Port Classification	222
4.9.4.1 QoS Ingress Port Tag Classification	224
4.9.5 Port Scheduler	225
4.9.6 Port Tag Remarking	226
4.9.6.1 QoS Egress Port Tag Remarking	227
4.9.7 Port DSCP	229
4.9.8 DSCP-Based QoS	231
4.9.9 DSCP Translation	233
4.9.10 DSCP Classification	234
4.9.11 QoS Control List	235
4.9.11.1 QoS Control Entry Configuration	237

4.9.12 QoS Status	240
4.9.13 Storm Control Configuration	242
4.9.14 WRED	244
4.9.15 QoS Statistics	246
4.9.16 Voice VLAN Configuration	248
4.9.17 Voice VLAN OUI Table	251
4.10 Access Control Lists.....	253
4.10.1 Access Control List Status	253
4.10.2 Access Control List Configuration	256
4.10.3 ACE Configuration	258
4.10.4 ACL Ports Configuration	269
4.10.5 ACL Rate Limiter Configuration	272
4.11 Authentication	274
4.11.1 Understanding IEEE 802.1X Port-Based Authentication.....	275
4.11.2 Authentication Configuration	279
4.11.3 Network Access Server Configuration	280
4.11.4 Network Access Overview	291
4.11.5 Network Access Statistics	293
4.11.6 RADIUS	301
4.11.7 TACACS+	303
4.11.8 RADIUS Overview	305
4.11.9 RADIUS Details	306
4.12 Security	314
4.12.1 Port Limit Control.....	314
4.12.2 Access Management	318
4.12.3 Access Management Statistics	319
4.12.4 HTTPs	321
4.12.5 SSH	321
4.12.6 Port Security Status	322
4.12.7 Port Security Detail.....	325
4.12.8 DHCP Snooping	327
4.12.9 DHCP Snooping Statistics	329
4.12.10 IP Source Guard Configuration.....	332
4.12.11 IP Source Guard Static Table	333
4.12.12 ARP Inspection	334
4.12.13 ARP Inspection Static Table	336
4.13 MAC Address Table.....	338

4.13.1 MAC Address Table Configuration	338
4.13.2 MAC Address Table Status	341
4.13.3 Dynamic ARP Inspection Table	342
4.13.4 Dynamic IP Source Guard Table	343
4.14 LLDP	345
4.14.1 Link Layer Discovery Protocol	345
4.14.2 LLDP Configuration	345
4.14.3 LLDP-MED Configuration	349
4.14.4 LLDP-MED Neighbor	357
4.14.5 Neighbor	362
4.14.6 Port Statistics	363
4.15 Diagnostics	366
4.15.1 Ping	367
4.15.2 IPv6 Ping	368
4.15.3 Remote IP Ping Test	368
4.15.4 Cable Diagnostics	370
4.16 Loop Protection	371
4.16.1 Configuration	371
4.16.2 Status	373
4.17 RMON	375
4.17.1 RMON Alarm Configuration	375
4.17.2 RMON Alarm Status	378
4.17.3 RMON Event Configuration	379
4.17.4 RMON Event Status	380
4.17.5 RMON History Configuration	381
4.17.6 RMON History Status	382
4.17.7 RMON Statistics Configuration	383
4.17.8 RMON Statistics Status	384
4.18 PTP	386
4.18.1 PTP Configuration	386
4.18.2 PTP Status	387
4.19 Ring	389
4.19.1 MEP Configuration	390
4.19.2 Detailed MEP Configuration	392
4.19.3 Ethernet Ring Protocol Switch	395
4.19.4 Ethernet Ring Protocol Switch Configuration	397

4.19.5 Ring Wizard	401
4.19.6 Ring Wizard Example:	402
5. SWITCH OPERATION	405
5.1 Address Table	405
5.2 Learning	405
5.3 Forwarding & Filtering	405
5.4 Store-and-Forward	405
5.5 Auto-Negotiation	406
6. TROUBLESHOOTING	407
APPENDIX A	409
A.1 Switch's Data RJ-45 Pin Assignments - 1000Mbps, 1000Base-T	409
A.2 10/100Mbps, 10/100Base-TX	409
APPENDIX B: GLOSSARY	411

1. INTRODUCTION

IFS **NS4750-24S-4T-4X** is a 24-port 100/1000Base-X SFP + 4-port 10G SFP+ L2/L4 Managed Switch. The **NS4750-24S-4T-4X** is all multiple Gigabit SFP mini-GBIC slots switch plus four Gigabit Copper combo ports with connective ability and robust layer 2 features. The description of the NS4750-24S-4T-4X is shown below:

NS4750-24S-4T-4X 24-port 100/1000Base-X SFP + 4-port 10G SFP+ L2/L4 Managed Metro Ethernet Switch
(-10~60 degrees C)

“**Managed Switch**” mentioned in this User’s Manual refers to the NS4750-24S-4T-4X.

1.1 Packet Contents

Open the box of the Managed Switch and carefully unpack it. The box should contain the following items:

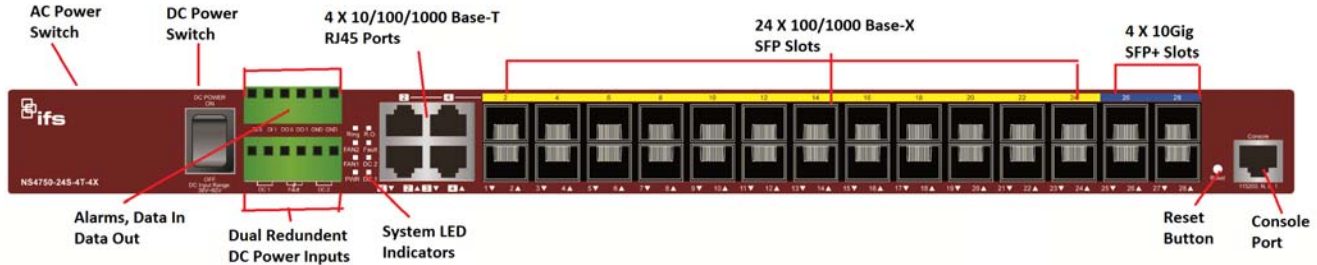
<input checked="" type="checkbox"/> The NS4750-24S-4T-4X	x 1
<input checked="" type="checkbox"/> Quick Installation Guide	x 1
<input checked="" type="checkbox"/> User’s Manual CD	x 1
<input checked="" type="checkbox"/> DB9 to RJ-45 Consol Cable	x 1
<input checked="" type="checkbox"/> Rubber Feet	x 4
<input checked="" type="checkbox"/> Rack Mount Accessory Kit	x 1
<input checked="" type="checkbox"/> AC Power Cord	x 1
<input checked="" type="checkbox"/> Dust Cap	x 33

If any of these are missing or damaged, please contact your dealer immediately. If possible, retain the carton including the original packing material, and use them again to repack the product in case there is a need to return it to us for repair.

1.2 Product Descriptions

Multiple SFP Fiber Port Switch for Increasing Long-reach Networking of Enterprise, Telecoms and Campus

The NS4750 is equipped with advanced management functions and provides **24 100/1000Mbps dual speed SFP fiber ports**, **4 10Gbps dual speed fiber ports** and **4 10/100/1000Mbps TP/SFP ports** delivered in a rugged strong case. It is capable of providing non-blocking switch fabric and wire-speed throughput as high as **128Gbps** in the temperature range from **-10 to 60 degrees C** without any packet loss and CRC error, which greatly simplify the tasks of upgrading the enterprise LAN for catering to increasing bandwidth demands. The NS4750 is specially designed for service provider to deliver profitable Ethernet network. The NS4750 adopts “**Front Access**” design, making the wiring and maintenance of the NS4750 placed in a cabinet very easy for technicians.



Support for 10Gb Ethernet

10Gb Ethernet which adopts full-duplex technology instead of low-speed, half-duplex CSMA/CD protocol, is a big leap in the evolution of Ethernet. 10Gb Ethernet can be deployed in star or ring topologies. With 10Gb Ethernet, the NS4750 switch provides broad bandwidth and powerful processing capacity. It is suitable for metropolitan networks and wide area networks. Using the NS4750 switch, users can simplify network structures and reduce cost of network construction.

Optimized Design for MAN Redundant Ring, Fast Recovery for Surveillance or Industrial System

The NS4750 supports redundant ring technology and features strong rapid self-recovery capability to prevent interruptions and external intrusions. It incorporates ITU G.8032 Ethernet Ring Protection Switching technology, Spanning Tree Protocol (802.1w RSTP), and redundant power supply system into customer's industrial automation network to enhance system reliability and uptime in harsh factory environments. The NS4750 also protects customer's industrial network connectivity with switching recovery capability that is used for implementing fault tolerant ring and mesh network architectures. If the Industrial network is interrupted accidentally, the fault recovery times could be less than 50ms to quickly bring the network back to normal operation.

Cost-effective IPv6 Managed Gigabit Switch Solution for Metro

Nowadays, lots of electronic products or mobile devices can browse the Internet, which means the need of IP address increases. However, the current IPv4 network infrastructure is not capable enough to provide IP address to each single user/client. The situation forces the ISP to come out with the IPv6 (Internet Protocol version 6) network infrastructure. To fulfill the demand, IFS releases the IPv6 management Gigabit Ethernet Switch. It supports both IPv4 and IPv6 management functions. It can work with the original network structure (IPv4) and also support the new network structure (IPv6). With easy and friendly management interfaces and plenty of management functions included, the NS4750 Managed Switch is the best choice for you to build the IPv6 FTTx edge service and for Industries to connect with IPv6 network.

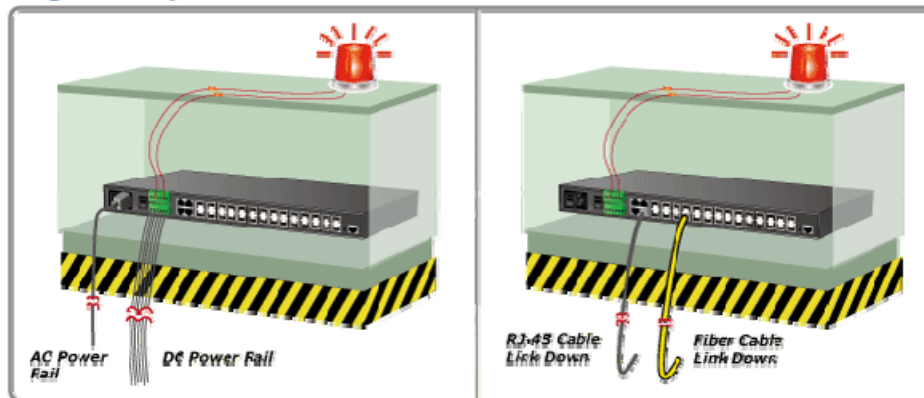
Digital Input and Digital Output for External Alarm

IFS NS4750 supports Digital Input, and Digital Output on the front panel. This external alarm offers technicians the ability to use Digital Input to detect, and log external device status (such as door intrusion detector) for the alarm. As Digital Output could be used to alarm if the NS4750 has port link down, link up or power failure.

Digital Input

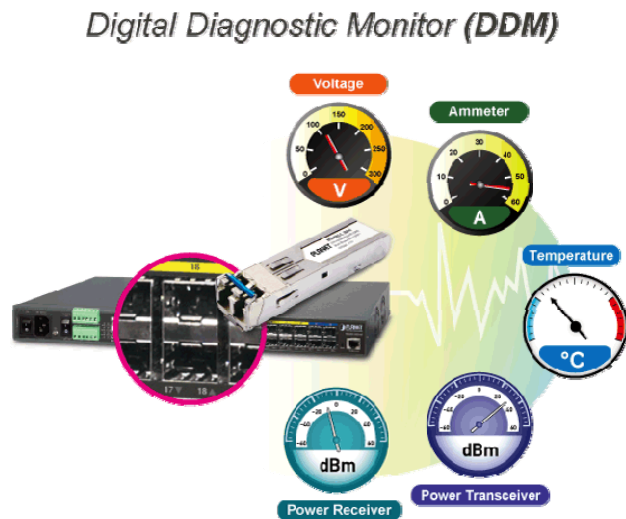


Digital Output



Flexible and Extendable Solution

The **24** mini-GBIC slots built in the NS4750 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 NS4750 supports **SFP-DDM (Digital Diagnostic Monitor)** function that can easily monitor real-time parameters of the SFP for network administrator, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.



AC and DC Redundant Power to Ensure Continuous Operation

IFS NS4750 is equipped with one **100~240V AC** power supply unit and one additional **36 ~ 60V DC** power supply unit for redundant power supply installation. A redundant power system is also provided to enhance the reliability with either the 100~240V AC power supply unit or the DC 36 ~ 60V power supply unit. Redundant Power Systems are specifically designed to handle the demands of high-tech facilities requiring the highest power integrity. Furthermore, with the 36~ 60V DC power supply implemented, the NS4750 can be applied as the telecom level device that could be located in the electronic room.

Layer 2 / Layer 4 Fully-functioned Managed Switch for Building Automation Networking

The NS4750 is ideal for applications in the factory data centers and distributions. It provides advanced Layer2 to Layer4 data switching and redundancy, Quality of Service traffic control, network access control and authentication, and Secure Management features to protect customer's industrial network connectivity with reliable switching recovery capability that is suitable for implementing fault tolerant and mesh network architectures.

Powerful Security

The Managed Switch offers comprehensive Access Control List (ACL) for enforcing security to the edge. Its protection mechanisms also comprise port-based 802.1x and MAC-based user and device authentication. The port-security is effective in limiting the number of clients that pass through, so that network administrators can now construct highly secured corporate networks with time and effort considerably less than before.

1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2, INSTALLATION

The section explains the functions of the **Managed Switch** and how to physically install the **Managed Switch**.

Section 3, SWITCH MANAGEMENT

The section contains the information about the software function of the **Managed Switch**.

Section 4, WEB CONFIGURATION

The section explains how to manage the **Managed Switch** by Web interface.

Section 5, COMMAND LINE INTERFACE

The section describes how to use the Command Line interface (CLI).

Section 6, CLI MODE

The section explains how to manage the **Managed Switch** by Command Line interface.

Section 7, SWITCH OPERATION

The chapter explains how to do the switch operation of the **Managed Switch**.

Section 8, TROUBLESHOOTING

The chapter explains how to do troubleshooting of the **Managed Switch**.

Appendix A

The section contains cable information of the **Managed Switch**.

Appendix B

The section contains glossary information of the **Managed Switch**.

1.4 Product Features

➤ **Physical Port**

- 24 100/1000Base-X SFP mini-GBIC slots
- 4 1/10GBase-SR/LR SFP mini-GBIC slots
- 4 10/100/1000Base-T Gigabit Ethernet RJ-45 combo ports
- One RJ-45 Console Interface for Basic Management and Setup

➤ **Redundant Power System**

- Redundant Power System: 100V ~ 240V AC / Dual 36V ~ 60V DC
- Active Redundant Power Failure Protection
- Backup of Catastrophic Power Failure on One Supply
- Fault Tolerance and Resilience.

➤ **Digital Input / Digital Output**

- 2 Digital Input (DI)
- 2 Digital Output (DO)
- Integrates sensors into Auto Alarm System
- Transfer Alarm to IP Network via SNMP Trap

➤ **Hardware Design**

- -10 to 60 degrees C Operating Temperature for DC Power Input only
- 19-inch Rack-mountable
- Relay Alarm for Port Breakdown, Power Failure
- 2 Thermal Fans Design

➤ **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 eliminate erroneous packets to optimize the network bandwidth
- Storm Control Support
 - Broadcast / Multicast / Unicast
- Supports **VLAN**
 - IEEE 802.1Q Tagged VLAN
 - Up to 255 VLAN 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 **Spanning Tree Protocol**

- 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**

- 802.3ad Link Aggregation Control Protocol (LACP)
- Cisco Ether-channel (Static Trunk)
- Maximum 5 trunk Groups, up to 8 ports per Trunk Group
- Up to 16Gbps Bandwidth (Duplex Mode)

- Provides Port Mirror (1-to-1)

- Port Mirroring to Monitor the Incoming or Outgoing Traffic on a Particular Port

- Loop Protection to Avoid Broadcast Loops

- Supports G.8032 Ethernet Ring Protection Switching (E.R.P.S.)

➤ **Quality of Service**

- Ingress Shaper and Egress Rate Limit Per Port Bandwidth Control
- 8 Priority Queues on All Switch Ports
- Traffic Classification
 - IEEE 802.1p CoS
 - IP TOS / DSCP / IP Precedence
 - 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
- MVR (Multicast VLAN Registration)

➤ **Security**

- IEEE 802.1x Port-based / MAC-based Network Access Authentication
- Built-in RADIUS Client to co-operate with the RADIUS Servers
- RADIUS / TACACS+ Users Access Authentication
- IP-based Access Control List (ACL)
- MAC-based Access Control List
- Source MAC / IP Address Binding
- DHCP Snooping to Filter Untrusted DHCP Messages
- Dynamic ARP Inspection discards ARP Packets with Invalid MAC Address to IP Address Binding
- IP Source Guard prevents IP spoofing attacks
- IP Address Access Management to Prevent Unauthorized Intruder

➤ **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
- Four RMON Groups (History, Statistics, Alarms, and Events)
- **IPv6** IP Address / NTP / DNS Management
- Built-in Trivial File Transfer Protocol (TFTP) Client
- BOOTP and DHCP for IP Address Assignment
- Firmware Upload / Download via HTTP / TFTP
- DHCP Relay
- DHCP Option 82
- User Privilege Levels Control
- NTP (Network Time Protocol)
- Link Layer Discovery Protocol (LLDP) Protocol
- SFP-**DDM** (Digital Diagnostic Monitor)
- Cable Diagnostic technology provides the mechanism to detect and report potential cabling issues
- Reset Button for System Reboot or Reset to Factory Default
- INTERLOGIX Smart Discovery Utility for Deploy Management

1.5 Product Specifications

Product	NS4750-24S-4T-4X
Hardware Specification	
SFP/mini-GBIC Slots	24 1000Base-SX/LX/BX SFP interfaces (Compatible with 100Base-FX SFP Transceiver)
10Gbps Fiber Ports	4 1/10GBase-SR/LR SFP+ slots
Copper Ports	4 10/ 100/1000Base-T TP/SFP combo ports
Console Port	1 x RS-232 RJ45 serial port (115200, 8, N, 1)
Switch Processing Scheme	Store-and-Forward
Switch Throughput@64Bytes	95.2Mpps
Switch Fabric	128Gbps / non-blocking
Address Table	16K entries, automatic source address learning and ageing
Share data Buffer	16Mbits
Flow Control	IEEE 802.3x pause frame for full-duplex Back pressure for half-duplex
Jumbo Frame	10Kbytes
Reset Button	< 5 seconds: System reboot > 10 seconds: Factory default
Dimensions (W x D x H)	440 x 200 x 44.5 mm, 1U high
Weight	2.935kg
LED	Power, DC1, DC2, Fault, Ring, R.O., Link/Act and speed per Gigabit port
Power Consumption	Max. 57 watts / 197.6BTU
Power Requirement – AC	AC 100~240V, 50/60Hz 1.5A
Power Requirement – DC	-36V DC @ 1.6A, Range: -36V ~ -60V DC
DI/DO	2 Digital Input (DI): Level 0: -24~2.4V ($\pm 0.1V$) Level 1: 2.4~24V ($\pm 0.1V$) Input Load Current: 10mA max. 2 Digital Output (DO): Open collector to 24VDC, 100mA max. load
Layer 2 Function	
Port Configuration	Port disable / enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Flow Control disable / enable Bandwidth control on each port Power saving mode control
Port Status	Display each port's speed duplex mode, link status, flow control status, auto negotiation status, trunk status

VLAN	802.1Q Tagged based VLAN Port-based VLAN Q-in-Q Private VLAN Edge (PVE) Up to 256 VLAN groups, out of 4094 VLAN IDs
Port Trunking	IEEE 802.3ad LACP / Static Trunk 12 groups of 16-port trunk support
QoS	Traffic classification based, Strict priority and WRR 4-level priority for switching - Port Number - 802.1p priority - 802.1Q VLAN tag DSCP/TOS field in IP Packet Policy-based QoS
IGMP Snooping	IGMP (v1/v2/v3) Snooping, up to 255 multicast Groups IGMP Querier and Fast Leave mode support
Access Control List	IP-based ACL / MAC-based ACL Up to 256 entries
Management	
Basic Management Interfaces	Console, Telnet, Web Browser, SNMPv1, v2c and v3
Secure Management Interface	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-2819 RMON MIB (Group 1, 2) RFC-2737 Entity MIB RFC-2618 RADIUS Client MIB RFC3411 SNMP-Frameworks-MIB IEEE 802.1X PAE LLDP MAU-MIB
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX/100Base-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000Base-T IEEE 802.3ae 10 Gigabit Ethernet 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 ITU G.8032 Ethernet Ring Protection Switching 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
Environment	
Operating	Temperature: -10 ~ 60 degrees C for DC power input 0 ~ 50 degrees C for AC power input Relative Humidity: 5 ~ 95% (non-condensing)
Storage	Temperature: -10 ~ 70 degrees C Relative Humidity: 5 ~ 95% (non-condensing)

2. INSTALLATION

2.1 Hardware Descriptions

The Managed Switch provides four different running speeds – 10Mbps, 100Mbps, 1000Mbps and 10Gbps in the same Switch and automatically distinguishes the speed of incoming connection. This section describes the hardware features of 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. Before connecting any network device to the Managed Switch, read this chapter carefully.

2.1.1 Front Panel

Figure 2-1 shows the front panel of **Managed Switch**.



Figure 2-1: NS4750-24S-4T-4X Switch Front Panel

■ Gigabit TP interface

10/100/1000Base-T Copper, RJ-45 Twist-Pair: Up to 100 meters.

■ Gigabit SFP slots

1000Base-SX/LX mini-GBIC slot, SFP (Small Factor Pluggable) Transceiver Module supports from 550 meters (Multi-mode Fiber), up to 10/30/50/70/120 kilometers (Single Mode Fiber).

■ 10 Gigabit SFP slots

10GBase-SR/LR mini-GBIC slot, SFP (Small Factor Pluggable) Transceiver Module supports from 300 meters (Multi-mode Fiber), up to 10 kilometers (Single Mode Fiber)

■ Console Port

The console port is a RJ-45 port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information including IP address setting, factory reset, port management, link status and system setting. Users can use the attached DB9 to RJ-45 console cable in the package and connect to the console port on the device. After the connection, users can run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the startup screen of the device.

■ Reset button

On the front panel, the reset button is designed for rebooting the Managed Switch without turning off and on the power. The following is the summary table of reset button functions:

Reset Button (Press and Release)	Function
< 5 sec: System Reboot	Reboot the Managed Switch
> 5 sec: Factory Default	<p>Reset the Managed Switch to Factory Default configuration. The Managed Switch will then reboot and load the default settings as shown below:</p> <ul style="list-style-type: none"> ◦ 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

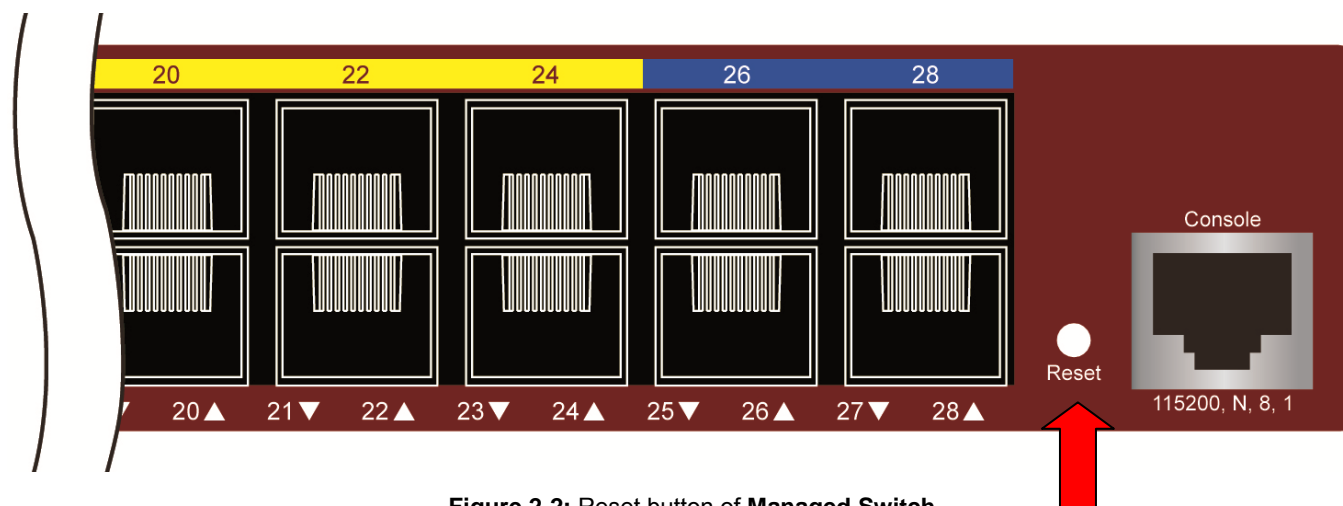


Figure 2-2: Reset button of Managed Switch



1. Press the RESET button once and the **Managed Switch** will reboot automatically.
2. Press the RESET button for 5 seconds and the **Managed Switch** will be back to the factory default mode; the entire configuration will be erased.

■ AC Power Receptacle

For compatibility with electric service in most areas of the world, the Managed Switch's power supply automatically adjusts to line power in the range of 100-240V AC and 50/60 Hz.

Plug the female end of the power cord firmly into the receptable on the front panel of the Managed Switch. Plug the other end of the power cord into an electric service outlet and then the power will be ready.



The device is a power-required device, which means it will not work till it is powered. If your networks should be active all the time, please consider using UPS (Uninterrupted Power Supply) for your device. It will prevent you from network data loss or network downtime. In some areas, installing a surge suppression device may also help to protect your Managed Switch from being damaged by unregulated surge or current to the Switch or the power adapter.

■ DC Power Connector

The front panel of the Managed Switch contains a power switch and a DC power connector, which accepts DC power input voltage from -36V to -60V DC. Connect the power cable to the Managed Switch at the input terminal block. The size of the two screws in the terminal block is M3.5.

■ Digital Input

The digitail input of the Managed Switch can be activated by the external sensor that senses physical changes. These changes can include intrusion detection or certain physical change in the monitored area. For example, the external sensor can be a door switch or an infrared motion detector.

■ Digital Output

The digital output main function is to allow the Managed Switch to trigger external devices, either automatically or by remote control from a human operator or a software application.

2.1.2 LED Indications

■ System

LED	Color	Function	
Ring	Green	Lights	Indicates that Ring state is in idle mode.
		Blinks	Indicates that the Ring state is in protected mode.
R.O.	Green	Lights	Indicates that the switch is set to ring owner.
		Off	Indicates that the switch doesn't set to ring owner.
DC1	Green	Lights	Indicates that the Switch is powered on by DC1 input.
DC2	Green	Lights	Indicates that the Switch is powered on by DC2 input.
FAN1	Green	Lights	Indicates that Fan 1 has stopped.

FAN2	Green	Lights	Indicates that Fan 2 has stopped.
Fault	Green	Lights	Indicates that Switch AC/DC or port has failed.
PWR	Green	Lights	Indicates that the Switch is powered on.
		Blinks	Indicates the system is running under booting procedure.

■ 10/100/1000Base-T interfaces for port1 to port24 SFP slot

LED	Color	Function	
LNK/ACT	Green	Lights	Indicates the link through that SFP port is successfully established with speed 1000Mbps .
		Blinks	Indicates that the switch is actively sending or receiving data over that port.
		Off	Indicates that the SFP port is link down.
	Orange	Lights	Indicates the link through that SFP port is successfully established with speed 10Mbps or 100Mbps.
		Blinks	Indicates that the switch is actively sending or receiving data over that port.
		Off	Indicates that the SFP port is link down.

■ 10/100/1000Base-T interfaces (Shared Port1~Port4)

LED	Color	Function	
LNK/ACT	Green	Lights	Indicates the link through that port is successfully established with 1Gbps.
		Off	Indicates that the port is link down
	Orange	Lights	Indicates the link through that SFP port is successfully established with speed 10Mbps or 100Mbps.
		Off	Indicates that the port is link down

■ 10Base-SR/LR SFP+ interfaces for port25 to port28

LED	Color	Function	
LNK/ACT	Green	Lights	Indicates the link through that SFP port is successfully established with 10Gbps
		Off	Indicates that the SFP port is link down
	Orange	Lights	Indicates the link through that SFP port is successfully established with 1Gbps
		Off	Indicates that the SFP port is link down

2.1.3 Wiring the AC Power Input

The rear panel of the NS4750 indicates an AC inlet power socket, which accepts input power from 100 to 240V AC, 50/60Hz.



2.1.4 Wiring the DC Power Input

The 6-contact terminal block connector on the front panel of NS4750 is used for two DC redundant power input. Please follow the steps below to insert the power wire.

1. Insert positive / negative DC power wires into contacts 1 and 2 for DC POWER 1, or 5 and 6 for DC POWER 2.

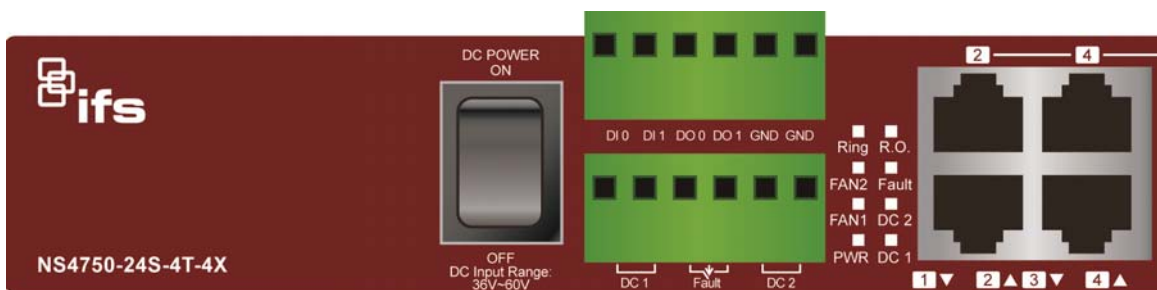


Figure 2-3: NS4750-24S-4T-4X Upper Panel

2. Tighten the wire-clamp screws for preventing the wires from loosening.

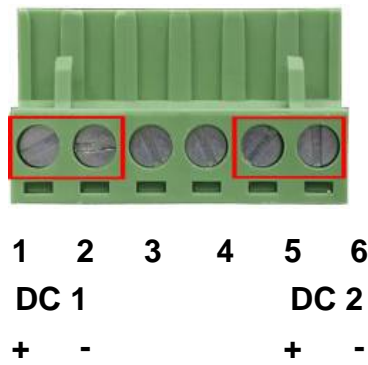


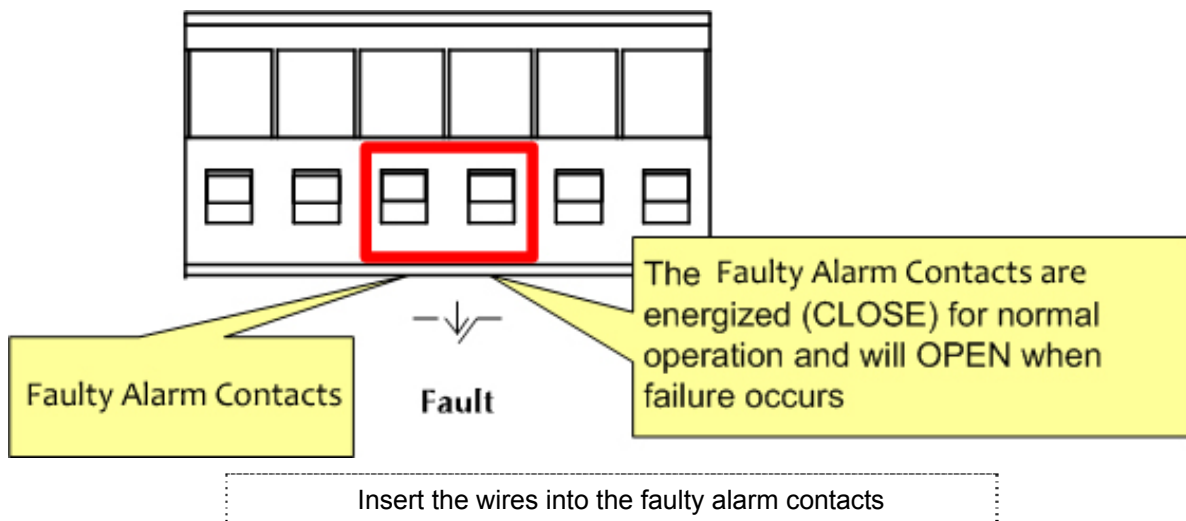
Figure 2-4 6-Pin Terminal Block Power Wiring Input



1. The wire gauge for the terminal block should be in the range of 12 ~ 24 AWG.
2. When performing any of the procedures like inserting the wires or tighten the wire-clamp screws, make sure the power is OFF to prevent from getting an electric shock.

2.1.5 Wiring the Faulty Alarm Contact

The fault alarm contacts are in the middle (3 & 4) of the terminal block connector as the picture shows below. Inserting the wires, the **Managed Switch** will detect the fault status of the power failure, or port link failure (available for managed model) when **Fault Alarm** function has been enabled. The following illustration shows an application example for wiring the fault alarm contacts



1. The wire gauge for the terminal block should be in the range of 12 ~ 24 AWG.
2. When performing any of the procedures like inserting the wires or tighten the wire-clamp screws, make sure the power is OFF to prevent from getting an electric shock.

2.1.6 Wiring the Digital Input / Output

The 6-contact terminal block connector on the front panel of NS4750-24S-4T-4X is used for Digital Input and Digital Output.

Please follow the steps below to insert wire.

1. The NS4750-24S-4T-4X offers two DI and DO groups. 1 and 2 are DI groups, 3 and 4 are DO groups and 5 and 6 are GND (ground).

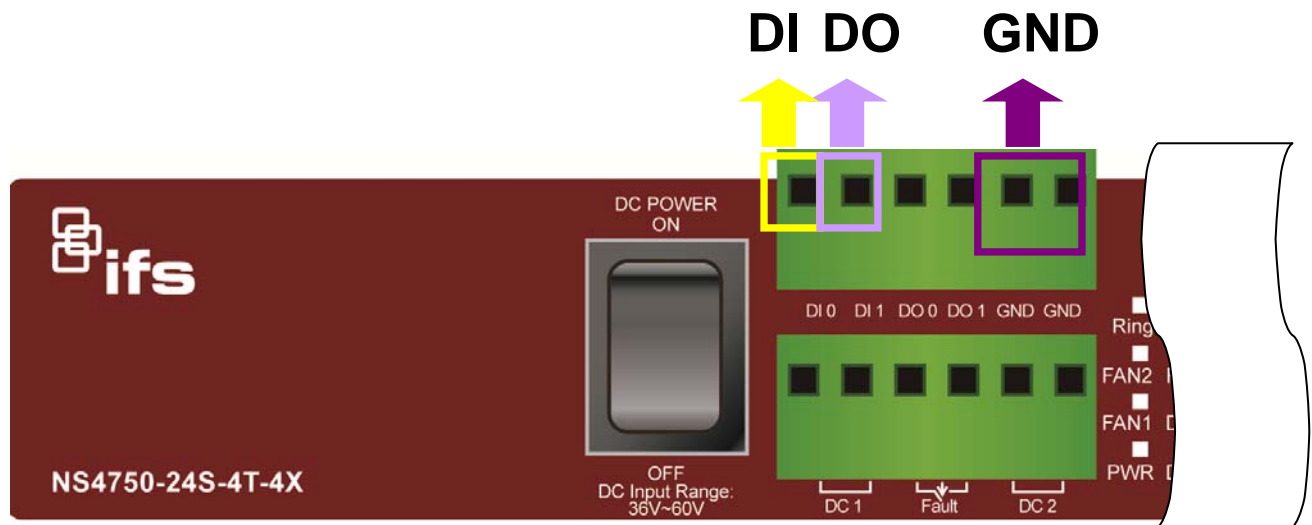


Figure 2-5 Wiring the Redundant Power Inputs

Tighten the wire-clamp screws for preventing the wires from loosening.

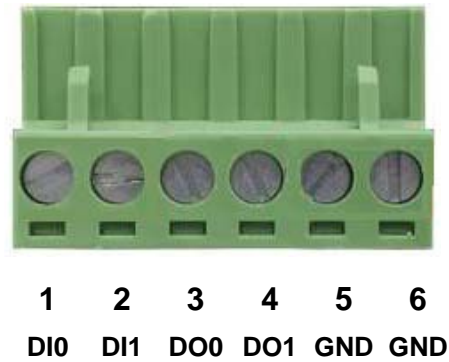


Figure 2-6 6-Pin Terminal Block DI / DO Wiring Input

2. There are two Digital Input groups for you to monitor two different devices. The following topology shows how to wire DI0 and DI1. We use the NS4750-24S-4T-4X to be an example for describing DI application.

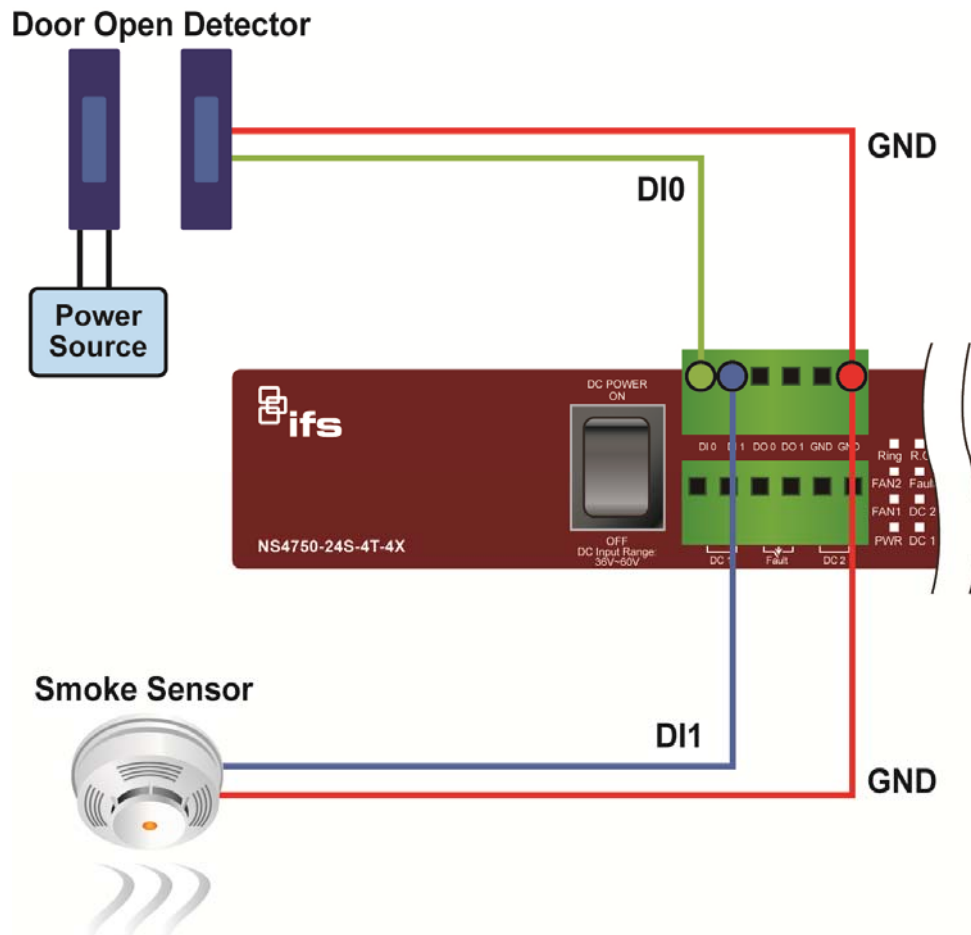


Figure 2-7 Wires DI0 and DI1 to Open Detector

3. There are two Digital Output groups for you to sense NS4750-24S-4T-4X port failure or power failure and issue a high or low signal to external device. The following topology shows how to wire DO0 and DO1.

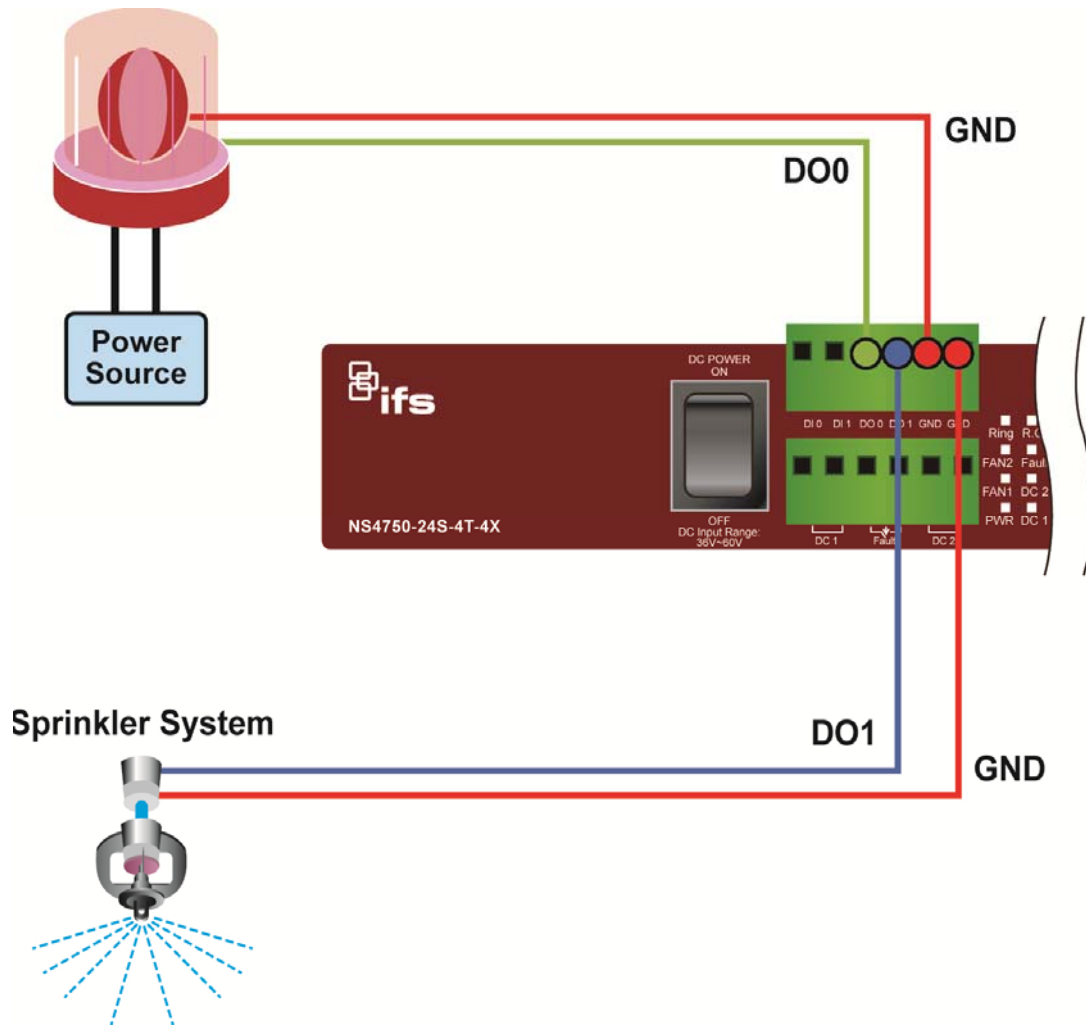


Figure 2-8 Wires DO0 and DO1 to Open Detector

2.2 Installing the Managed Switch

This section describes how to install your **Managed Switch** and make connections to the **Managed Switch**. Please read the following topics and perform the procedures in the order being presented. To install your **Managed Switch** on a desktop or shelf, simply complete the following steps.

In this paragraph, we will describe how to install the **Managed Switch** and the installation points attended to it.

2.2.1 Desktop Installation

To install the Managed Switch on desktop or shelf, please follow these steps:

Step1: Attach the rubber feet to the recessed areas on the bottom of the Managed Switch.

Step2: Place the Managed Switch on the desktop or the shelf near an AC/DC power source as shown in Figure 2-4.

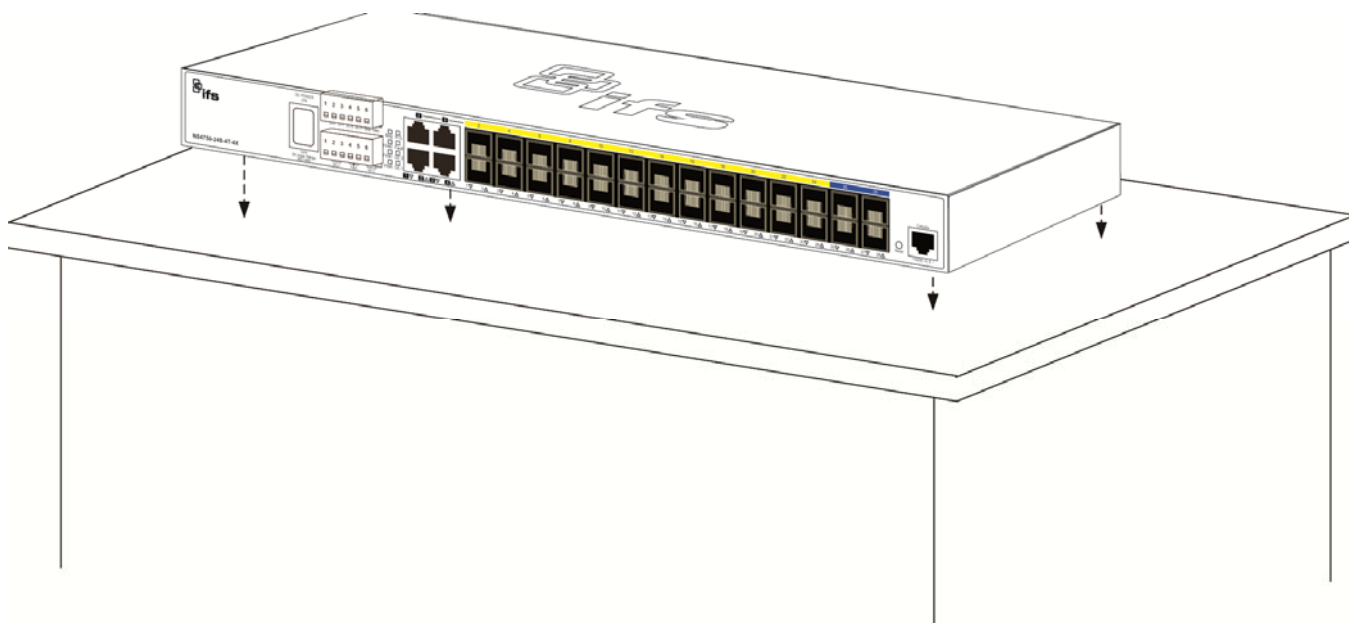


Figure 2-4 Place the Managed Switch on the Desktop

Step3: Keep enough ventilation space between the Managed Switch and the surrounding objects.

Step4: Connect the Managed Switch to network devices.

Connect one end of a standard network cable to the 10/100/1000 RJ-45 ports on the front of the Managed Switch.

Connect the other end of the cable to the network devices such as printer servers, workstations or routers, etc.



Connecting to the Managed Switch requires UTP Category 5 network cabling with RJ-45 tips. For more information, please see the Cabling Specification in Appendix A.

Step5: Supply power to the Managed Switch.

Connect one end of the power cable to the Managed Switch.

Connect the power plug of the power cable to a standard wall outlet.

When the Managed Switch receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting

To install the Managed Switch in a 19-inch standard rack, please follow the instructions described below.

Step1: Place the Managed Switch on a hard flat surface, with the front panel positioned towards the front side.

Step2: Attach the rack-mount bracket to each side of the Managed Switch with supplied screws attached to the package.

Figure 2-5 shows how to attach brackets to one side of the Managed Switch.

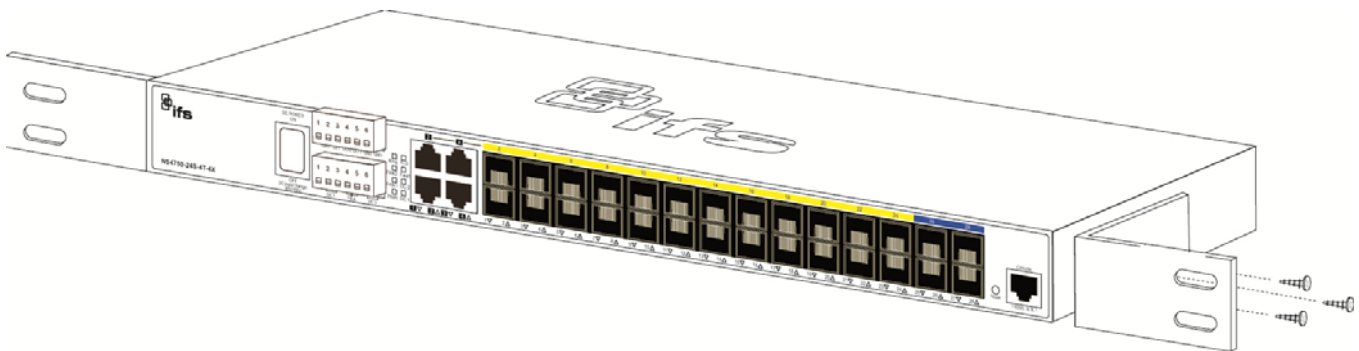


Figure 2-5 Attach Brackets to the Managed Switch.



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

Step3: Secure the brackets tightly.

Step4: Follow the same steps to attach the second bracket to the opposite side.

Step5: After the brackets are attached to the Managed Switch, use suitable screws to securely attach the brackets to the rack as shown in Figure 2-6.

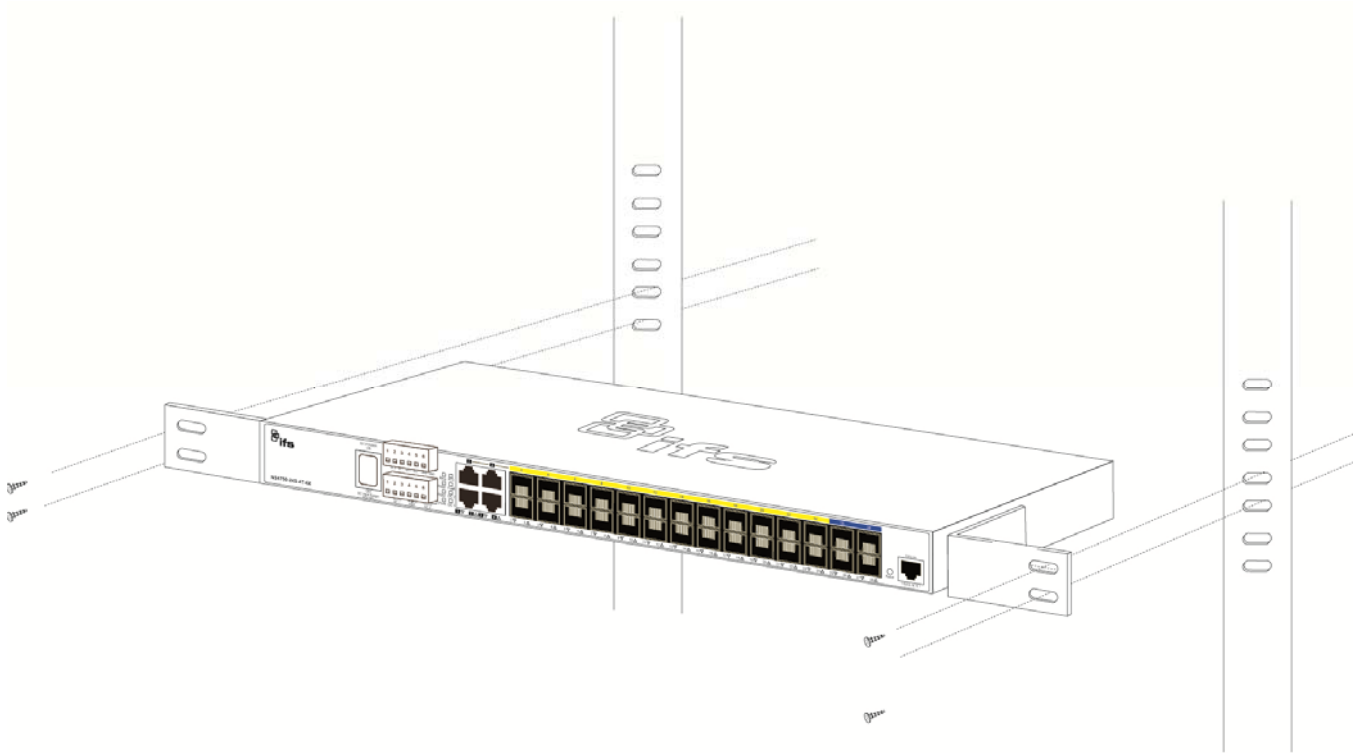


Figure 2-6 Mounting the Managed Switch on a Rack

Step6: Proceeds with steps 4 and 5 of session 2.2.1 Desktop Installation to connect the network cabling and supply power to the Managed Switch.

2.3 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 10Mbps, 20Mbps, 100Mbps or 200Mbps and 1000Mbps or 2000Mbps after the negotiation with the connected device. The **Managed Switch** has eight SFP interfaces that support 100/1000Mbps dual speed mode (Optional multi-mode/ single-mode 100Base-FX/1000Base-SX/LX SFP module)

■ Cabling

Each 10/100/1000Base-T port uses RJ-45 sockets -- 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 100Mbps 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 is used as LC connector with optional SFP module. Please see table below and know more about the cable specifications.

Port Type	Cable Type	Connector
10Base-T	Cat 3, 4, 5, 2-pair	RJ-45
100Base-TX	Cat.5 UTP, 2-pair	RJ-45
1000Base-T	Cat.5/5e/6 UTP, 2-pair	RJ-45
100Base-FX	50 / 125µm or 62.5 / 125µm multi-mode 9 / 125µm single-mode	LC (multi/single mode)
1000Base-SX/LX	50 / 125µm or 62.5 / 125µm multi-mode 9 / 125µm single-mode	LC (multi/single mode)
10GBase-SR/LR	50 / 125µm or 62.5 / 125µm multi-mode 9 / 125µm single-mode	LC (multi/single mode)

Any Ethernet devices like hubs/PCs can be connected to the **Managed Switch** by using straight-through wires. The two 10/100/1000Mbps ports are auto-MDI/MDI-X, which can be used on straight-through or crossover cable.

2.3.1 Installing the SFP Transceiver

The sections describe how to insert an SFP transceiver into an SFP slot. The SFP transceivers are hot-pluggable and hot-swappable. You can plug in and out the transceiver to/from any SFP port without having to power down the **Managed Switch** as [Figure 2-9](#) shows below:

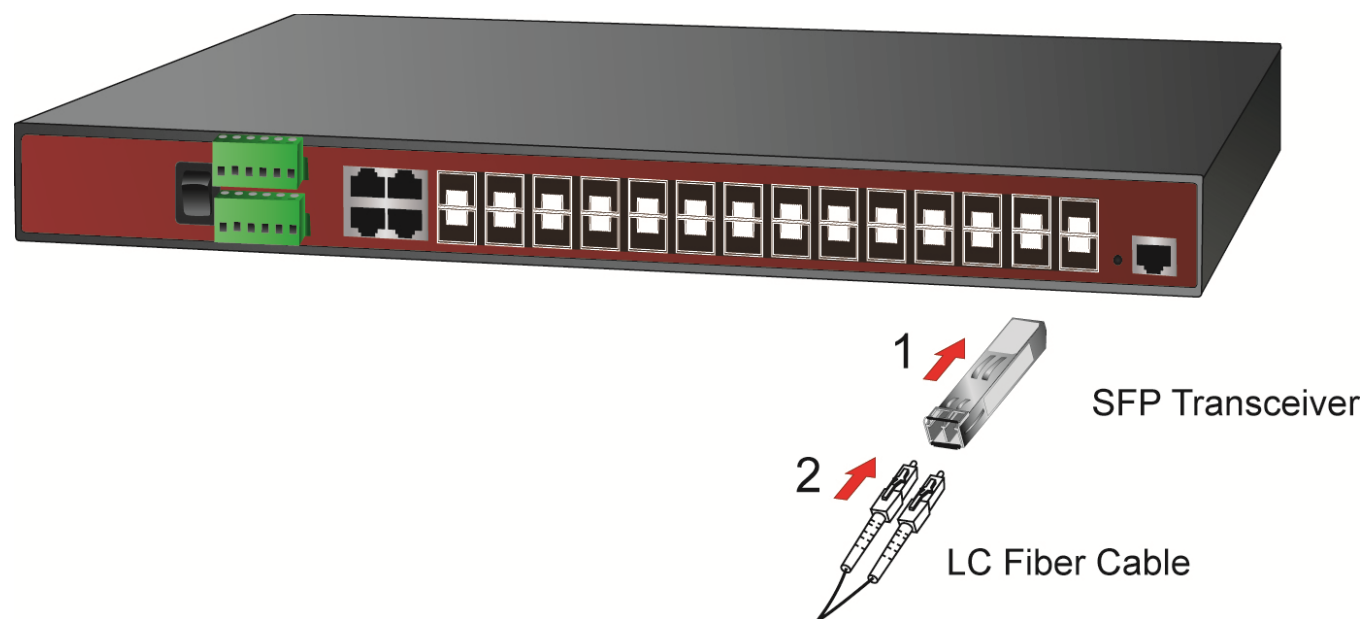


Figure 2-9: Plugging in the SFP Transceiver

■ Approved INTERLOGIX SFP Transceivers

INTERLOGIX **Managed Switch** supports 100/1000 dual mode with both single mode and multi-mode SFP transceivers. The following list of approved INTERLOGIX SFP transceivers is correct at the time of publication:

Gigabit SFP Transceiver Modules

S30-RJ	SFP-Port 1000Base-T Module – 100M	
S30-2MLC	SFP-Port 1000Base-SX mini-GBIC module – 550M	0~50°C
S35-2MLC	SFP-Port 1000Base-SX mini-GBIC module – 550M	-40~75°C
S30-2MLC-2	SFP-Port 1000Base-SX mini-GBIC module – 2KM	0~50°C
S30-2SLC-10	SFP-Port 1000Base-LX mini-GBIC module – 10KM	0~50°C
S35-2SLC-10	SFP-Port 1000Base-LX mini-GBIC module – 10KM	-40~75°C
S30-2SLC-30	SFP-Port 1000Base-LX mini-GBIC module - 30KM	0~50°C
S35-2SLC-30	SFP-Port 1000Base-LX mini-GBIC module - 30KM	-40~75°C

S30-2SLC-70	SFP-Port 1000Base-LX mini-GBIC module - 70KM	0~50•C
--------------------	--	--------

S35-2SLC-70	SFP-Port 1000Base-LX mini-GBIC module - 70KM	-40~75•C
--------------------	--	----------

S30-1SLC/A-10	SFP-Port 1000Base-BX GBIC module - 10KM	0~50•C
----------------------	---	--------

S30-1SLC/B-10	SFP-Port 1000Base-BX GBIC module - 10KM	0~50•C
----------------------	---	--------

S30-1SLC/A-20	SFP-Port 1000Base-BX GBIC module - 20KM	0~50•C
----------------------	---	--------

S30-1SLC/B-20	SFP-Port 1000Base-BX GBIC module - 20KM	0~50•C
----------------------	---	--------

S30-1SLC/A-60	SFP-Port 1000Base-BX GBIC module - 60KM	0~50•C
----------------------	---	--------

S30-1SLC/B-60	SFP-Port 1000Base-BX GBIC module - 60KM	0~50•C
----------------------	---	--------

Fast Ethernet SFP Transceiver Modules

S20-2SLC-2	SFP-Port 100Base-FX Transceiver (1310nm) - 2KM	0~50•C
-------------------	--	--------

S25-2SLC-2	SFP-Port 100Base-FX Transceiver (1310nm) - 2KM	-40~75•C
-------------------	--	----------

S20-2SLC-20	SFP-Port 100Base-FX Transceiver (1310nm) - 20KM	0~50•C
--------------------	---	--------

S25-2SLC-20	SFP-Port 100Base-FX Transceiver (1310nm) - 20KM	-40~75•C
--------------------	---	----------

S20-ISLC/A-20	SFP-Port 100Base-BX Transceiver (WDM,TX:1310nm) - 20KM	0~50•C
----------------------	--	--------

S20-ISLC/B-20	SFP-Port 100Base-BX Transceiver (WDM,TX:1550nm) - 20KM	-40~75•C
----------------------	--	----------

10 Giga SFP+ Transceiver Modules

S40-2MLC	SFP-Port 1G Base-SX Transceiver – 300M*	0~50•C
-----------------	---	--------

S40-2SLC-10	SFP-Port 1G Base-SX Transceiver - 10KM	0~50•C
--------------------	--	--------

- * 62.5/125um fiber only supports 33meter, for 300m use OM3 50/125um.



1. It is recommended to use INTERLOGIX SFPs on the **Managed Switch**. If you insert an SFP transceiver that is not supported, the **Managed Switch** will not recognize it.
2. Please choose the SFP transceiver which can be operated under -40~75 degrees C temperature if the switch device is working in an 0~50 degrees C temperature environment.

1000Base-SX/LX:

Before connecting the 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 the fiber-optic cable type that matches the SFP transceiver model.
 - To connect to 1000Base-SX SFP transceiver, use the multi-mode fiber cable with one side being the male duplex LC connector type.
 - To connect to 1000Base-LX SFP transceiver, use the single-mode fiber cable with one side being the male duplex LC connector type.

Connecting the fiber cable

1. Insert the duplex LC connector on the network cable into the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a media converter.
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 the other switches, workstation or media converter.

1. Make sure both sides of the SFP transceiver are with the same media type or WDM pair, for example, 100Base-FX to 100Base-FX, 100Base-BX20-U to 100Base-BX20-D.
2. Check the fiber-optic cable type that matches the SFP transceiver model.
 - To connect to MFB-FX SFP transceiver, use the multi-mode fiber cable with one side being the male duplex LC connector type.
 - To connect to MFB-F20/F40/F60/FA20/FB20 SFP transceiver, use the single-mode fiber cable with one side being the male duplex LC connector type.

Connecting the fiber cable

1. Attach the duplex LC connector on the network cable into the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a media converter.
3. Check the LNK/ACT LED of the SFP slot of the switch/converter. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link fails. Co works with some fiber-NICs or media converters. Set the Link mode to “**100 Force**” when needed.

2.3.2 Removing the 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) to disable the port in advance.
2. Remove the Fiber Optic Cable gently.
3. Lift up the lever of the MGB module and turn it to a horizontal position.
4. Pull out the module gently through the lever.

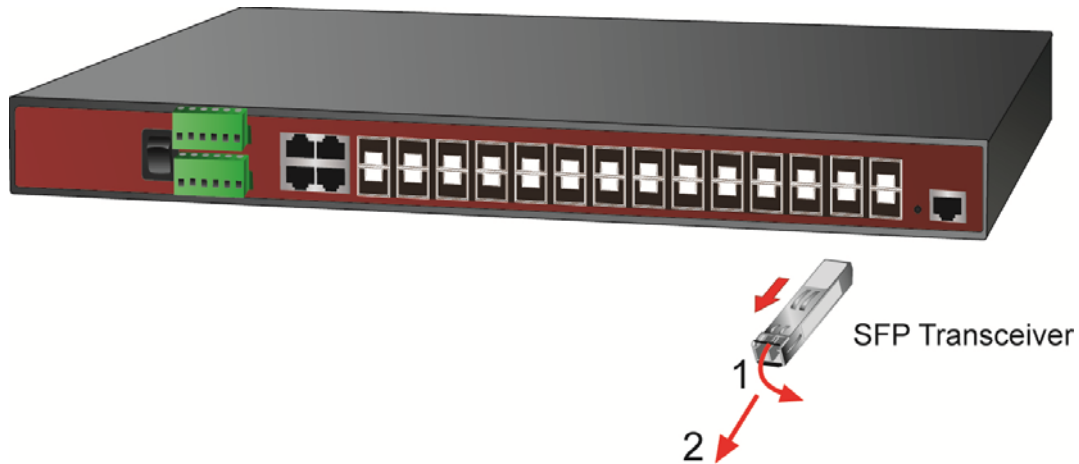


Figure 2-10: How to Pull Out the SFP Transceiver Module



Never pull out the module without lifting up the lever of the module and turning it to a horizontal position. Directly pulling out the module could damage the module and the SFP module slot of the Managed Switch.

3. SWITCH MANAGEMENT

This chapter explains the methods that you can use to configure management access to the **Managed Switch**. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Requirements
- Management Access Overview
- Remote Telnet Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Requirements

- Workstations of subscribers running Windows XP/2003, Vista, Windows 7, MAC OS X, Linux, Fedora, Ubuntu or other platform compatible with **TCP/IP** protocols.
- **Workstation** installed with **Ethernet NIC** (Network Interface Card)
- Ethernet Port connect
 - Network cables - Use standard network (UTP) cables with RJ45 connectors.
 - The above Workstation is installed with **WEB Browser** and **JAVA runtime environment** Plug-in



It is recommended to use Internet Explore 7.0 or above to access **Managed Switch**.

3.2 Management Access Overview

The **Managed Switch** gives you 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 Remote Telnet and Web browser interface support are embedded in the **Managed Switch** software and are available for immediate use. Each of these management methods has their own advantages. Table 3-1 compares the three management methods.

Method	Advantages	Disadvantages
Remote Telnet	<ul style="list-style-type: none">• Text-based• Telnet functionality built into Windows XP/2003, Vista, Windows 7 operating systems• Can be accesses from any location	<ul style="list-style-type: none">• Security can be compromised (hackers need only know the IP address)
Web Browser	<ul style="list-style-type: none">• Ideal for configuring the switch remotely• Compatible with all popular browsers• Can be accessed from any location• Most visually appealing	<ul style="list-style-type: none">• Security can be compromised (hackers need only know the IP address and subnet mask)• May encounter lag times on poor connections
SNMP Agent	<ul style="list-style-type: none">• Communicates with switch functions at the MIB level• Based on open standards	<ul style="list-style-type: none">• Requires SNMP manager software• Least visually appealing of all three methods• Some settings require calculations• Security can be compromised (hackers need only know the community name)

Table 3-1: Comparison of Management Methods

3.3 CLI Mode Management

There are two ways for CLI mode management, one is remote telnet, and the other is operating from console port. Remote telnet is an IP-based protocol, and console port is for user to operate the NS4750-24S-4T-4X on local only, however their operation is the same.

The command line user interface is for performing system administration, such as displaying statistics or changing option settings. Using this method, you can access the **Managed Switch** remote telnet interface from personal computer, or workstation in the same Ethernet environment as long as you know the current IP address of the **Managed Switch**.

**PC / Workstation with
IE Browser
192.168.0.X**

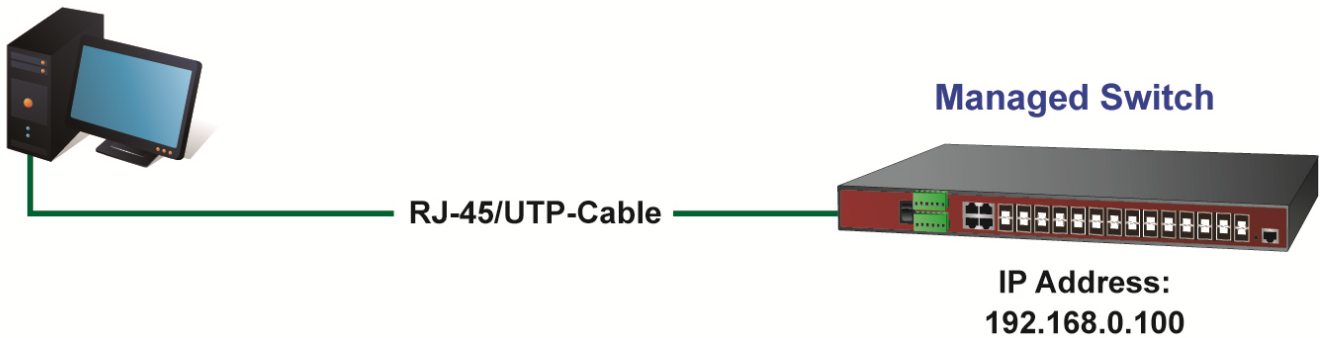


Figure 3-1: Remote Telnet and Console Port Interface Management

In Windows system, you may click “**Start**”, then choose “**Accessories**” and “**Command Prompt**”. Please input “**telnet 192.168.0.100**” and press “**enter**” from your keyboard. You will see the following screen (see Figure 3-2) appear.

```
COM1_115200 -
Username:
Password: +Jaguar-1 board detected (VSC7460 Rev. B).
RAM: 0x80000000-0x88000000 [0x80020908-0x87fe1000 available]
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
== Executing boot script in 3.000 seconds - enter ^C to abort
> fis load -d managed
Image loaded from 0x80040000-0x8083d8b8
> go
exit
Welcome to NS4750-24S-4T-4X Command Line Interface.
Port Numbers:

+-----+
| 2| 4| | 2| 4| 6| 8|10|12|14|16|18|20|22|24| |26|28|
+-----+
| 1| 3| | 1| 3| 5| 7| 9|11|13|15|17|19|21|23| |25|27|
+-----+

Username: admin
Password:
Login in progress...
NS4750-24S-4T-4X:/>
```

Figure 3-2: Remote Telnet Interface Main Screen of **Managed Switch**

For more information about using the Remote Telnet interface, refer to **Chapter 5 Remote Telnet Interface Management**.

3.4 Web Management

The **Managed Switch** offers management features that allow users to manage the **Managed Switch** from anywhere on the network through a standard browser such as Microsoft Internet Explorer. After you set up your IP address for the **Managed Switch**, you can access the **Managed Switch**'s Web interface applications directly in your Web browser by entering the IP address of the **Managed Switch**.

**PC / Workstation with
IE Browser
192.168.0.X**

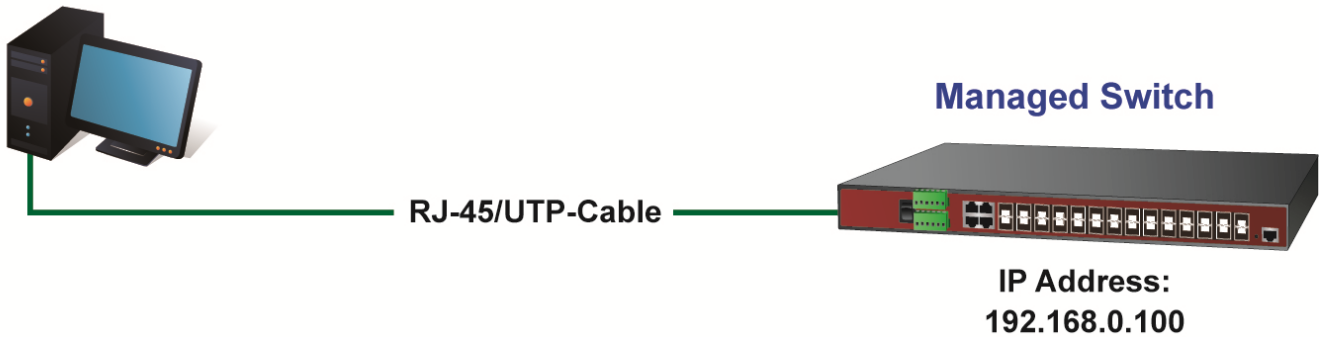


Figure 3-3: Web Management

You can then use your Web browser to list and manage the **Managed Switch** configuration parameters from one central location; the Web Management requires **Microsoft Internet Explorer 7.0** or later.

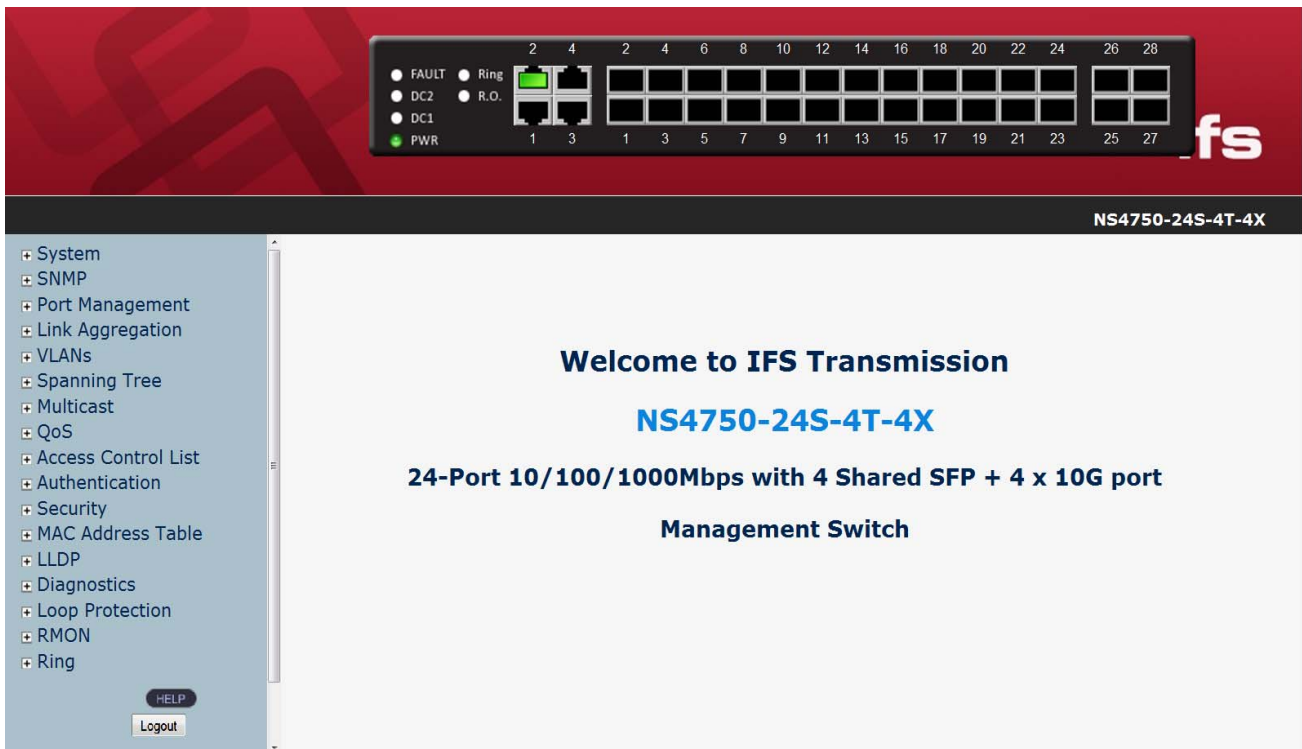


Figure 3-4: Web Main Screen of Managed Switch

3.5 SNMP-based Network Management

You can 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 **Managed Switch** and the SNMP Network Management Station to use the **same community string**. This management method, in fact, 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 getting and setting community strings for the **Managed Switch** is public.

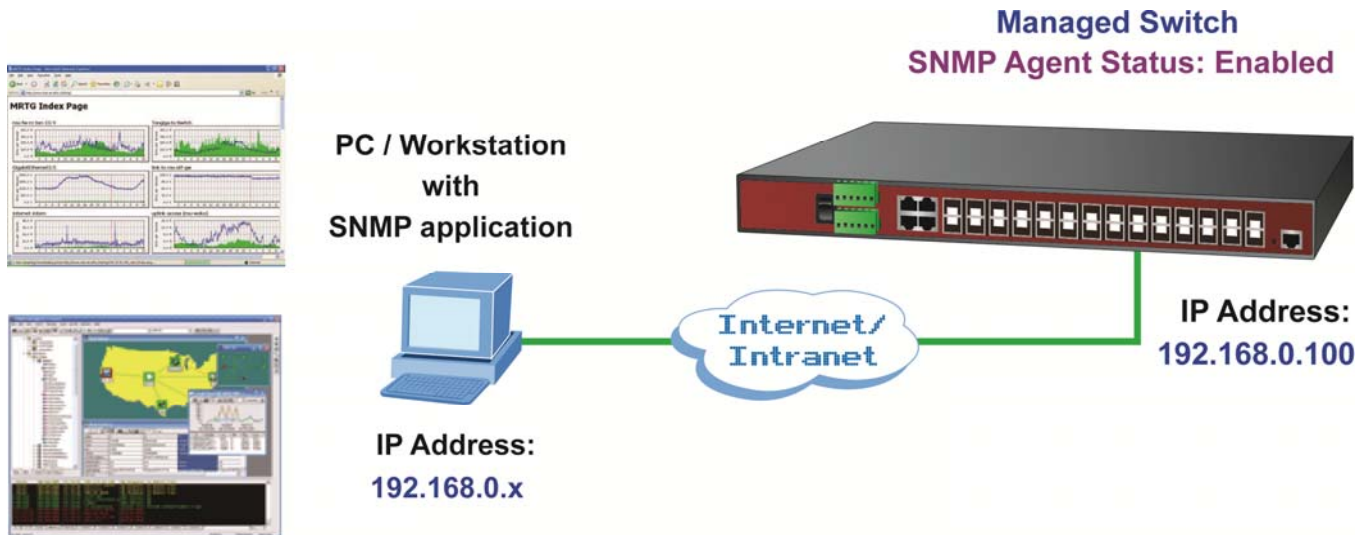


Figure 3-5: SNMP Management

4. WEB CONFIGURATION

This section introduces the configuration and functions of the Web-based management.

About Web-based Management

The **Managed Switch** offers management features that allow users to manage the **Managed Switch** from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 7.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.



By default, IE8.0 or later version 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 Switch** can be configured through an Ethernet connection, making sure the manager PC must be set on the same IP subnet address with the **Managed Switch**.

For example, the default IP address of the **Managed Switch** is **192.168.0.100**, then the manager PC 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 you have changed the default IP address of the **Managed Switch** to 192.168.1.1 with subnet mask 255.255.255.0 via console, then the manager PC should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on manager PC.

**PC / Workstation with
IE Browser
192.168.0.X**



RJ-45/UTP-Cable

Managed Switch



**IP Address:
192.168.0.100**

Figure 4-1-1: Web Management

■ Logging on the Managed Switch

1. Use Internet Explorer 7.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP Address is shown as follows:

http://192.168.0.100

2. When the following login screen appears, please enter the default username "**admin**" with password "**admin**" (or the username/password you have changed via console) to login the main screen of **Managed Switch**. The login screen in [Figure 4-1-2](#) appears.



Figure 4-1-2: Login Screen

Default User name: **admin**

Default Password: **admin**

After entering the username and password, the main screen appears as shown in [Figure 4-1-3](#).



Figure 4-1-3: Default Main Page

Now, you can use the Web management interface to continue the switch management or manage the **Managed Switch** by Web interface. The Switch Menu on the left of the web page let you access all the commands and statistics the Managed Switch provides.



1. It is recommended to use Internet Explorer 7.0 or above to access **Managed Switch**.
2. The changed IP address take effect immediately after clicking on the **Save** button, you need to use the new IP address to access the Web interface.
3. For security reason, please change and memorize the new password after this first setup.
4. Only accept command in lowercase letter under web interface.

4.1 Main Web Page

The **Managed Switch** provides a Web-based browser interface for configuring and managing it. This interface allows you to access the **Managed Switch** using the Web browser of your choice. This chapter describes how to use the **Managed Switch**'s Web browser interface to configure and manage it.

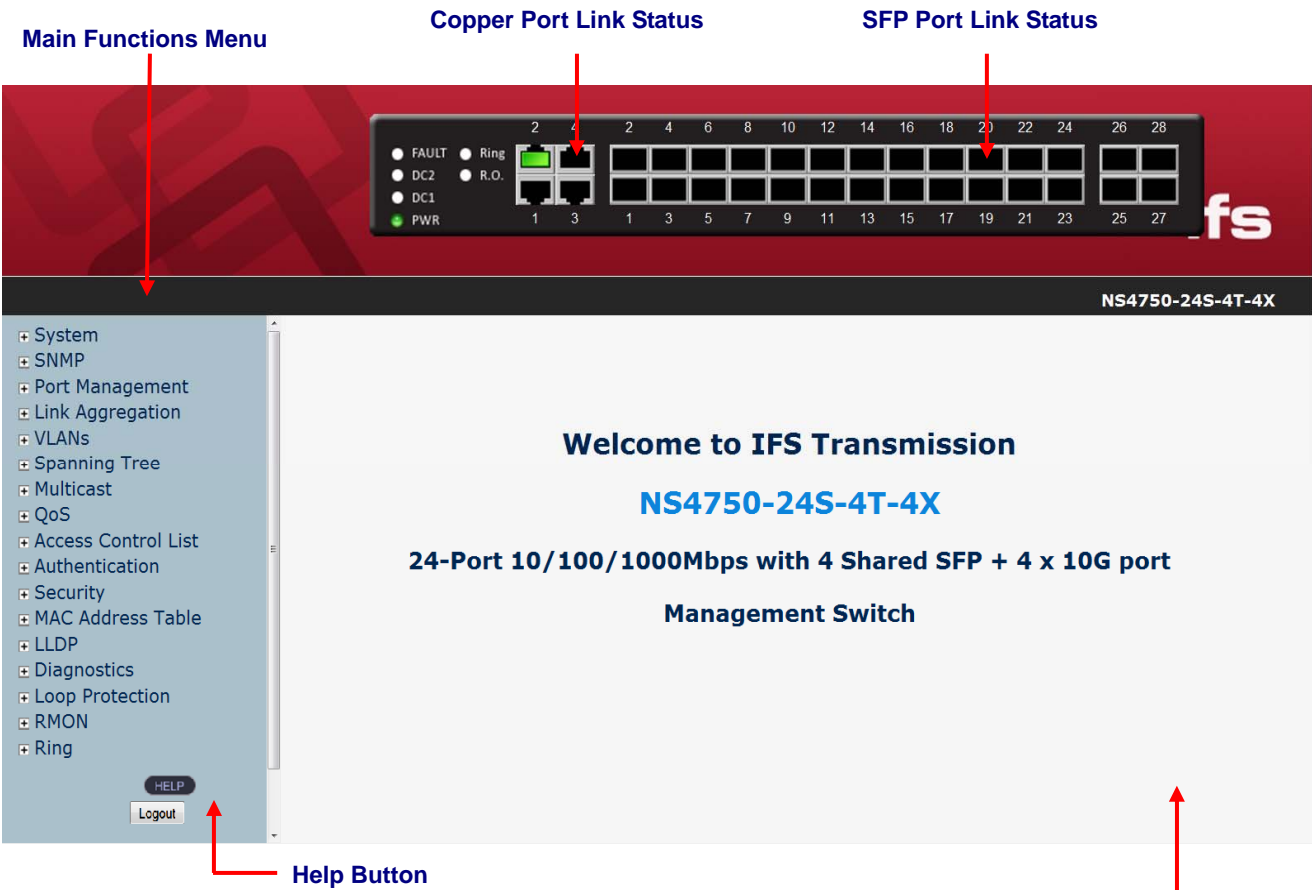


Figure 4-1-4: Main Page

Panel Display

The web agent 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.

The port states are illustrated as follows:

State	Disabled	Link Down	Link Up
RJ-45 Ports			
SFP Ports			

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the **Managed Switch**, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can setup the **Managed Switch** by selecting the functions those listed in the Main Function. The screen in [Figure 4-1-5](#) appears.

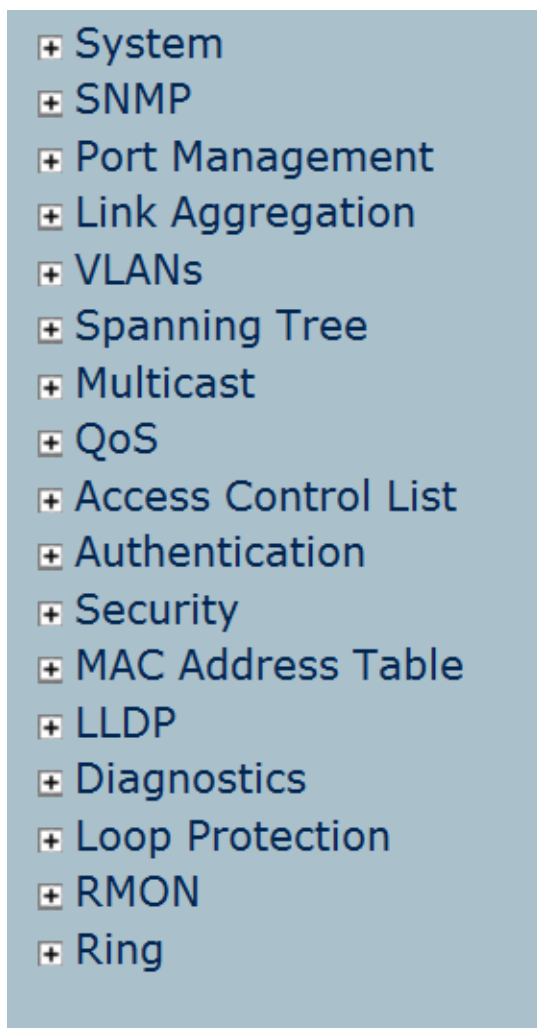


Figure 4-1-5: Managed Switch Main Functions Menu

4.2 System

Use the System menu items to display and configure basic administrative details of the **Managed Switch**. Under the System the following topics are provided to configure and view the system information.

4.2.1 System Information

The System Info page provides information for the current device information. System Info page helps a switch administrator to identify the hardware MAC address, software version and system uptime. The screen in [Figure 4-2-1](#) appears.

System Information	
System	
Contact	
Name	NS4750-24S-4T-4X
Location	
Hardware	
MAC Address	00-23-6f-6b-45-5a
Power Status	DC PWR1 :OFF DC PWR2 :OFF AC PWR :ON
Temperature	54.0 C - 129.0 F
Time	
System Date	1970-01-03 Sat 22:56:24+00:00
System Uptime	2d 22:56:24
Software	
Software Version	v1.5b140618
Software Date	2014-06-18T19:00:10+0800

Figure 4-2-1: System Information Page Screenshot

The page includes the following fields:

Object	Description
• Contact	The system contact configured in Configuration System Information System Contact.
• Name	The system name configured in Configuration System Information System Name.
• Location	The system location configured in Configuration System Information System Location.
• MAC Address	The MAC Address of this Managed Switch .

• Power	The AC Power, Power 1 and Power 2 ON/OFF Status display.
• Temperature	The temperature shows current of the switch inside temperature status.
• System Date	The current (GMT) system time and date. The system time is obtained through the configured SNTP Server, if any.
• 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 switch software was produced.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page.

4.2.2 IP Configuration

The IP Configuration includes the IP Address, Subnet Mask and Gateway. The Configured column is used to view or change the IP configuration. Fill up the IP Address, Subnet Mask and Gateway for the device. The screen in [Figure 4-2-2](#) appears.

IP Configuration

Mode	Host <input type="button" value="v"/>
DNS Server	No DNS server <input type="button" value="v"/> <input style="width: 100px;" type="text"/>
DNS Proxy	<input type="checkbox"/>

IP Interfaces

Delete	VLAN	IPv4 DHCP			IPv4		IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		192.168.0.100	24		

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
<input type="checkbox"/>	0.0.0.0	0	192.168.0.254	0

Figure 4-2-2: IP Configuration Page Screenshot

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

Object	Description		
• IP Configurations	Mode	Configure whether the IP stack should act as a Host or a Router . In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.	
	DNS Server	<p>This setting controls the DNS name resolution done by the switch. The following modes are supported:</p> <ul style="list-style-type: none">■ From any DHCP interfaces The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.■ No DNS server No DNS server will be used.■ Configured Explicitly provide the IP address of the DNS Server in dotted decimal notation.■ From this DHCP interface Specify from which DHCP-enabled interface a provided DNS server should be preferred.	
	DNS Proxy	When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.	
• IP 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 a new interface.	
	IPv4 DHCP	Enabled	Enable the DHCP client by checking this box.
		Fallback	The number of seconds for trying to obtain a DHCP lease.
		Current Lease	For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.
	IPv4	Address	Provide the IP address of this Managed Switch in dotted decimal notation.
		Mask Length	The IPv4 network mask, in number of bits (<i>prefix length</i>). Valid values are between 0 and 30 bits for a IPv4 address.
	IPv6	Address	Provide 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 (:).

		Mask Length	The IPv6 network mask, in number of bits (<i>prefix length</i>). Valid values are between 1 and 128 bits for a IPv6 address.
• 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 notation or 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 (<i>prefix length</i>).
	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.

Buttons

Add Interface : Click to add a new IP interface. A maximum of 128 interfaces is supported.

Add Route : Click to add a new IP route. A maximum of 32 routes is supported.

Apply : Click to apply changes.

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

4.2.3 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. The screen in [Figure 4-2-3](#) appears.

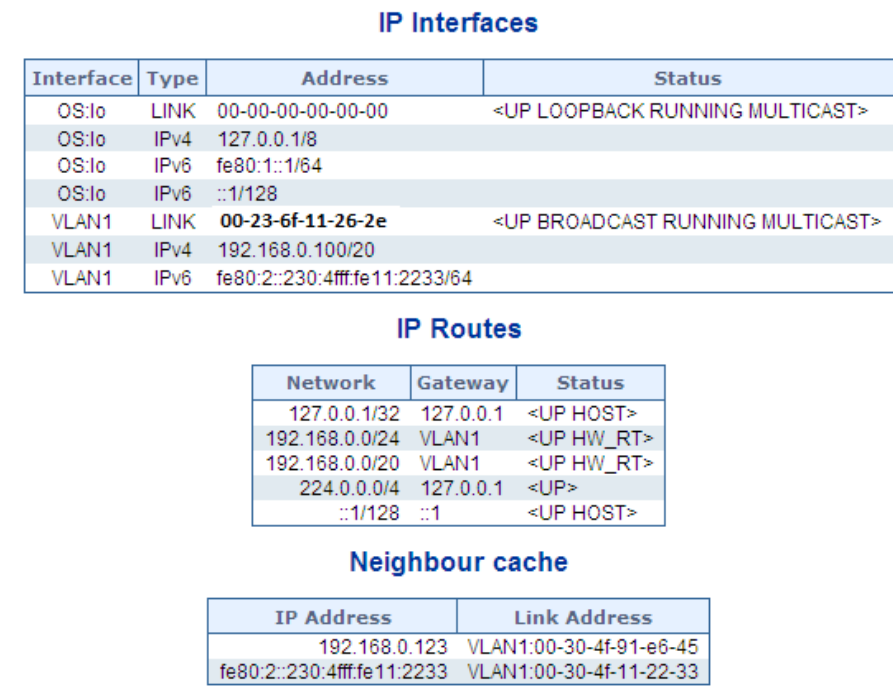




Figure 4-2-3: IPv6 Configuration Page Screenshot


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 exist.

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

: Click to renew IPv6 Auto Configuration. This button is only available if IPv6 Auto Configuration is enabled.

4.2.4 Users Configuration

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser. After setup is completed, please press “**Save**” button to take effect. Please login web interface with new user name and password, the screen in [Figure 4-2-4](#) appears.

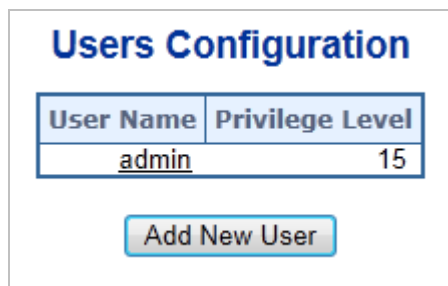


Figure 4-2-4: Users Configuration Page Screenshot

The page includes the following fields:

Object	Description
• User Name	The name identifying the 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. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, almost group privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

Add New User: Click to add a new user.

Add / Edit User

This page configures a user – add, edit or delete user.

Add User

User Settings	
User Name	Test
Password	••••
Password (again)	••••
Privilege Level	1

Save

Reset

Cancel

Figure 4-2-5: Add / Edit User Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">User Name	A string identifying 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.
<ul style="list-style-type: none">Password	The password of the user. The allowed string length is 0 to 32.
<ul style="list-style-type: none">Privilege Level	The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

Save

: Click to save changes.

Reset

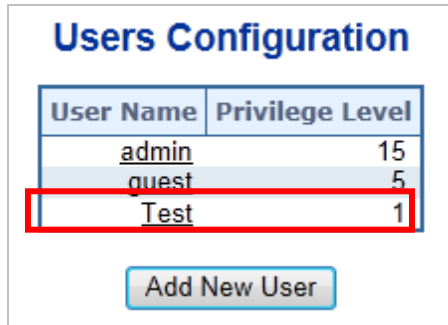
: Click to undo any changes made locally and revert to previously saved values.

Cancel

: Click to undo any changes made locally and return to the Users.

Delete User

: Delete the current user. This button is not available for new configurations (Add new user)



User Name	Privilege Level
admin	15
guest	5
Test	1

Add New User

Figure 4-2-6: User Configuration Page Screenshot



If you forget the new password after changing the default password, please press the **“Reset”** button on the front panel of the Managed Switch for over 10 seconds and then release it. The current setting including VLAN will be lost and the Managed Switch will restore to the default mode.

4.2.5 Privilege Levels

This page provides an overview of the privilege levels. After setup is completed, please press **“Save”** button to take effect. Please login web interface with new user name and password and the screen in [Figure 4-2-7](#) 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
DHCP_Client	5	10	5	10
Diagnostics	5	10	5	10
ERPS	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
MEP	5	10	5	10
Mirroring	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
POE	5	10	5	10
PoE_ping	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
Security	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
UPnP	5	10	5	10
VLAN_Translation	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10


Figure 4-2-7: Privilege Levels Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Group Name	<p>The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:</p> <ul style="list-style-type: none">■ 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.
<ul style="list-style-type: none">• Privilege Level	<p>Every group has an authorization Privilege level for the following sub groups:</p> <ul style="list-style-type: none">■ Configuration read-only■ Configuration/execute read-write■ Status/statistics read-only■ Status/statistics read-write (e.g. for clearing of statistics). <p>User Privilege should be same or greater than the authorization Privilege level to have the access to that group.</p>

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.2.6 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 transport layer. You can specify NTP Servers and set GMT Time zone. The NTP Configuration screen in [Figure 4-2-8](#) appears.

NTP Configuration	
Mode	Disabled
Server 1	pool.ntp.org
Server 2	europa.pool.ntp.org
Server 3	north-america.pool.ntp.org
Server 4	asia.pool.ntp.org
Server 5	oceania.pool.ntp.org

Apply Reset

Figure 4-2-8: NTP Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">Mode	Indicates the NTP mode operation. Possible modes are: <ul style="list-style-type: none">Enabled: Enable NTP mode operation. When NTP mode operation is enabled, the agent forwards NTP messages between the clients and the server when they are not on the same subnet domain.Disabled: Disable NTP mode operation.
<ul style="list-style-type: none">Timezone	Allow select the time zone according to current location of switch.
<ul style="list-style-type: none">Server #	Provide 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 (:). 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'.

Buttons

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.2.7 Time Configuration

Configure Time Zone on this Page. 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 keep the same time, so time zones tend to follow the boundaries of countries and their subdivisions. The Time Zone Configuration screen in Figure 4-2-9 appears

Time Zone Configuration

Time Zone Configuration	
Time Zone	None
Acronym	(0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled

Start Time Settings	
Month	Jan
Date	1
Year	2000
Hours	0
Minutes	0
End Time Settings	
Month	Jan
Date	1
Year	2000
Hours	0
Minutes	0
Offset Settings	
Offset	1 (1 - 1440) Minutes

ApplyReset

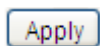
Figure 4-2-9: Time Configuration Page Screenshot

The Page includes the following fields:

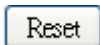
Object	Description
--------	-------------

• Time Zone	Lists various Time Zones world wide. Select appropriate Time Zone from the drop down and click Save to set.
• Acronym	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 characters)
• 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 to add during Daylight Saving Time. (Range: 1 to 1440)

Buttons



: Click to apply changes.

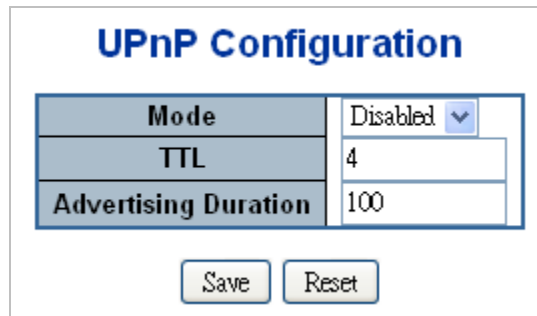


: Click to undo any changes made locally and revert to previously saved values.

4.2.8 UPnP

Configure UPnP on this page.

UPnP is an acronym for **Universal Plug and Play**. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. The UPnP Configuration screen in [Figure 4-2-10](#) appears.




The screenshot shows a web interface titled "UPnP Configuration". It contains three input fields: "Mode" with a dropdown menu set to "Disabled", "TTL" with a text input set to "4", and "Advertising Duration" with a text input set to "100". Below these fields are two buttons: "Save" and "Reset".


Figure 4-2-10: UPnP Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Mode 	<p>Indicates the UPnP operation mode. Possible modes are:</p> <ul style="list-style-type: none"> ■ Enabled: Enable UPnP mode operation. ■ Disabled: Disable UPnP mode operation. <p>When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.</p>
<ul style="list-style-type: none"> TTL 	<p>The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range of 1 to 255.</p>
<ul style="list-style-type: none"> Advertising Duration 	<p>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.</p>

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

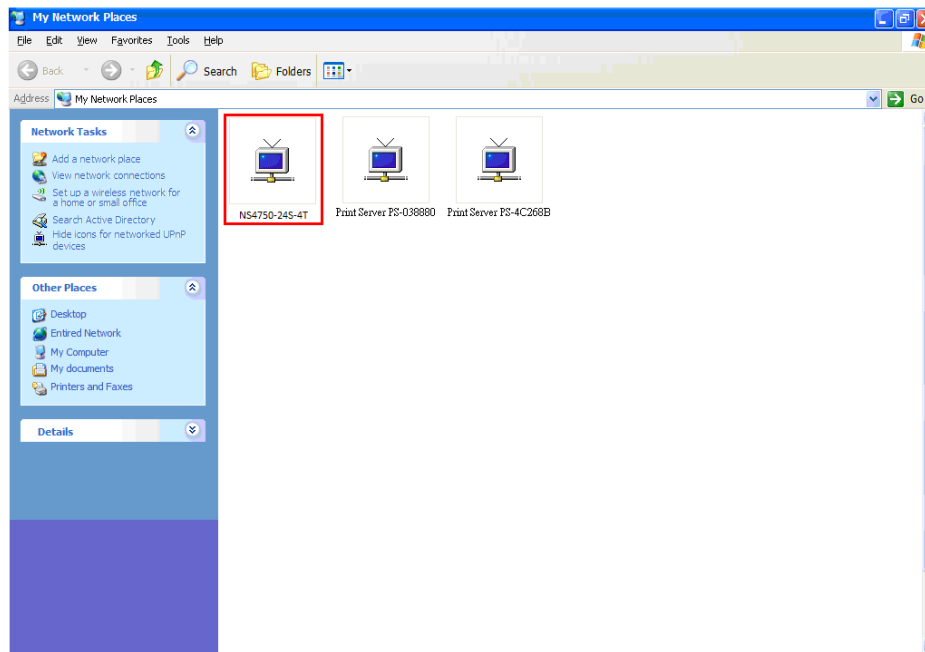


Figure 4-2-11: UPnP Devices shows on Windows My Network Places

4.2.9 DHCP Relay

Configure DHCP Relay on this page. **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)
- Remote ID (option2).

The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on.

The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes representing the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equals 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agent's MAC address. The DHCP Relay Configuration screen in [Figure 4-2-12](#) appears.

DHCP Relay Configuration

Relay Mode	Disable ▼
Relay Server	0.0.0.0
Relay Information Mode	Disable ▼
Relay Information Policy	Replace ▼

Figure 4-2-12: DHCP Relay Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Relay Mode 	<p>Indicates the DHCP relay mode operation. Possible modes are:</p> <ul style="list-style-type: none"> ■ Enabled: Enable DHCP relay mode operation. 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. ■ Disabled: Disable DHCP relay mode operation.
<ul style="list-style-type: none"> Relay Server 	<p>Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.</p>
<ul style="list-style-type: none"> Relay Information Mode 	<p>Indicates the DHCP relay information mode option operation. Possible modes are:</p> <ul style="list-style-type: none"> ■ Enabled: Enable DHCP relay information mode operation. When enable DHCP relay information mode operation, the agent insert specific information (option82) into a DHCP message when forwarding to DHCP server and remove it from a DHCP message when transferring to DHCP client. It only works under DHCP relay operation mode enabled. ■ Disabled: Disable DHCP relay information mode operation.
<ul style="list-style-type: none"> Relay Information Policy 	<p>Indicates the DHCP relay information option policy. When enable DHCP relay information mode operation, if agent receive a DHCP message that already contains relay agent information. It will enforce the policy. And it only works under DHCP relay information operation mode enabled. Possible policies are:</p> <ul style="list-style-type: none"> ■ 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

	<p>that already contains it.</p> <ul style="list-style-type: none"> ■ Drop: Drop the package when receiving a DHCP message that already contains relay information.
--	---

Buttons

Save: Click to save changes.

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

4.2.10 DHCP Relay Statistics

This page provides statistics for DHCP relay. The DHCP Relay Statistics screen in [Figure 4-2-13](#) appears.

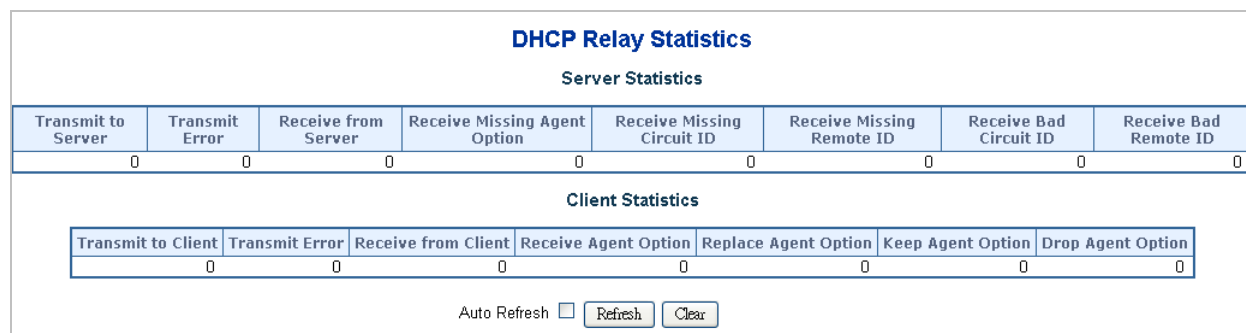


Figure 4-2-12: DHCP Relay Statistics Page Screenshot

The page includes the following fields:

Server Statistics

Object	Description
• Transmit to Server	The number of packets that are relayed from client to server.
• Transmit Error	The number of packets that resulted in errors while being sent to clients.
• Receive form Server	The number of packets received from server.
• Receive Missing Agent Option	The number of packets received without agent information options.
• Receive Missing Circuit ID	The number of packets received with the Circuit ID option missing.
• Receive Missing Remote ID	The number of packets received with the Remote ID option missing.

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

Client Statistics

Object	Description
• Transmit to Client	The number of relayed packets from server to client.
• Transmit Error	The number of packets that resulted in error while being sent to servers.
• Receive form Client	The number of received packets from server.
• Receive Agent Option	The number of received packets with relay agent information option.
• Replace Agent Option	The number of packets which were replaced with relay agent information option.
• Keep Agent Optin	The number of packets whose relay agent information was retained.
• Drop Agent Option	The number of packets that were dropped which were received with relay agent information.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

: Clear all statistics.

4.2.11 CPU Load

This page displays the CPU load, using a **SVG graph**.

The load is measured as average over the last 100ms, 1sec and 10 seconds intervals. The last 120 samles are graphed, and the last numbers are displayed as text as well.

In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG. The CPU Load screen in [Figure 4-2-14](#) appears.

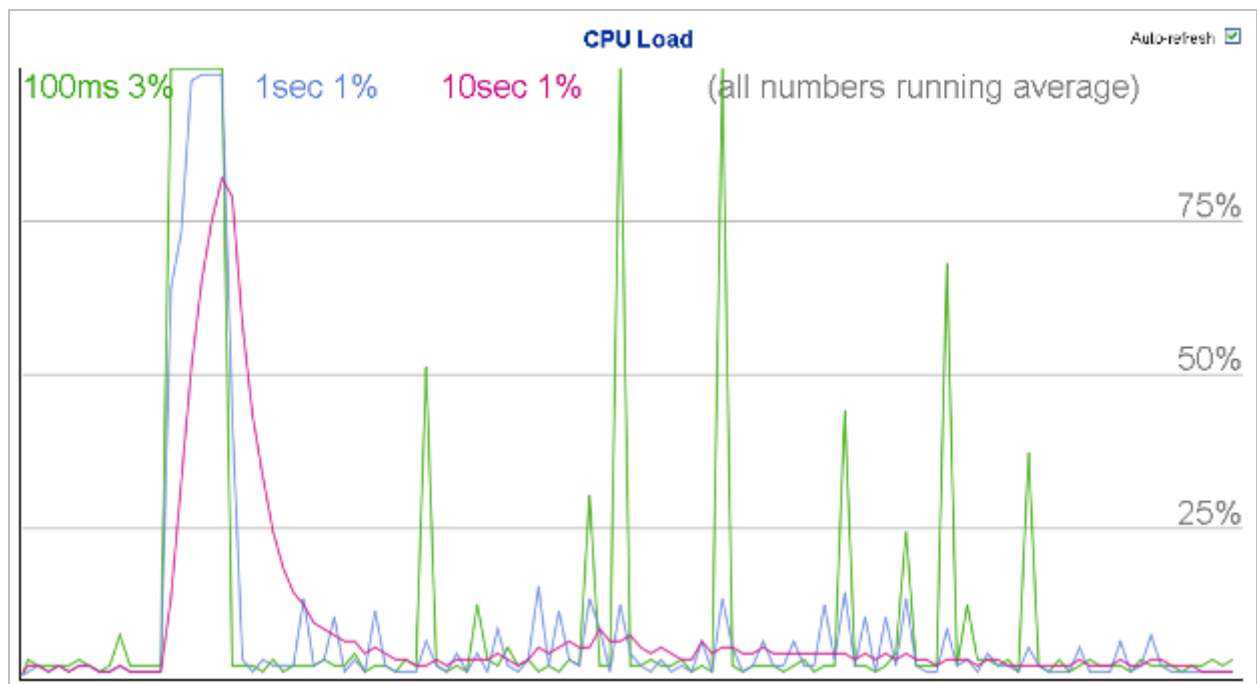


Figure 4-2-13: CPU Load Page Screenshot

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.



If your browser cannot display anything on this page, please download Adobe SVG tool and install it in your computer.

4.2.12 System Log

The switch system log information is provided here. The System Log screen in [Figure 4-2-15](#) appears.

System Log Information

Auto-refresh ☒

Refresh

Clear

Hide

Download

|<<

<<

>>

>>|

Level

All

Clear Level

All

The total number of entries is 0 for the given level.

Start from ID 1 with 20 entries per page.

ID

Level

Time

Message

No system log entries

Figure 4-2-15: System Log Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">ID	The ID (>= 1) of the system log entry.
<ul style="list-style-type: none">Level	The level of the system log entry. The following level types are supported: <ul style="list-style-type: none">■ Info: Information level of the system log.■ Warning: Warning level of the system log.■ Error: Error level of the system log.■ All: All levels.
<ul style="list-style-type: none">Time	The time of the system log entry.
<ul style="list-style-type: none">Message	The message of the system log entry.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to updates the system log entries, starting from the current entry ID.

: Flushes the selected log entries.

Hide: Hide system log according to entry page. As default System Log Information shows 20 entries for one page. Hide button can hide the system log entry that has been over one page.

Download: Click this button could download system log with CSV format file.

<<: Updates the system log entries, starting from the first available entry ID.

<<: Updates the system log entries, ending at the last entry currently displayed.

>>: Updates the system log entries, starting from the last entry currently displayed.

>>|: Updates the system log entries, ending at the last available entry ID.

4.2.13 Detailed Log

The switch system detailed log information is provided here. The Detailed Log screen in [Figure 4-2-16](#) appears.

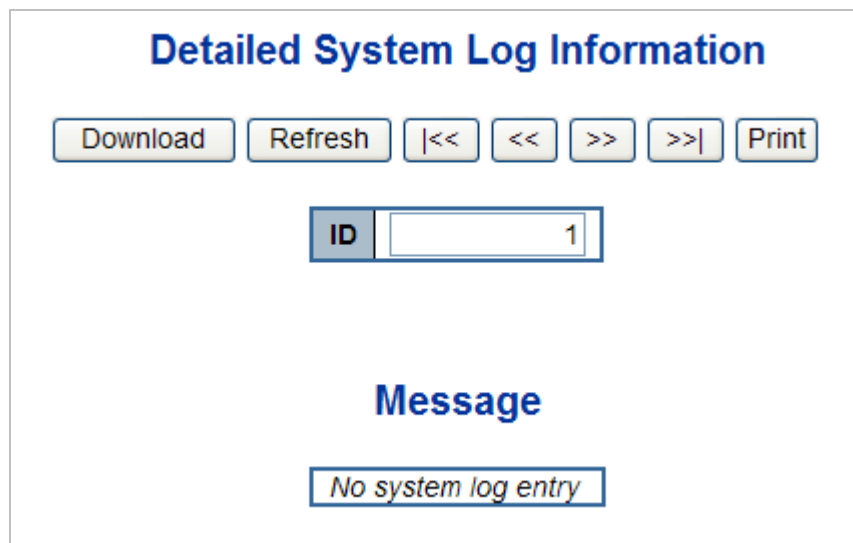


Figure 4-2-16: Detailed Log Page Screenshot

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

Download: Click this button could download system log with CSV format file.

- Refresh** : Updates the system log entry to the current entry ID.
- <<** : Updates the system log entry to the first available entry ID
- <<** : Updates the system log entry to the previous available entry ID.
- >>** : Updates the system log entry to the next available entry ID.
- >>|** : Updates the system log entry to the last available entry ID.
- Print** : Click this button to print out system log.

4.2.14 Remote Syslog

Configure remote syslog on this page. The Remote Syslog screen in [Figure 4-2-17](#) appears.

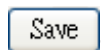
Figure 4-2-17: Remote Syslog Page Screenshot

The page includes the following fields:

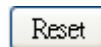
Object	Description
<ul style="list-style-type: none"> Server Mode 	<p>Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are:</p> <ul style="list-style-type: none"> ■ Enabled: Enable server mode operation. ■ Disabled: Disable server mode operation.
<ul style="list-style-type: none"> Server Address 	<p>Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.</p>
<ul style="list-style-type: none"> Syslog Level 	<p>Indicates what kind of message will send to syslog server. Possible modes are:</p> <ul style="list-style-type: none"> ■ Info: Send information, warnings and errors.

	<ul style="list-style-type: none">■ Warning: Send warnings and errors.■ Error: Send errors.
--	--

Buttons



: Click to save changes.



: Click to undo any changes made locally and revert to previously saved values.

4.2.15 SMTP Configuration

Configure SMTP Configuration on this page. The SMTP Configuration screen in [Figure 4-2-18](#) appears.

SMTP Configuration

SMTP Mode	<input type="checkbox"/> Enable
SMTP Server	<input type="text" value="Interlogix.com"/> (<128 Digits) <input type="button" value="test"/>
SMTP Port	<input type="text" value="25"/> (1 ~ 65535)
SMTP Authentication	<input type="checkbox"/> Enable
Authentication User Name	<input type="text" value="1234"/> (< 64 Digits)
Authentication Password	<input type="password" value="••••"/> (< 21 Digits)
E-mail From	<input type="text" value="abcd@Interlogix.com"/> (< 128 Digits)
E-mail Subject	<input type="text" value="Interlogix"/> (< 64 Digits)
E-mail 1 To	<input type="text" value="abcd@Interlogix.com"/> (< 128 Digits)
E-mail 2 To	<input type="text" value="abcd@Interlogix.com"/> (< 128 Digits)

Figure 4-2-18: SMTP Configuration Page Screenshot


The page includes the following fields:


Object	Description
• SMTP Mode	Enabled It is for you to enable SMTP mode function. This mode offers you to configure SMTP server and SMTP account information, system will refer it to send an E-mail for alarm noticing
• SMTP Server	It is for you to set up a specify SMTP server DNS name or IP address. If it is inputted a DNS name, please remember to input DNS server IP address at IP configuration page.
• SMTP Port	It is for you to input the SMTP server port number. As default is "25".
• SMTP Authentication	Enabled As usual SMTP server is denied to relay a mail from a different domain, so you have to enable this option and input your mail account and password for SMTP sever authorizing to forward a mail from different domain. For example, you want a SMTP server which located on mail.123.com send a mail to mail.456.net.com. If you want to send the mail to a SMTP server which located on the same domain or the same SMTP server, you don't have to enable SMTP authentication.
• Authentication User Name	It is for you to input your mail account name.

• Authentication Password	It is for you to input your mail account password.
• E-mail From	It is for you to input who send this mail.
• E-mail Subject	It is for you to input mail subject.
• E-mail 1 To	It is for you to input recipient mail address.
• E-mail 2 To	It is for you to input secondary recipient mail address.

Buttons

: Click to test SMTP server address.

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.2.16 Digital Input/Output

Digital Input allows user can log external device (such as industrial cooler) dead or alive or something else, system will logs a user customize message into system log, syslog, issue SNMP trap or issue an alarm E-mail.

Digital Output allows user to monitor the switch port and power , and let system issue a high or low signal to an external device (such as alarm) when the monitor port or power has been failed. The Configuration screen in [Figure 4-2-19](#) appears.

Digital Input/Output Control Configuration

Digital Input 0				Digital Input 1			
Enable	<input type="checkbox"/> Enable			Enable	<input type="checkbox"/> Enable		
Condition	High to Low ▼			Condition	High to Low ▼		
Event Description	<div style="border: 1px solid #ccc; height: 20px;"></div>			Event Description	<div style="border: 1px solid #ccc; height: 20px;"></div>		
Event	<input type="checkbox"/> System Log <input type="checkbox"/> SNMP Trap			Event	<input type="checkbox"/> System Log <input type="checkbox"/> SNMP Trap		

Digital Output 0				Digital Output 1			
Enable	<input type="checkbox"/> Enable			Enable	<input type="checkbox"/> Enable		
Event	<input type="checkbox"/> Power Fail <input type="checkbox"/> Port Fail <input type="checkbox"/> DI 0 <input type="checkbox"/> DI 1			Event	<input type="checkbox"/> Power Fail <input type="checkbox"/> Port Fail <input type="checkbox"/> DI 0 <input type="checkbox"/> DI 1		
Condition	High to Low ▼			Condition	High to Low ▼		
Power Alarm	<input type="checkbox"/> DC 1 <input type="checkbox"/> DC 2 <input type="checkbox"/> AC Power			Power Alarm	<input type="checkbox"/> DC 1 <input type="checkbox"/> DC 2 <input type="checkbox"/> AC Power		
Port Fail Alarm	<div style="display: flex; justify-content: space-between;"> 1 2 3 4 5 6 7 8 </div> <div style="display: flex; justify-content: space-between;"> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> </div> <div style="display: flex; justify-content: space-between;"> 9 10 </div> <div style="display: flex; justify-content: space-between;"> <input type="checkbox"/> <input type="checkbox"/> </div>			<div style="display: flex; justify-content: space-between;"> 1 2 3 4 5 6 7 8 </div> <div style="display: flex; justify-content: space-between;"> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> </div> <div style="display: flex; justify-content: space-between;"> 9 10 </div> <div style="display: flex; justify-content: space-between;"> <input type="checkbox"/> <input type="checkbox"/> </div>			

Figure 4-2-19 Windows File Selection Menu Popup

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Enable 	<p>Checks the Enable checkbox will enable Digital Input / output function.</p> <p>Unchecks the Enable checkbox will disable Digital input / output function.</p>
<ul style="list-style-type: none"> Condition 	<p>As Digital Input:</p> <p>Allows user selecting to High to Low or Low to High. This is means a signal received by system is from High to Low or From Low to High, it will trigger an action that logs a customize message or issue the message from the switch.</p> <p>As Digital Output:</p> <p>Allows user selecting to High to Low or Low to High. This is means that when the switch has power failed or port failed then system will issue a High or Low signal to an external device (such as an alarm).</p>
<ul style="list-style-type: none"> Event Description 	<p>Allows user setting a customize message for Digital Input function alarming.</p>
<ul style="list-style-type: none"> Event 	<p>As Digital Input:</p> <p>Allows user to record alarm message to System log, syslog or issues out via SNMP Trap or SMTP.</p> <p>As default SNMP Trap and SMTP are disabled, please enable them first if you want to issue alarm message via them.</p>

	As Digital Output: Allows user to monitor and alarm from port fail, power fail, Digital Input 0 (DI 0) and Digital Input 1(DI 1) which means if Digital Output has detected these event then Digital Output would be triggered according to the setting of Condition.
• Power Alarm	Allows user to choose which power module want to be monitored.
• Port Alarm	Allows user to choose which port want to be monitored.

Buttons

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.2.17 Faulty Alarm

The Faulty Relay Alarm function provides the Power Failure and Port Link Down/Broken detection. With both power input 1 and power input 2 installed and the check boxes of power 1/power 2 ticked, the FAULTY LED indicator will then be possible to light up when any one of the power failures occurs. As for the Port Link Down/Broken detection, the FAULT LED indicator will light up when the port failure occurs; certainly the check box beside the port must be ticked first. Please refer to the segment of **Wiring the Fault Alarm Contact** for the failure detection. The Configuration screen in [Figure 4-2-20](#) appears.

Fault Alarm Control Configuration

Enable

Record

Action

Power Alarm

Port Alarm

☐ Enable

☐ System Log ☐ SNMP Trap

☐ Port Fail ☐ Power Fail

☐ DC 1 ☐ DC 2 ☐ AC Power

12345678

☐☐☐☐☐☐☐☐

910

☐☐

Save

Reset

Figure 4-2-20 Windows File Selection Menu Popup

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">Enable	Allows user to enable Fault Alarm function.
<ul style="list-style-type: none">Record	Allows user to record alarm message to System log, syslog or issues out via SNMP Trap or SMTP. As default SNMP Trap and SMTP are disabled, please enable them first if you want to issue alarm message via them.
<ul style="list-style-type: none">Action	Allows user to monitor and alarm from port fail or power fail.
<ul style="list-style-type: none">Power Alarm	Allows user to choose which power module want to be monitored.
<ul style="list-style-type: none">Port Alarm	Allows user to choose which port want to be monitored.

Buttons



: Click to save changes.



: Click to undo any changes made locally and revert to previously saved values.

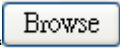

4.2.18 Web Firmware Upgrade

This page facilitates an update of the firmware controlling the **Managed Switch**. The Web Firmware Upgrade screen in [Figure 4-2-21](#) appears.



Figure 4-2-21: Web Firmware Upgrade Page Screenshot

To open **Firmware Upgrade** screen perform the following:

1. Click **System** -> Web **Firmware Upgrade**.
2. The Firmware Upgrade screen is displayed as in [Figure 4-2-21](#).
3. Click the  "button of the main page, the system would pop up the file selection menu to choose firmware.
4. Select on the firmware and then click  ". The **Software Upload Progress** would show the file upload status.
5. Once the software be loaded to the system successfully, the following screen appears. The system will load the new software after reboot.

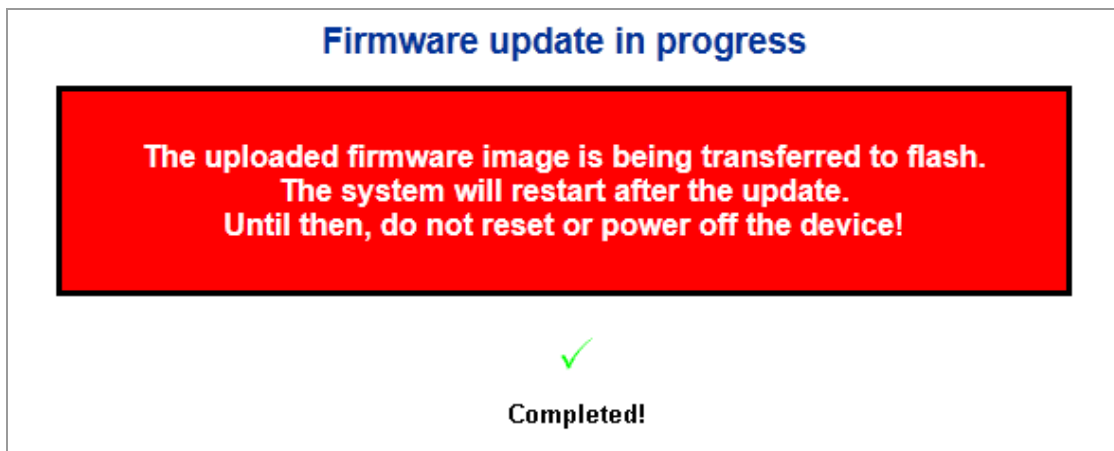


Figure 4-2-21: Software successfully Loaded Notice Screen



DO NOT Power OFF the **Managed Switch** until the update progress is complete.



Do not quit the Firmware Upgrade page without pressing the “**OK**” button after the image is loaded. Or the system won’t apply the new firmware. User has to repeat the firmware upgrade processes again.

4.2.19 TFTP Firmware Upgrade

The **Firmware Upgrade** page provides the functions to allow a user to update the **Managed Switch** firmware from the TFTP server in the network. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server. The TFTP Firmware Upgrade screen in [Figure 4-2-23](#) appears.

TFTP Firmware Upgrade

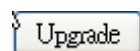
TFTP Server IP	<input type="text"/>
Firmware File Name	<input type="text"/>

Figure 4-2-23: TFTP Firmware Update Page Screenshot

The page includes the following fields:

Object	Description
• TFTP Server IP	Fill in your TFTP server IP address.
• Firmware File Name	The name of firmware image. (Maximum length : 24 characters)

Buttons



: Click to upgrade firmware.



DO NOT Power OFF the **Managed Switch** until the update progress is complete.

Do not quit the Firmware Upgrade page without pressing the “**OK**” button after the image is loaded. Or the system won’t apply the new firmware. User has to repeat the firmware upgrade processes again.

4.2.20 Save Startup Config

This function allows save the current configuration, thereby ensuring that the current active configuration can be used at the next reboot screen in [Figure 4-2-24](#) appears. After saving the configuration, the screen [Figure 4-2-25](#) will appear.

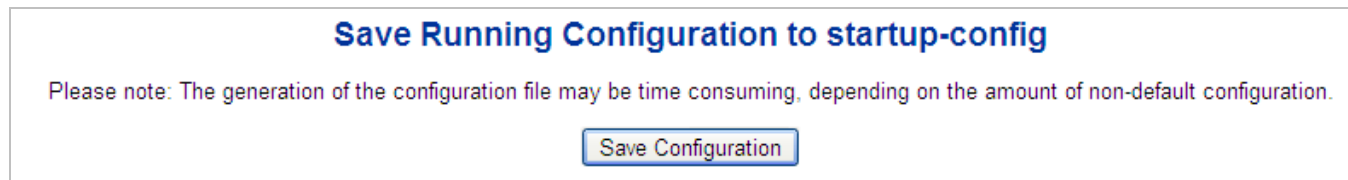


Figure 4-2-24: Configuration Save Page Screenshot

Save Running Configuration to startup-config

startup-config saved successfully.

Figure 4-2-25: Finish Saving Page Screenshot

4.2.21 Configuration Download

The 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.

Configuration Download page allows the download the running-config, startup-config and default-config on the switch. Please refer to the Figure 4-2-26 shown below.

Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
<input type="radio"/> running-config
<input type="radio"/> default-config
<input type="radio"/> startup-config

Download Configuration

Figure 4-2-26: Configuration Download Page Screenshot

4.2.22

Configuration Upload page allows the upload the running-config and startup-config on the switch. Please refer to the Figure 4-2-27 shown below:

Upload Configuration

File To Upload

Browse...

Destination File

File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> startup-config	
<input type="radio"/> Create new file	<div></div>

Upload Configuration

Figure 4-2-27: Configuration Upload Page Screenshot

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. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

4.2.23 Configuration Activate

Configuration Activate page allows to activate the startup-config and default-config files present on the switch. Please refer to the Figure 4-2-28 shown below.

Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.


Please note: The activated configuration file will not be saved to startup-config automatically.

File Name
<input type="radio"/> default-config
<input type="radio"/> startup-config

Activate Configuration

Figure 4-2-28: Configuration Activate Page Screenshot

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 . This will initiate the process of completely replacing the existing configuration with that of the selected file.

4.2.24 Configuration Delete

Configuration Delete page allows to delete the startup-config and default-config files which stored in FLASH. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration. Please refer to the Figure 4-2-29 shown below.

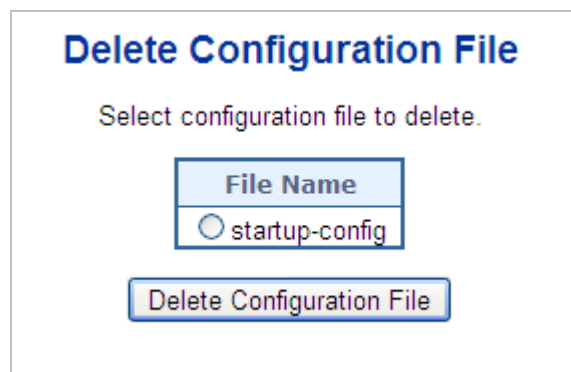


Figure 4-2-29: Configuration Delete Page Screenshot

4.2.25 Image Select

This Page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image. The web Page displays two tables with information about the active and alternate firmware images. The Image Select screen in Figure 4-2-30 appears.



In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.



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

Software Image Selection

Active Image	
Image	managed
Version	v1.5b140618
Date	2014-06-18T19:00:10+0800

Alternate Image	
Image	managed.bk
Version	v1.5b140611
Date	2014-06-11T18:06:17+0800

Figure 4-2-30: Software Image Selection Page Screenshot

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 where the firmware was produced.

Button

: Click to choose Alternate Image as Activate Image.

4.2.26 Factory Default

You can reset the configuration of the stack switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary. The Factory Default screen in [Figure 4-2-31](#) appears.

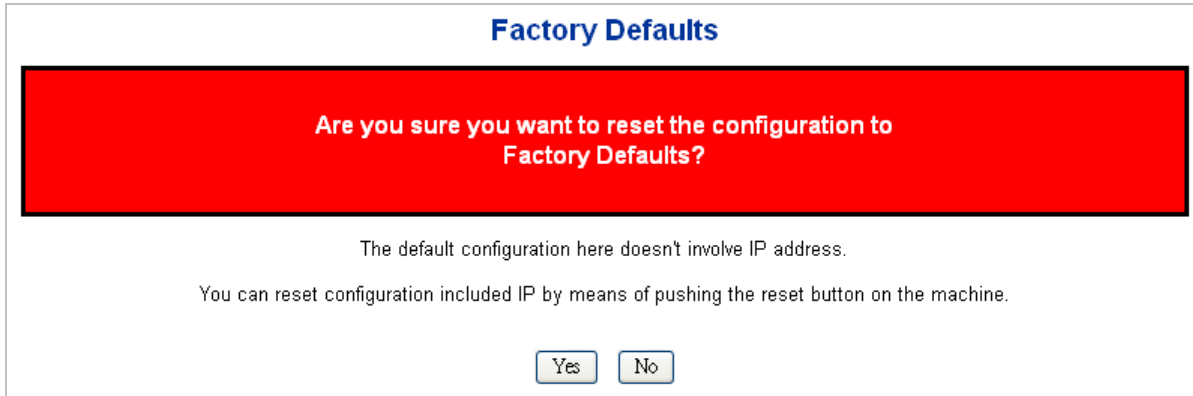


Figure 4-2-31: Factory Default Page Screenshot

Buttons



: Click to reset the configuration to Factory Defaults.



: Click to return to the Port State Page without resetting the configuration.



To reset the Managed Switch to the Factory default setting, you can also press the hardware reset button at the front panel about 10 seconds. After the device be rebooted. You can login the management WEB interface within the same subnet of 192.168.0.xx.

4.2.27 System Reboot

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user will re-access the WEB interface about 60 seconds later, the System Reboot screen in [Figure 4-2-32](#) appears.



Figure 4-2-32: System Reboot Page Screenshot

Buttons



: Click to reboot the system.



: Click to return to the web main page without reboot the system.

4.3 Simple Network Management Protocol

4.3.1 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 enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network consists of three key components: Network management stations (NMSs), SNMP agents, Management information base (MIB) and network-management protocol :

- **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)** : A 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. A 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 Accesses** Configure SNMPv3 accesses table on this page.

4.3.2 SNMP System Configuration

Configure SNMP on this page. The SNMP System Configuration screen in [Figure 4-3-1](#) appears.

SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Figure 4-3-1: SNMP System Configuration Page Screenshot

The SNMP System Configuration page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Mode 	<p>Indicates the SNMP mode operation. Possible modes are:</p> <ul style="list-style-type: none"> ■ Enabled: Enable SNMP mode operation. ■ Disabled: Disable SNMP mode operation.
<ul style="list-style-type: none"> Version 	<p>Indicates the SNMP supported version. Possible versions are:</p> <ul style="list-style-type: none"> ■ SNMP v1: Set SNMP supported version 1. ■ SNMP v2c: Set SNMP supported version 2c. ■ SNMP v3: Set SNMP supported version 3.
<ul style="list-style-type: none"> Read Community 	<p>Indicates the community read access string to permit access to SNMP agent.</p> <p>The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.</p> <p>The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a</p>

	SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
<ul style="list-style-type: none"> • Write Community 	<p>Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.</p> <p>The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.</p>
<ul style="list-style-type: none"> • Engine ID 	Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

4.3.3 TRAP Configuration

Configure SNMP trap on this page. The SNMP trap configuration screen in [Figure 4-3-2](#) appears.

SNMP Trap Configuration

Trap Config Name	<input style="width: 90%;" type="text"/>
Trap Mode	Disabled ▼
Trap Version	SNMP v2c ▼
Trap Community	Public
Trap Destination Address	<input style="width: 90%;" type="text"/>
Trap Destination Port	162
Trap Inform Mode	Disabled ▼
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled ▼
Trap Security Engine ID	<input style="width: 90%;" type="text"/>
Trap Security Name	None ▼

SNMP Trap Event

System	<input type="checkbox"/> * <input type="checkbox"/> Warm Start <input type="checkbox"/> Cold Start
Interface	Link up <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches
	* Link down <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches
	LLDP <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches
AAA	<input type="checkbox"/> * <input type="checkbox"/> Authentication Fail
Switch	<input type="checkbox"/> * <input type="checkbox"/> STP <input type="checkbox"/> RMON

Figure 4-3-2: SNMP Trap Configuration Page Screenshot

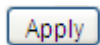
The Page includes the following fields:

Object	Description
• Trap Config	Indicates which trap Configuration's name for configuring. 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. Possible modes are: <ul style="list-style-type: none"> ■ Enabled: Enable SNMP trap mode operation. ■ Disabled: Disable SNMP trap mode operation.
• Trap Version	Indicates the SNMP trap supported version. Possible versions are: <ul style="list-style-type: none"> ■ SNMP v1: Set SNMP trap supported version 1. ■ SNMP v2c: Set SNMP trap supported version 2c. ■ SNMP v3: Set SNMP trap supported version 3.
• Trap Community	Indicates the community access string when send SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

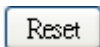
<ul style="list-style-type: none"> • Trap Destination Address 	<p>Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.</p> <p>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'.</p>
<ul style="list-style-type: none"> • Trap Destination Port 	<p>Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.</p>
<ul style="list-style-type: none"> • Trap Inform Mode 	<p>Indicates the SNMP trap inform mode operation. Possible modes are:</p> <ul style="list-style-type: none"> ■ Enabled: Enable SNMP trap authentication failure. ■ Disabled: Disable SNMP trap authentication failure.
<ul style="list-style-type: none"> • Trap Inform Timeout (seconds) 	<p>Indicates the SNMP trap inform timeout.</p> <p>The allowed range is 0 to 2147.</p>
<ul style="list-style-type: none"> • Trap Inform Retry Times 	<p>Indicates the SNMP trap inform retry times.</p> <p>The allowed range is 0 to 255.</p>
<ul style="list-style-type: none"> • Trap Probe Security Engine ID 	<p>Indicates the SNMPv3 trap probe security engine ID mode of operation. Possible values are:</p> <ul style="list-style-type: none"> ■ Enabled: Enable SNMP trap probe security engine ID mode of operation. ■ Disabled: Disable SNMP trap probe security engine ID mode of operation.
<ul style="list-style-type: none"> • Trap Security Engine ID 	<p>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.</p>
<ul style="list-style-type: none"> • Trap Security Name 	<p>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.</p>
<ul style="list-style-type: none"> • System 	<p>Enable/disable that the Interface group's traps. Possible traps are:</p> <ul style="list-style-type: none"> ■ Warm start: Enable/disable Warm Start trap. ■ Cold start: Enable/disable Cold Start trap.

<ul style="list-style-type: none"> • Interface 	<p>Indicates that the Interface group's traps. Possible traps are:</p> <ul style="list-style-type: none"> ■ Link Up: Enable/disable Link up trap. ■ Link Down: Enable/disable Link down trap. ■ LLDP: Enable/disable LLDP trap.
<ul style="list-style-type: none"> • AAA 	<p>Indicates that the AAA group's traps. Possible traps are:</p> <p>Authentication Fail : Enable/disable SNMP trap authentication failure trap.</p>
<ul style="list-style-type: none"> • Switch 	<p>Indicates that the Switch group's traps. Possible traps are:</p> <ul style="list-style-type: none"> ■ STP: Enable/disable STP trap. ■ RMON: Enable/disable RMON trap.

Buttons



: Click to apply changes



: Click to undo any changes made locally and revert to previously saved values.

4.3.4 SNMP System Information

The switch system information is provided here. The SNMP System Information screen in [Figure 4-3-3](#) appears.

System Information Configuration

System Contact	
System Name	NS4750-24S-4T-4X
System Location	

Apply

Reset

Figure 4-3-3: System Information Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
<ul style="list-style-type: none">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.
<ul style="list-style-type: none">System Location	The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Buttons

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.3.5 SNMPv3 Configuration

4.3.5.1 SNMPv3 Communities

Configure SNMPv3 communities table on this page. The entry index key is Community. The SNMPv3 Communities screen in [Figure 4-3-4](#) appears.



Figure 4-3-4: SNMPv3 Communities Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Delete	Check to delete the entry. It will be deleted during the next save.
<ul style="list-style-type: none">• Community	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.
<ul style="list-style-type: none">• Source IP	Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
<ul style="list-style-type: none">• Source Mask	Indicates the SNMP access source address mask.

Buttons

: Click to add a new community entry.

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.3.5.2 SNMPv3 Users

Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name. The SNMPv3 Users screen in Figure 4-3-5 appears.

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Figure 4-3-5: SNMPv3 Users Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Delete	Check to delete the entry. It will be deleted during the next save.
• Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
• User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• Security Level	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none">■ NoAuth, NoPriv: None authentication and none privacy.■ Auth, NoPriv: Authentication and none privacy.■ Auth, Priv: Authentication and privacy. The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.
• Authentication	Indicates the authentication protocol that this entry should belong to. Possible

Protocol	<p>authentication protocol are:</p> <ul style="list-style-type: none"> ■ 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. ■ The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
• Authentication Password	A string identifying the authentication 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	<p>Indicates the privacy protocol that this entry should belong to. Possible privacy protocol are:</p> <ul style="list-style-type: none"> ■ None: None privacy protocol. ■ DES: An optional flag to indicate that this user using DES 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

Add New User

: Click to add a new user entry.

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.3.5.3 SNMPv3 Groups

Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name. The SNMPv3 Groups screen in [Figure 4-3-6](#) appears.

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group

Figure 4-3-6: SNMPv3 Groups Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Delete	Check to delete the entry. It will be deleted during the next save.
• Security Model	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none"> ■ 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 to add a new group entry.

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.3.5.4 SNMPv3 Views

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

in [Figure 4-3-6](#) appears.

SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included	.1

Add New Entry

Save

Reset

Figure 4-3-7: SNMPv3 Views Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">Delete	Check to delete the entry. It will be deleted during the next save.
<ul style="list-style-type: none">View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
<ul style="list-style-type: none">View Type	<p>Indicates the view type that this entry should belong to. Possible view type are:</p> <ul style="list-style-type: none">included: An optional flag to indicate that this view subtree should be included.excluded: An optional flag to indicate that this view subtree should be excluded. <p>General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.</p>
<ul style="list-style-type: none">OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*)

Buttons

Add New User

: Click to add a new view entry.

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.3.5.5 SNMPv3 Access

Configure SNMPv3 accesses table on this page. The entry index keys are Group Name, Security Model and Security Level. The SNMPv3 Access screen in [Figure 4-3-8](#) appears.

SNMPv3 Access Configuration


Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view ▼	None ▼
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view ▼	default_view ▼


Figure 4-3-8: SNMPv3 Accesses Configuration Page Screenshot


The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Delete	Check to delete the entry. It will be deleted during the next save.
<ul style="list-style-type: none">• 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.
<ul style="list-style-type: none">• Security Model	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none">■ any: Accepted any security model (v1 v2c usm).■ v1: Reserved for SNMPv1.■ v2c: Reserved for SNMPv2c.■ usm: User-based Security Model (USM)
<ul style="list-style-type: none">• Security Level	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none">■ NoAuth, NoPriv: None authentication and none privacy.■ Auth, NoPriv: Authentication and none privacy.■ Auth, Priv: Authentication and privacy.
<ul style="list-style-type: none">• 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.
<ul style="list-style-type: none">• 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 to add a new access entry.

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.4 Port Management

Use the Port Menu to display or configure the Managed Switch's 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 Information** Displays SFP information
- **Port Mirror** Sets the source and target ports for mirroring

4.4.1 Port Configuration

This page displays current port configurations. Ports can also be configured here. The Port Configuration screen in [Figure 4-4-1](#) appears.

Port Configuration										
Port	Port Description	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode	Power Control
			Current	Configured	Current Rx	Current Tx	Configured			
*			1Gfdx	<All> ▾			<input type="checkbox"/>	10056	<All> ▾	<All> ▾
1		●	Down	Auto ▾	×	×	<input type="checkbox"/>	10056	Discard ▾	Disabled ▾
2		●	Down	Auto ▾	×	×	<input type="checkbox"/>	10056	Discard ▾	Disabled ▾
3		●	Down	Auto ▾	×	×	<input type="checkbox"/>	10056	Discard ▾	Disabled ▾
4		●	Down	Auto ▾	×	×	<input type="checkbox"/>	10056	Discard ▾	Disabled ▾
5		●	Down	Auto ▾				10056		
6		●	Down	Auto ▾				10056		
7		●	Down	Auto ▾				10056		
8		●	Down	Auto ▾				10056		
9		●	Down	Auto ▾				10056		
10		●	Down	Auto ▾				10056		
11		●	Down	Auto ▾				10056		
12		●	Down	Auto ▾				10056		
13		●	Down	Auto ▾				10056		
14		●	Down	Auto ▾				10056		
15		●	Down	Auto ▾				10056		
16		●	Down	Auto ▾				10056		
17		●	Down	Auto ▾				10056		
18		●	Down	Auto ▾				10056		
19		●	Down	Auto ▾				10056		
20		●	Down	Auto ▾				10056		
21		●	Down	Auto ▾				10056		
22		●	Down	Auto ▾				10056		
23		●	Down	Auto ▾				10056		
24		●	Down	Auto ▾				10056		
25		●	Down	Auto Fiber (10G) ▾				10056		
26		●	Down	Auto Fiber (10G) ▾				10056		
27		●	Down	Auto Fiber (10G) ▾				10056		
28		●	Down	Auto Fiber (10G) ▾				10056		

Figure 4-4-1: Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Port	This is the logical port number for this row, * means selection all ports of Managed Switch.
• Port Description	This function provides input per port description and the available letters is 12.
• Link	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
• Current Link Speed	Provides the current link speed of the port.
• Configured Link Speed	<p>Select any available link speed for the given switch port. Draw the menu bar to select the mode.</p> <ul style="list-style-type: none"> ■ All - Setups whole ports with the same setting. ■ Disable – Shutdowns the port manually. ■ 10 HDX - Forces setting 10Mbps/Half-Duplex mode. ■ 10 FDX - Forces setting 10Mbps/Full-Duplex mode. ■ 100 HDX - Forces setting 100Mbps/Half-Duplex mode. ■ 100 FDX - Forces setting 100Mbps/Full-Duplex mode. ■ 1G FDX - Force setting 1000Mbps/Full-Duplex mode. ■ 10G FDX – Forces setting 10000Mbps/Full-duplex mode. ■ Auto Fiber (10G) – Setup 10G fiber port for negotiation automatically. ■ Auto Fiber - Setup 1G fiber port for negotiation automatically. ■ Auto - Setup Auto negotiation.
• Flow Control	<p>When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.</p> <p>When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.</p> <p>Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.</p>
• Maximum Frame Size	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes for TP port and 9000 bytes for Fiber port.
• Excessive Collision Mode	<p>Configure port transmit collision behavior.</p> <ul style="list-style-type: none"> ■ Discard: Discard frame after 16 collisions (default). ■ Restart: Restart back off algorithm after 16 collisions.

- **Power Control**

The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port.

- **Disabled**: All power savings mechanisms disabled.
 - **ActiPHY**: Link down power savings enabled.
 - **PerfectReach**: Link up power savings enabled.
 - **Enabled**: Both link up and link down power savings enabled.
-



When setting each port to run at 100M Full, 100M Half, 10M Full, and 10M Half-speed modes, the Auto-MDIX function will disable.

Buttons

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

Refresh

: Click to refresh the page. Any changes made locally will be undone.

4.4.2 Port Statistics Overview

This page provides an overview of general traffic statistics for all switch ports. The Port Statistics Overview screen in [Figure 4-4-2](#) appears.

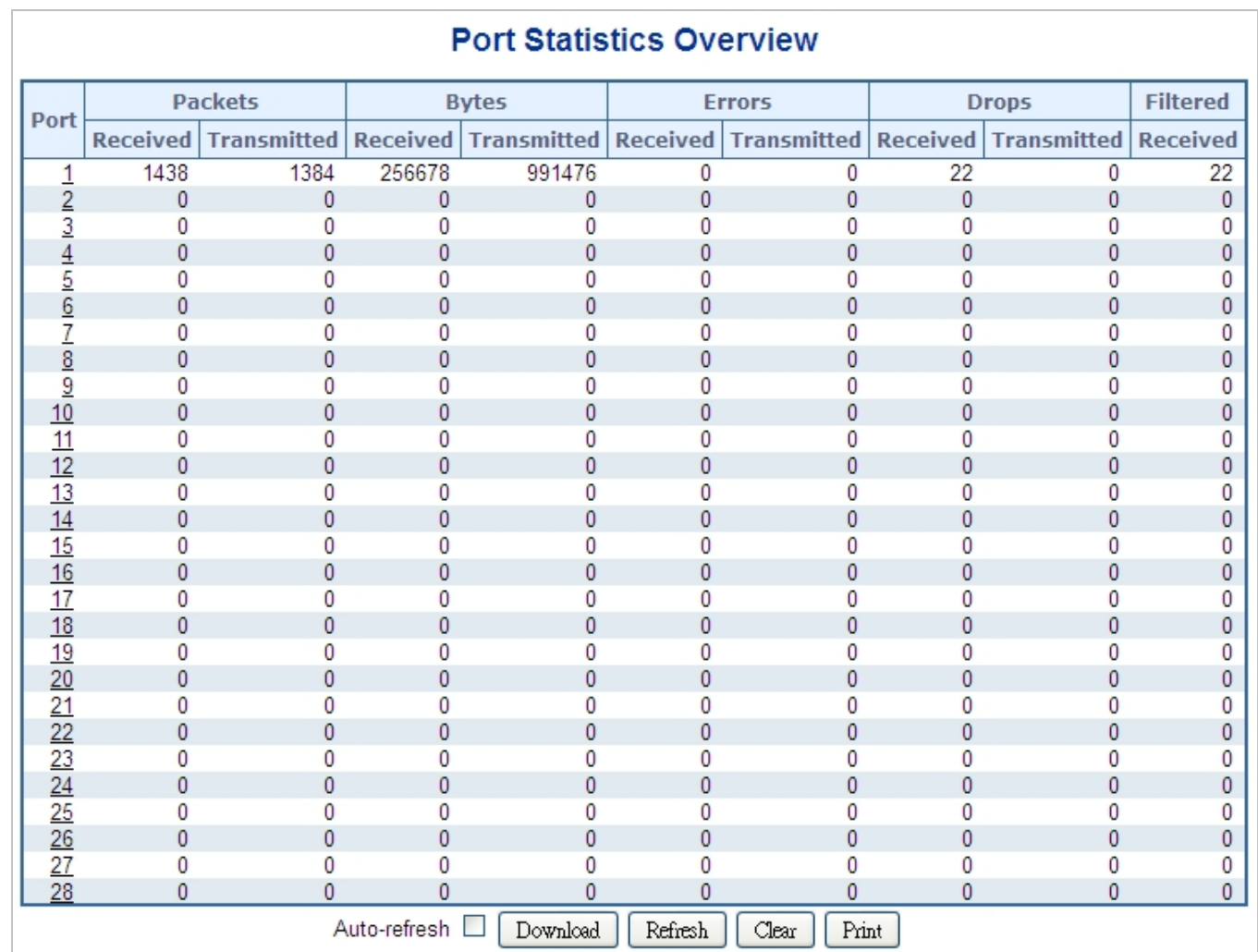


Figure 4-4-2: Port Statistics Overview Page Screenshot

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Auto-refresh ☐: Check this box to enable an automatic refresh of the page at regular intervals.

4.4.3 Detailed Port Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The selected port belongs to the currently selected stack unit, as reflected by the page header. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

The Detailed Port Statistics screen in [Figure 4-4-3](#) appears.

Detailed Port Statistics Port 1			
Port 1 <input type="button" value="Auto-refresh"/>		<input type="button" value="Refresh"/>	<input type="button" value="Clear"/>
Receive Total		Transmit Total	
Rx Packets	353	Tx Packets	408
Rx Octets	58126	Tx Octets	401574
Rx Unicast	352	Tx Unicast	408
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	1	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	258	Tx 64 Bytes	28
Rx 65-127 Bytes	12	Tx 65-127 Bytes	8
Rx 128-255 Bytes	0	Tx 128-255 Bytes	48
Rx 256-511 Bytes	68	Tx 256-511 Bytes	66
Rx 512-1023 Bytes	15	Tx 512-1023 Bytes	26
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	232
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	353	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	408
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Figure 4-4-3: Detailed Port Statistics Port 1 Page Screenshot

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 have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The numeric of received and transmitted packet is per input and output queue.

Receive Error Counters

Object	Description
• Rx Drops	The numeric of frames is 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 frame received with valid CRC.
• Rx Oversize	The number of long ² frame received with valid CRC.
• Rx Fragments	The number of short ¹ fram received with invalid CRC.
• Rx Jabber	The number of long ² frame received with invalid CRC.
• Rx Filtered	The number of received frames filtered by the forwarding process. Short frames are frames that are smaller than 64 bytes. Long frames are frames that are longer than the configured maximum frame length for this port.

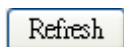


- 1 Short frame is the frames that are smaller than 64 bytes.
- 2 Long frames are frames that are longer than the configured maximum frame length for this port.

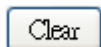
Transmit Error Counters

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 to refresh the page immediately.



: Clears the counters for all ports.

Auto-refresh ☐: Check this box to enable an automatic refresh of the page at regular intervals.

4.4.4 SFP 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, and wavelength and supports distance of SFP module on a specific interface. You can also use the hyperlink of port no. to check the statistics on a specific interface. The SFP Module Information screen in [Figure 4-4-4](#) appears.

SFP Module Information

Port	Type	Speed	Wave Length(nm)	Distance(m)	Temperature (C)	Voltage(V)	Current(mA)	TX power(dBm)	RX power(dBm)
1	--	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--	--
9	--	--	--	--	--	--	--	--	--
10	--	--	--	--	--	--	--	--	--
11	--	--	--	--	--	--	--	--	--
12	--	--	--	--	--	--	--	--	--
13	--	--	--	--	--	--	--	--	--
14	--	--	--	--	--	--	--	--	--
15	--	--	--	--	--	--	--	--	--
16	--	--	--	--	--	--	--	--	--
17	--	--	--	--	--	--	--	--	--
18	--	--	--	--	--	--	--	--	--
19	--	--	--	--	--	--	--	--	--
20	--	--	--	--	--	--	--	--	--
21	--	--	--	--	--	--	--	--	--
22	--	--	--	--	--	--	--	--	--
23	--	--	--	--	--	--	--	--	--
24	--	--	--	--	--	--	--	--	--
25	--	--	--	--	--	--	--	--	--
26	--	--	--	--	--	--	--	--	--
27	--	--	--	--	--	--	--	--	--
28	--	--	--	--	--	--	--	--	--

SFP Monitor Event Alert: ☐ send trap
Warning Temperature: Degree C

Auto-refresh ☐

Figure 4-4-4: SFP Module Information for Switch Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Type 	Display the type of current SFP module; the possible types are: <ul style="list-style-type: none"> ■ 10GBase-SR ■ 10GBase-LR ■ 1000Base-SX ■ 1000Base-LX ■ 100Base-FX
<ul style="list-style-type: none"> Speed 	Display the speed of current SFP module. The speed value or description is gotten from the SFP module. Different vendors of SFP modules might show different speed information.
<ul style="list-style-type: none"> Wave Length(nm) 	Display the wavelength of current SFP module. The wavelength value is gotten from the SFP module. Use this column to check if the wavelength values of two nodes are matched while the fiber connection is failed.

• Distance(m)	Display the support distance of current SFP module. The distance value is gotten from the SFP module.
• Temperature (C)	Display the temperature of current SFP module. The temperature value is gotten from the SFP module.
• Voltage (V)	Display the voltage of current SFP module. The voltage value is gotten from the SFP module.
• Current (mA)	Display the ampere of current SFP module. The ampere value is gotten from the SFP module.
• TX Power (dBm)	Display the TX power of current SFP module. The TX power value is gotten from the SFP module.
• RX Power (dBm)	Display the RX power of current SFP module. The RX power value is gotten from the SFP module.

Buttons

Auto-refresh ☐: Check this box to enable an automatic refresh of the page at regular intervals.

: Click to refresh the page immediately.

4.4.5 Port Mirror

Configure port mirroring on this page. This function provides to monitor 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.

Port Mirror Application

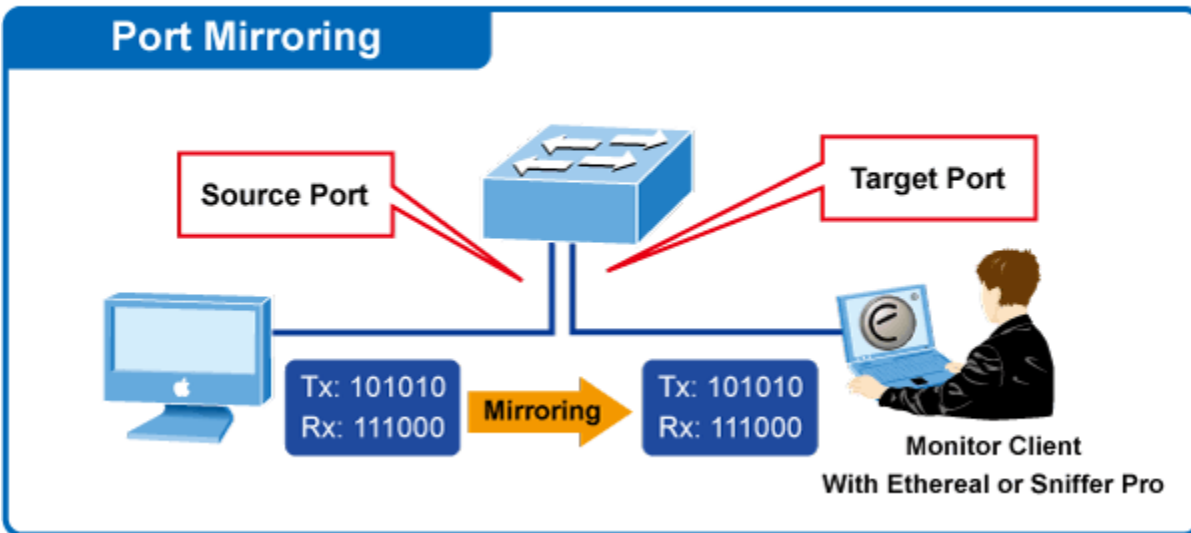


Figure 4-4-5: Port Mirror Application


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 Port Mirror screen in [Figure 4-4-6](#) appears.

Mirror Configuration

Port to mirror to Disabled 

Mirror Port Configuration

Port	Mode
*	<All> 
1	Disabled 
2	Disabled 
3	Disabled 
4	Disabled 
5	Disabled 
6	Disabled 
7	Disabled 
8	Disabled 
9	Disabled 
10	Disabled 
11	Disabled 
12	Disabled 
13	Disabled 
14	Disabled 
15	Disabled 
16	Disabled 
17	Disabled 
18	Disabled 
19	Disabled 
20	Disabled 
21	Disabled 
22	Disabled 
23	Disabled 
24	Disabled 
25	Disabled 
26	Disabled 
27	Disabled 
28	Disabled 

Save

Reset

Figure 4-4-6: Mirror Configuration Page Screenshot

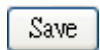
The page includes the following fields:

Object	Description
• Port to mirror on	Port to mirror also known as the mirror port . Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.
• Port	The logical port for the settings contained in the same row, * means selection of all ports of Managed Switch.
• Mode	Select mirror mode. <ul style="list-style-type: none">■ 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 nor frames received are mirrored.■ Both: Frames received and frames transmitted are mirrored to the mirror port.

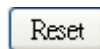


For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the **mirror port**. Because of this, **mode** for the selected mirror port is limited to **Disabled** or **Rx only**.

Buttons



: Click to save changes.



: Click to undo any changes made locally and revert to previously saved values.

4.5 Link Aggregation

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Groups (LAGs). 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 device 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 LAG 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.

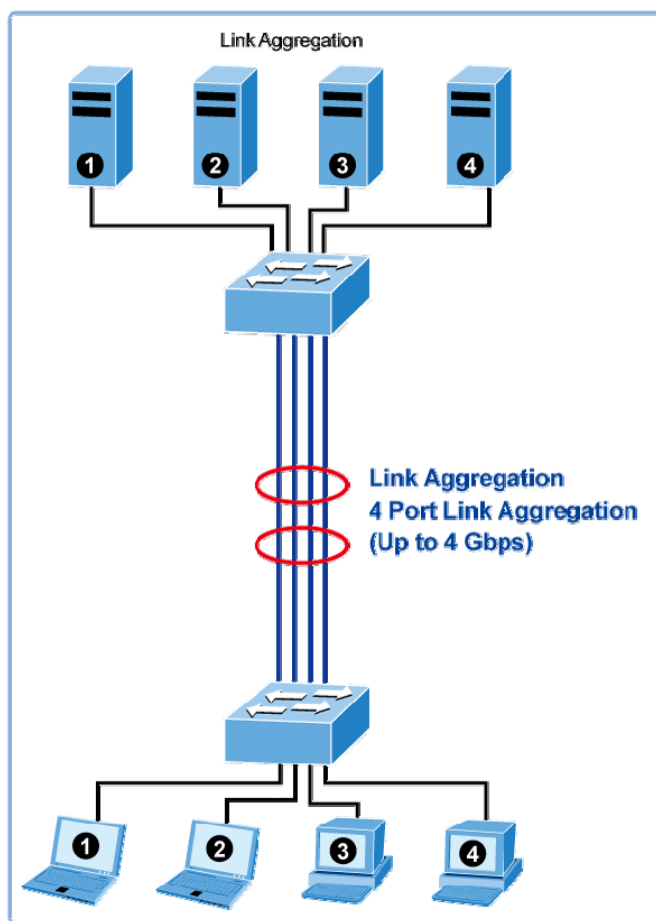


Figure 4-5-1: Link Aggregation Topology

The **Link Aggregation Control Protocol (LACP)** provides a standardized means for exchanging information between Partner Systems that require high speed redundant links. Link aggregation lets you group 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, more detail information refer to the IEEE 802.3ad standard.

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation lets you group up to 4 consecutive ports into a single dedicated connection between any two the Switch 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 (RJ-45, 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 5 groups). If the group is defined as a LACP static link aggregation 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 aggregation 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. Recording 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 5 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 (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.

4.5.1 Static Aggregation

This page is used to configure the Aggregation hash mode and the aggregation group. The aggregation hash mode settings are global, whereas the aggregation group relates to the currently selected stack unit, as reflected by the page header.

Hash Code Contributors

The Static Aggregation screen in [Figure 4-5-2](#) appears.

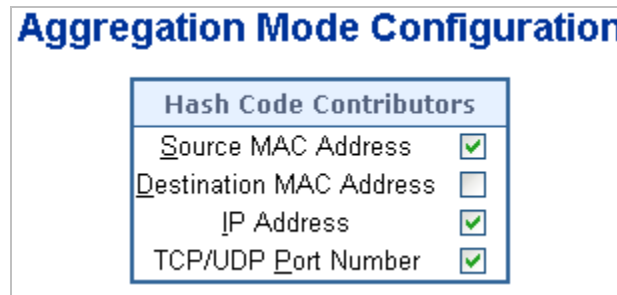


Figure 4-5-2 : Aggregation Mode Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Source MAC Address	<p>The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable.</p> <p>By default, Source MAC Address is enabled.</p>
<ul style="list-style-type: none">• Destination MAC Address	<p>The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable.</p> <p>By default, Destination MAC Address is disabled.</p>
<ul style="list-style-type: none">• IP Address	<p>The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable.</p> <p>By default, IP Address is enabled.</p>
<ul style="list-style-type: none">• TCP/UDP Port Number	<p>The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable.</p> <p>By default, TCP/UDP Port Number is enabled.</p>

Static Aggregation Group Configuration

The Aggregation Group Configuration screen in [Figure 4-5-3](#) appears.

Aggregation Group Configuration

	Port Members																											
Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Normal	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	
1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
9	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
10	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
11	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
12	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
13	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
14	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	

Save

Reset

Figure 4-5-3: Aggregation Group Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">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.
<ul style="list-style-type: none">Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Buttons

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.5.2 LACP Configuration

Link Aggregation Control Protocol (LACP) - LACP LAG negotiate 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 the current LACP port configurations, and possibly change them as well. The LACP port settings relate to the currently selected stack unit, as reflected by the page header. The LACP Configuration screen in [Figure 4-5-4](#) appears.

LACP Port Configuration


Port	LACP Enabled	Key		Role	Timeout	Priority
*	<input type="checkbox"/>	<All> ▼		<All> ▼	<All> ▼	32768
1	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
2	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
3	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
4	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
5	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
6	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
7	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
8	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
9	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
10	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
11	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
12	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
13	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
14	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
15	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
16	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
17	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
18	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
19	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
20	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
21	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
22	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
23	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
24	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
25	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
26	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
27	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768
28	<input type="checkbox"/>	Auto ▼		Active ▼	Fast ▼	32768


Figure 4-5-4 : LACP Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number, * means selection of all ports of Managed Switch.
• LACP Enabled	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form max 12 LLAGs per switch and 2 GLAGs per stack.
• Key	<p>The Key value incurred by the port range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.</p> <p>The default setting is “Auto”</p>
• Role	The Role shows the LACP activity status. The Active will transmit LACP packets each second; while Passive will wait for a LACP packet from a partner (speak if spoken to).
• Timeout	The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.
• Partner Priority	The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.5.3 LACP System Status

This page provides a status overview for all LACP instances. The LACP Status page display the current LACP aggregation Groups and LACP Port status. The LACP System Status screen in [Figure 4-5-5](#) appears.

LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Priority	Last Changed	Local Ports
No ports enabled or no existing partners					
Auto-refresh <input type="checkbox"/> <input type="button" value="Refresh"/>					

Figure 4-5-5: LACP System Status Page Screenshot

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.
• Last changed	The time since this aggregation changed.
• Local Ports	Shows which ports are a part of this aggregation for this switch. .

Buttons

: Click to refresh the page immediately.

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

4.5.4 LACP Port Status

This page provides a status overview for LACP status for all ports. The LACP Port Status screen in [Figure 4-5-6](#) appears.

LACP Status						
Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Priority
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-
11	No	-	-	-	-	-
12	No	-	-	-	-	-
13	No	-	-	-	-	-
14	No	-	-	-	-	-
15	No	-	-	-	-	-
16	No	-	-	-	-	-
17	No	-	-	-	-	-
18	No	-	-	-	-	-
19	No	-	-	-	-	-
20	No	-	-	-	-	-
21	No	-	-	-	-	-
22	No	-	-	-	-	-
23	No	-	-	-	-	-
24	No	-	-	-	-	-
25	No	-	-	-	-	-
26	No	-	-	-	-	-
27	No	-	-	-	-	-
28	No	-	-	-	-	-

Auto-refresh ☐ [Refresh](#)

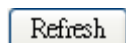
Figure 4-5-6: LACP Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number.
• LACP	<p>'Yes' means that LACP is enabled and the port link is up.</p> <p>'No' means that LACP is not enabled or that the port link is down.</p> <p>'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile its LACP status is disabled.</p>
• Key	The key assigned to this port. Only ports with the same key can aggregate together.

• Aggr ID	The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.
• Partner System ID	The partners System ID (MAC address).
• Partner Port	The partner port number connected to this port.

Buttons



: Click to refresh the page immediately.

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

4.5.5 LACP Port Statistics

This page provides an overview for LACP statistics for all ports. The LACP Port Statistics screen in [Figure 4-5-7](#) appears.

LACP Statistics					
Port	LACP Received	LACP Transmitted	Discarded		
			Unknown	Illegal	
1	0	0	0	0	
2	0	0	0	0	
3	0	0	0	0	
4	0	0	0	0	
5	0	0	0	0	
6	0	0	0	0	
7	0	0	0	0	
8	0	0	0	0	
9	0	0	0	0	
10	0	0	0	0	
11	0	0	0	0	
12	0	0	0	0	
13	0	0	0	0	
14	0	0	0	0	
15	0	0	0	0	
16	0	0	0	0	
17	0	0	0	0	
18	0	0	0	0	
19	0	0	0	0	
20	0	0	0	0	
21	0	0	0	0	
22	0	0	0	0	
23	0	0	0	0	
24	0	0	0	0	
25	0	0	0	0	
26	0	0	0	0	
27	0	0	0	0	
28	0	0	0	0	

Auto-refresh ☐

Figure 4-5-7: LACP Statistics Page Screenshot

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

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

: Clears the counters for all ports.

4.6 VLAN

4.6.1 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 segments 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 to only members of the VLAN on which the broadcast was initiated.



-
1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, 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.
 3. The Switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLAN is created, the member ports assigned to the new VLAN will be removed from the DEFAULT_VLAN port member list. The DEFAULT_VLAN has a VID = 1.
-

This section has the following items:

- | | |
|----------------------------------|---|
| ■ VLAN Basic Information | Displays VLAN information |
| ■ VLAN Port Configuration | Enables VLAN group |
| ■ VLAN Memberships | Configures the VLAN membership |
| ■ 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/disables port isolation on port |
| ■ MAC-based VLAN | Configures the MAC-based VLAN entries |
| ■ MAC-based VLAN Status | Displays MAC-based VLAN entries |
| ■ IP Subnet-based VLAN | Configures the IP Subnet-based VLAN entries |
| ■ Protocol-based VLAN | Configures the protocol-based VLAN entries |
| ■ Protocol-based VLAN | Displays the protocol-based VLAN entries |

4.6.2 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 allowing you to move 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 e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make 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 requires 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 your network. IEEE 802.1Q VLAN will only deliver 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:

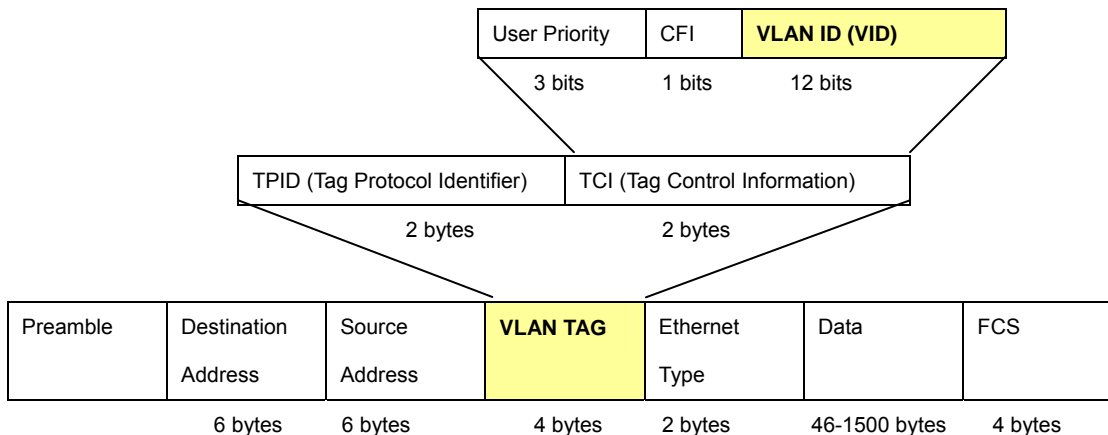
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

■ 802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. 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 3 bits of user priority, 1 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 3 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.

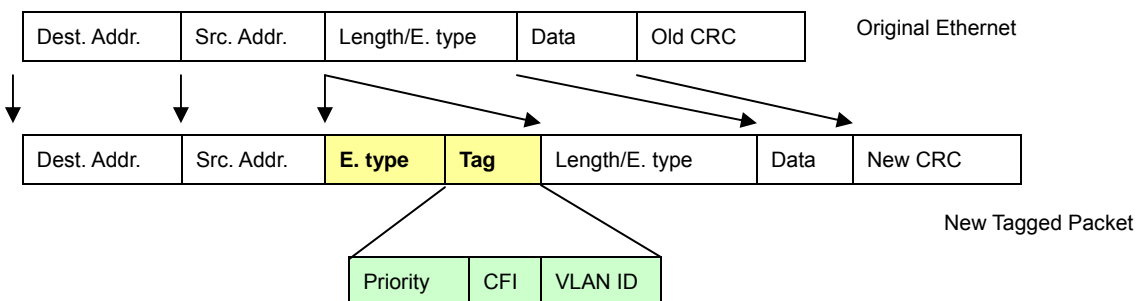
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

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 (are 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 (and indeed, 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 VLAN 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 VLAN are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VID are different the switch will drop 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 VID 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 Switch initially configures one VLAN, VID = 1, called "**default**." The factory default setting assigns all ports on the Switch to the "**default**". As new VLAN 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 if you want it to 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 you should add this port to the VLAN as an untagged port.



VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it 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). But 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 which do not overlap, but still need to communicate, you can connect them by enabled 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.

4.6.3 VLAN Port Configuration

This Page is used for configuring the Managed Switch port VLAN. The VLAN per Port Configuration Page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the VLAN Port Configuration Page. All untagged packets arriving to the device are tagged by the ports PVID.

Understand nomenclature of the Switch

■ 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 will 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 will 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 will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

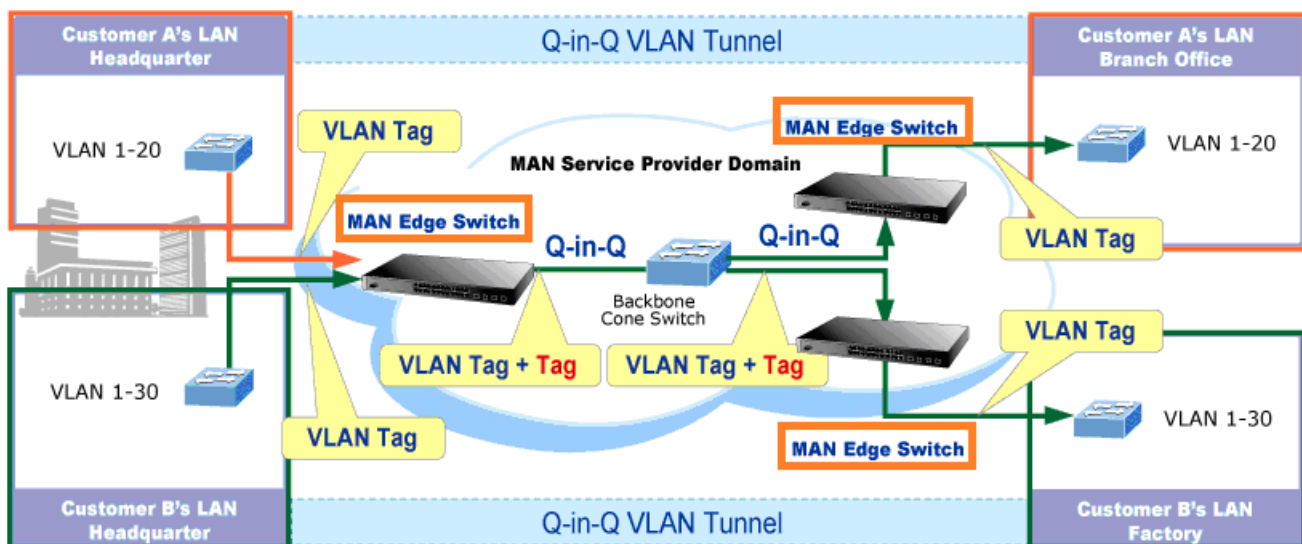
Frame Income Frame Leave	Income Frame is tagged	Income Frame is untagged
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remain untagged

Table 4-6-1: Ingress / Egress Port with VLAN VID Tag / Untag Table

■ IEEE 802.1Q Tunneling (Q-in-Q)

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ 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 applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** 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

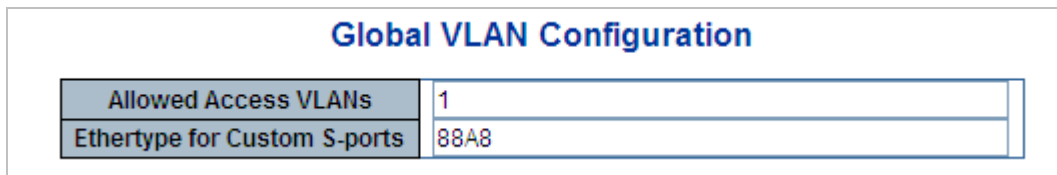
of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

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 are 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 is reduced.

Global VLAN Configuration

The Global VLAN Configuration screen in [Figure 4-6-1](#) appears.



Global VLAN Configuration	
Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Figure 4-6-1 : Global VLAN Configuration Screenshot

The Page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Allowed Access VLANs 	<p>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.</p> <p>By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.</p> <p>The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.</p>
<ul style="list-style-type: none"> Ethertype for Custome S-ports 	<p>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.</p>

Port VLAN Configuration

The VLAN Port Configuration screen in [Figure 4-6-2](#) appears.

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<All> ▼		<All> ▼	<input type="checkbox"/>	<All> ▼	<All> ▼		
1	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
2	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
3	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
4	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
5	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
6	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
7	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
8	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
9	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
10	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
11	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
12	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
13	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
14	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
15	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
16	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
17	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
18	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
19	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
20	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
21	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
22	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
23	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
24	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
25	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
26	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
27	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	
28	Access ▼	1	C-Port ▼	<input checked="" type="checkbox"/>	Tagged and Untagged ▼	Untag Port VLAN ▼	1	

Figure 4-6-2 : Port VLAN Configuration Screenshot

The Page includes the following fields:

Object		Description
• Port		This is the logical port number for this row.
• Mode	Access	<p>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:</p> <ul style="list-style-type: none"> Member of exactly one VLAN, the Port VLAN (Access VLAN), which by default is 1

		<ul style="list-style-type: none"> • 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	<p>Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:</p> <ul style="list-style-type: none"> • 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	<p>Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:</p> <ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • Port VLAN 		<p>Determines the port's VLAN ID (PVID). Allowed VLANs are in the range 1 through 4095, default being 1.</p> <ul style="list-style-type: none"> ■ 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. <p>The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.</p>
<ul style="list-style-type: none"> • Port Type 		<p>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.</p> <ul style="list-style-type: none"> ■ Unaware:

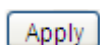
	<p>On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.</p> <ul style="list-style-type: none"> <u>C-Port:</u> <p>On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. 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.</p> <u>S-Port:</u> <p>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.</p> <u>S-Custom-Port:</u> <p>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.</p>
<ul style="list-style-type: none"> • Ingress Filtering 	<p>Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.</p> <ul style="list-style-type: none"> <p>If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.</p> <p>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.</p> <p>However, the port will never transmit frames classified to VLANs that it is not a member of.</p>
<ul style="list-style-type: none"> • Ingress Acceptance 	<p>Hybrid ports allow for changing the type of frames that are accepted on ingress.</p> <ul style="list-style-type: none"> <u>Tagged and Untagged</u> <p>Both tagged and untagged frames are accepted.</p> <u>Tagged Only</u> <p>Only tagged frames are accepted on ingress. Untagged frames are discarded.</p> <u>Untagged Only</u> <p>Only untagged frames are accepted on ingress. Tagged frames are discarded.</p>
Egress Tagging	<p>This option is only available for ports in Hybrid mode. Ports in Trunk and Hybrid mode may control the tagging of frames on egress.</p> <ul style="list-style-type: none"> <u>Untag Port VLAN</u>

	<p>Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.</p> <p>■ Tag All</p> <p>All frames, whether classified to the Port VLAN or not, are transmitted with a tag.</p> <p>■ Untag All</p> <p>All frames, whether classified to the Port VLAN or not, are transmitted without a tag.</p>
<ul style="list-style-type: none"> • Allowed VLANs 	<p>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.</p> <p>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.</p>
<ul style="list-style-type: none"> • Forbidden VLANs 	<p>A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field.</p> <p>By default, the field is left blank, which means that the port may become a member of all possible VLANs.</p>

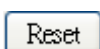


The port must be a member of the same VLAN as the Port VLAN ID.

Buttons



: Click to apply changes



: Click to undo any changes made locally and revert to previously saved values.

4.6.4 VLAN Membership Status

This Page provides an overview of membership status for VLAN users. The VLAN Membership Status screen in [Figure 4-6-4](#) appears.

VLAN Membership Status for Combined users

Combined Auto-refresh ☐

Start from VLAN with entries per page.

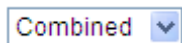
	Port Members																											
VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 4-6-4: VLAN Membership Status for Static User Page Screenshot

The Page includes the following fields:

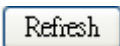
Object	Description
<ul style="list-style-type: none"> VLAN User 	<p>A VLAN User is a module that uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN :</p> <ul style="list-style-type: none"> - Admin : This is referred as static. - 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.
<ul style="list-style-type: none"> Port Members 	<p>A row of check boxes for each port is displayed for each VLAN ID.</p> <p>If a port is included in a VLAN, an image <input checked="" type="checkbox"/> will be displayed.</p> <p>If a port is included in a Forbidden port list, an image <input checked="" type="checkbox"/> will be displayed.</p> <p>If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as conflict port.</p>
<ul style="list-style-type: none"> VLAN Membership 	<p>The VLAN Membership Status Page shall show 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 shall show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.</p>

Buttons



: Select VLAN Users from this drop down list.

Auto-refresh ☐: Check this box to refresh the Page automatically. Automatic refresh occurs every 3 seconds.



: Click to refresh the Page immediately.



: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.



: Updates the table, starting with the entry after the last entry currently displayed.

4.6.5 VLAN Port Status

This Page provides VLAN Port Status. The VLAN Port Status screen in [Figure 4-6-5](#) appears.

VLAN Port Status for Combined users

Combined ▼ Auto-refresh ☐ Refresh





























Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port		All	1	Untag PVID		No
2	C-Port		All	1	Untag PVID		No
3	C-Port		All	1	Untag PVID		No
4	C-Port		All	1	Untag PVID		No
5	C-Port		All	1	Untag PVID		No
6	C-Port		All	1	Untag PVID		No
7	C-Port		All	1	Untag PVID		No
8	C-Port		All	1	Untag PVID		No
9	C-Port		All	1	Untag PVID		No
10	C-Port		All	1	Untag PVID		No
11	C-Port		All	1	Untag PVID		No
12	C-Port		All	1	Untag PVID		No
13	C-Port		All	1	Untag PVID		No
14	C-Port		All	1	Untag PVID		No
15	C-Port		All	1	Untag PVID		No
16	C-Port		All	1	Untag PVID		No
17	C-Port		All	1	Untag PVID		No
18	C-Port		All	1	Untag PVID		No
19	C-Port		All	1	Untag PVID		No
20	C-Port		All	1	Untag PVID		No
21	C-Port		All	1	Untag PVID		No
22	C-Port		All	1	Untag PVID		No
23	C-Port		All	1	Untag PVID		No
24	C-Port		All	1	Untag PVID		No
25	C-Port		All	1	Untag PVID		No
26	C-Port		All	1	Untag PVID		No
27	C-Port		All	1	Untag PVID		No
28	C-Port		All	1	Untag PVID		No

Figure 4-6-5: VLAN Port Status for Static User Page Screenshot

The Page includes the following fields:

Object	Description
• Port	The logical port for the settings contained in the same row.
• Port Type	<p>Show the VLAN Awareness for the port.</p> <p>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.</p> <p>If VLAN awareness is disabled, all frames are classified to the Port VLAN ID and tags are not removed.</p>
• Ingress Filtering	Show 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 whether 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 whether tagged or untagged.
• Untagged VLAN ID	Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.
• Conflicts	<p>Shows status of Conflicts whether exists or Not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:</p> <ul style="list-style-type: none"> ■ Functional Conflicts between feature. ■ Conflicts due to hardware limitation. ■ Direct conflict between user modules.

Buttons

: Select VLAN Users from this drop down list.

Auto-refresh ☐: Check this box to refresh the Page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the Page immediately.

4.6.6 Prvivate VLAN

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

The Private VLAN screen in [Figure 4-6-6](#) appears.

Auto-refresh ☐ Refresh

Private VLAN Membership Configuration

		Port Members																											
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add New Private VLAN

SaveReset

Figure 4-6-6: Private VLAN Membership Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">Delete	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
<ul style="list-style-type: none">Private VLAN ID	Indicates the ID of this particular private VLAN.
<ul style="list-style-type: none">Port Members	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

Add new Private VLAN: Click to add new VLAN.

Save: Click to save changes.

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

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh

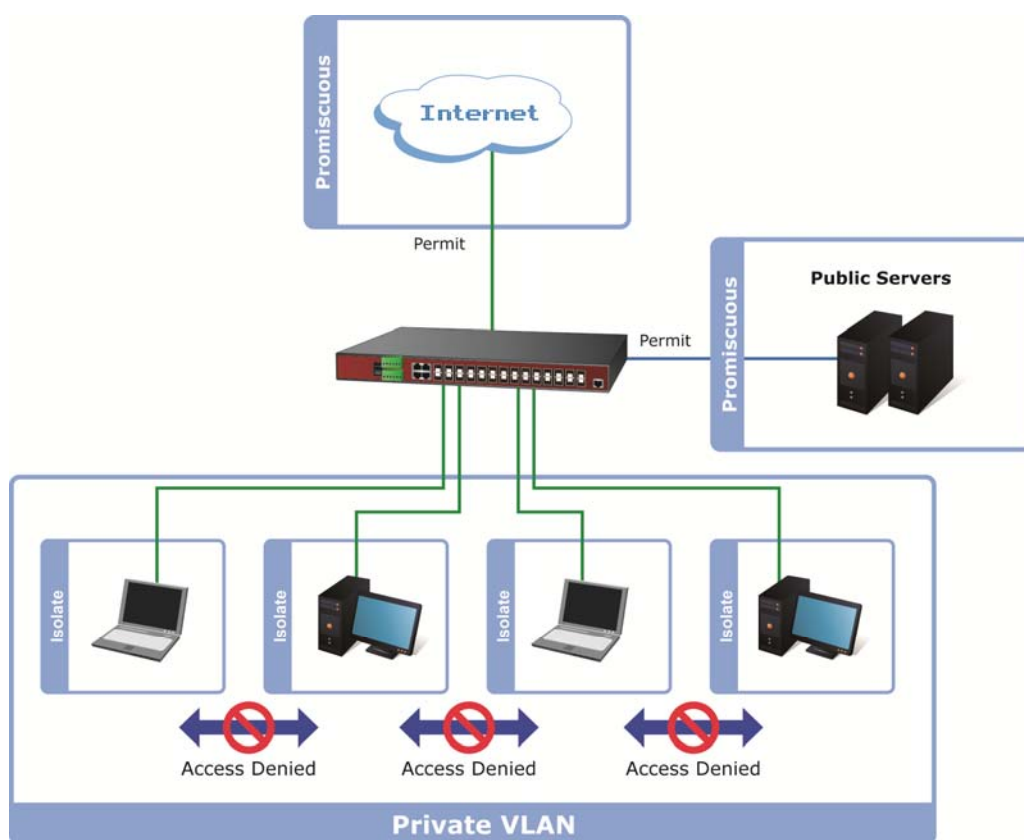
: Click to refresh the page immediately.

4.6.7 Port Isolation

Overview

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 which 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 which 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.

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN. The Port Isolation screen in [Figure 4-6-7](#) appears.

Auto-refresh ☐ Refresh

Port Isolation Configuration

Port Number																											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save Reset

Figure 4-6-7: Port Isolation Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">Port Members	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

Buttons

Save: Click to save changes.

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

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.6.8 VLAN Setting Example:

- Separate VLAN
- - 802.1Q VLAN Trunk
- - Port Isolate

4.6.8.1 Two separate 802.1Q VLANs

The diagram shows how the Managed Switch handles Tagged and Untagged traffic flow for two VLANs. VLAN Group 2 and VLAN Group 3 are separated VLAN. Each VLAN isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. The screen in [Figure 4-6-8](#) appears and [Table 4-1](#) describes the port configuration of the **Managed Switch**.

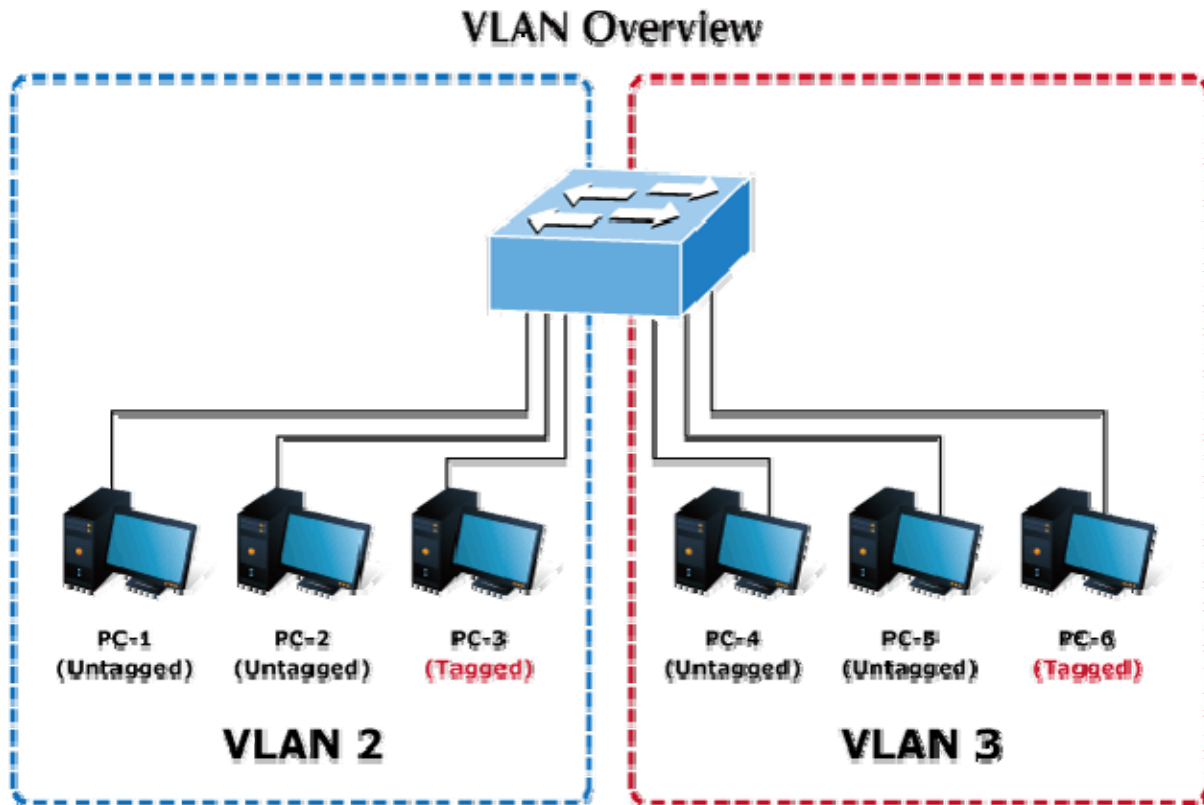


Figure 4-6-8: Two Separate VLAN Diagrams

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

Table 4-1: VLAN and Port Configuration

The scenario described as follows:

■ **Untagged packet entering VLAN 2**

1. While [PC-1] transmit 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 its tag becoming an **untagged** packet.
4. While the packet leaves **Port-3**, it will keep as a **tagged** packet with **VLAN Tag=2**.

■ **Tagged packet entering VLAN 2**

5. While **[PC-3]** transmits 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**.
6. While the packet leaves **Port-1** and **Port-2**, it will be stripped away its tag becoming an **untagged** packet.

■ Untagged packet entering VLAN 3

1. While **[PC-4]** transmits 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 its tag becoming an **untagged** packet.
3. While the packet leaves **Port-6**, it will keep as a **tagged** packet with **VLAN Tag=3**.



For this example, VLAN Group 1 is set as default VLAN, but only focuses on VLAN 2 and VLAN 3 traffic flow. The example screenshot comes from the other switch but the configuration interface is the same with NS4750-24S-4T-4X.

Setup steps

1. Create VLAN Group

Add two VLANs – VLAN 2 and VLAN 3

Type 1-3 in Allowed Access VLANs column, the 1-3 is including VLAN1 and 2 and 3.

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

Figure 4-6-9: Add VLAN 2 and VLAN 3

2. Assign VLAN Member :

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

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>	<input type="checkbox"/>	<All>	<All>	2	
1	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	2	
2	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	2	
3	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	2	
4	Access	3	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	3	
5	Access	3	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	3	
6	Access	3	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	3	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

Figure 4-6-10: Change Port VLAN of Port 1~3 to be VLAN2 and Port VLAN of Port 4~6 to be VLAN3

3. Remove VLAN Member for VLAN 1:

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

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

Change Port 6 Mode as Trunk and Selects Egress Tagging as Tag All and Types 3 in the Allowed VLANs column.

The Per Port VLAN configuration in [Figure 4-6-11](#) appears.

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>	<input type="checkbox"/>	<All>	<All>	2	
1	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	2	
2	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	2	
3	Trunk	2	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	2	
4	Access	3	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	3	
5	Access	3	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	3	
6	Trunk	3	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	3	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

Figure 4-6-11: Check VLAN 2 and 3 Members on VLAN Membership Page

4.6.8.2 VLAN Trunking between two 802.1Q aware Switches

The most cases are used for “Uplink” to other switches. VLANs are separated at different switches, but they need to access with other switches within the same VLAN group. The screen in [Figure 4-6-12](#) appears.

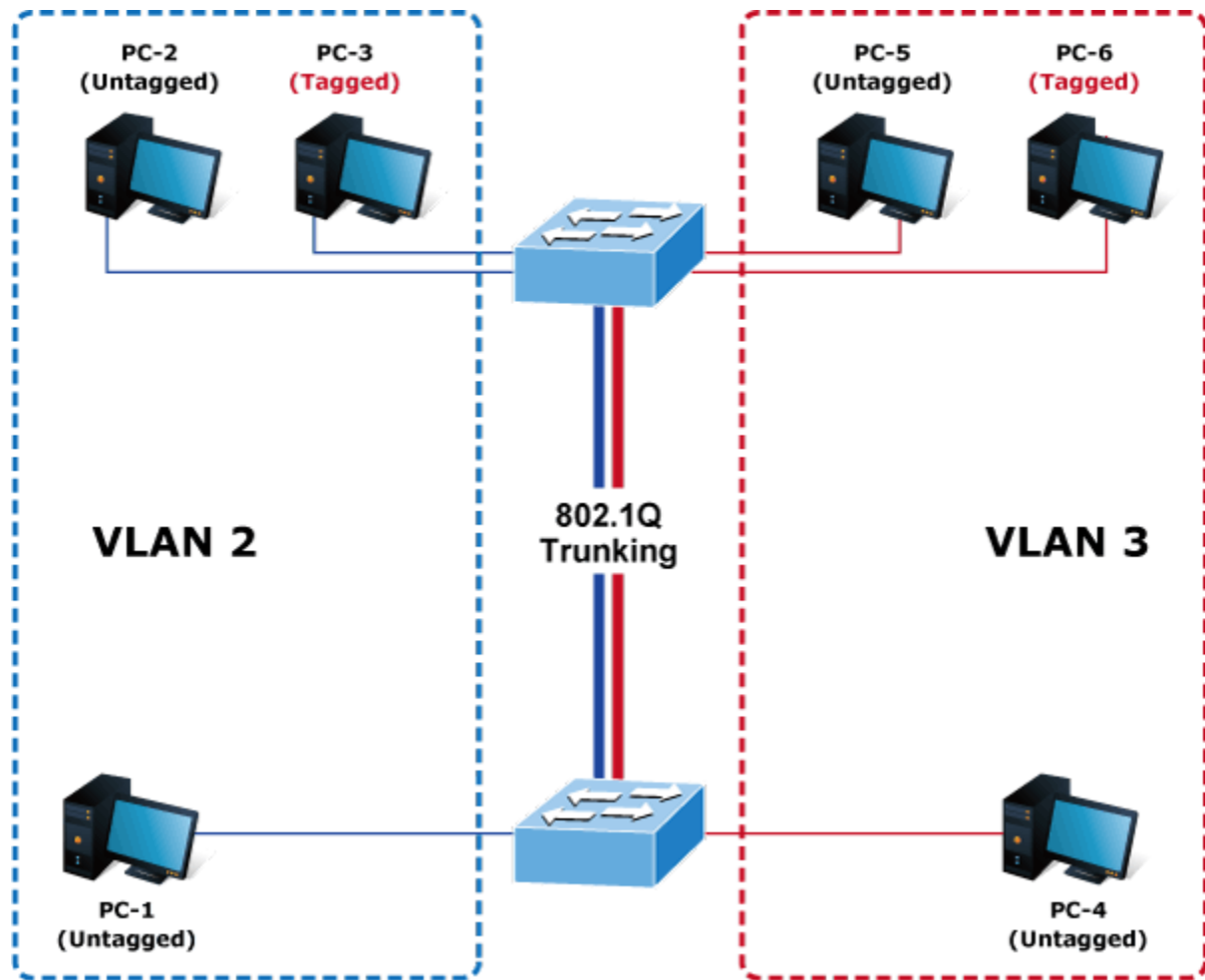


Figure 4-6-12: VLAN Trunking Diagram

Setup steps

1. Add VLAN Group

Add two VLANs – VLAN 2 and VLAN 3

Type 1-3 in Allowed Access VLANs column, the 1-3 is including VLAN1 and 2 and 3.

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

Figure 4-6-13: Add VLAN 2 and VLAN 3

2. Assign VLAN Member and PVID for 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>	<input type="checkbox"/>	<All>	<All>	2	
1	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	2	
2	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	2	
3	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	2	
4	Access	3	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	3	
5	Access	3	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	3	
6	Access	3	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	3	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

Figure 4-6-14: Changes Port VLAN of Port 1~3 to be VLAN2 and Port VLAN of Port 4~6 to be VLAN3

For the VLAN ports connecting to the hosts, please refer to 4.6.10.1 examples. The following steps will 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** at the VLAN Member configuration Page.
3. Define a **VLAN 1** as a “**Public Area**” that overlapping with both **VLAN 2 members** and **VLAN 3 members**.
4. Assign the VLAN Trunk Port to be the member of each VLAN – which wants to be aggregated. For this example, add **Port-7** to be **VLAN 2** and **VLAN 3** member port.
5. Specify **Port-7** to be the 802.1Q VLAN **Trunk port**, and the Trunking port must be a **Tagged** port while egress. The Port-7 configuration is shown in [Figure 4-6-15](#).

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>	<input type="checkbox"/>	<All>	<All>	2	1
1	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	2	1
2	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	2	1
3	Access	2	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	2	1
4	Access	3	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	3	1
5	Access	3	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	3	1
6	Access	3	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	3	1
7	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1-3	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

Figure 4-6-15: VLAN Overlap Port Setting & VLAN 1 – The Public Area Member Assign

That is, although the VLAN 2 members: Port-1 to Port-3 and VLAN 3 members: Port-4 to Port-6 also belongs to VLAN 1. But with different PVID settings, packets from VLAN 2 or VLAN 3 is not able to access to the other VLAN.

6. Repeat Steps 1 to 6, set 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.

4.6.10.3 Port Isolate

The diagram shows how the Managed Switch handles isolate and promiscuous ports, and the each PC is not able to access each other PCs of each isolate port. But they all need to access with the same server/AP/Printer. The screen in [Figure 4-6-16](#) appears. This section will show you how to configure the port for the server – that could be accessed by each isolate port.

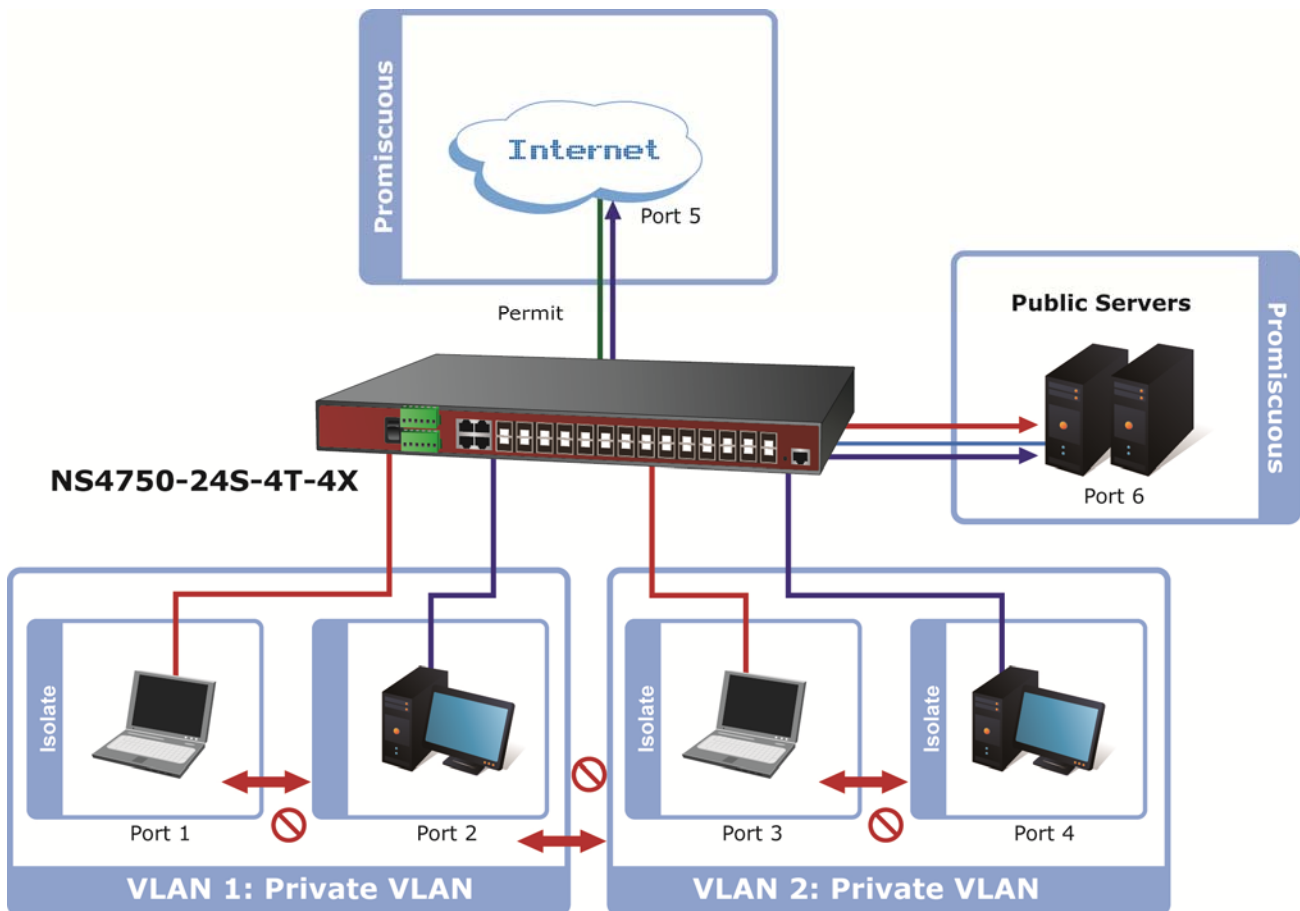


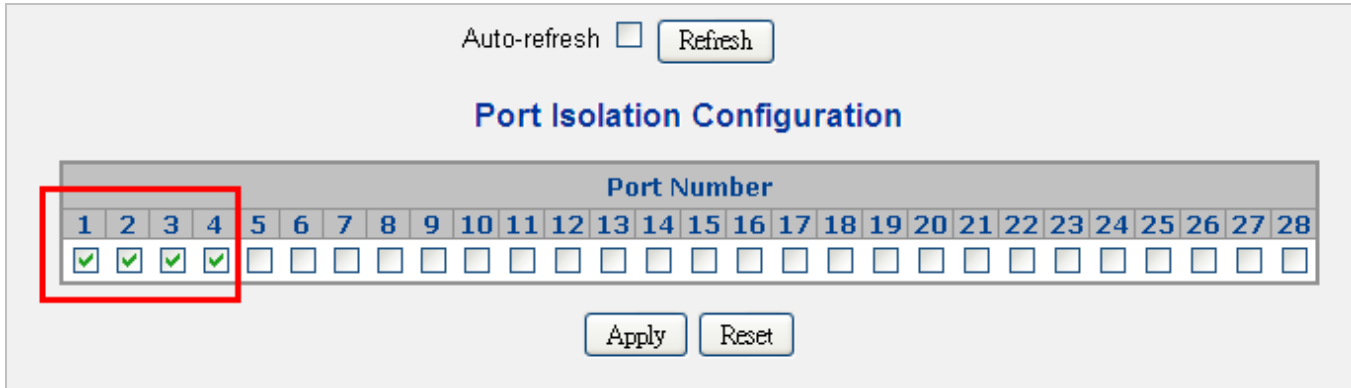
Figure 4-6-16: The Port Isolate VLAN Diagram

Setup steps

1. Assign Port Mode

Set Port-1~Port-4 in Isolate port.

Set Port5 and Port-6 in Promiscuous port. The screen in [Figure 4-6-17](#) appears.



The interface shows a configuration table for 28 ports. Ports 1-4 are checked for isolation, while ports 5-6 are checked for promiscuous mode. The interface includes an 'Auto-refresh' checkbox, a 'Refresh' button, and 'Apply' and 'Reset' buttons at the bottom.

Port Isolation Configuration																											
Port Number																											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Auto-refresh ☐ Refresh

Apply Reset

Figure 4-6-17: The Configuration of Isolated and Promiscuous Port

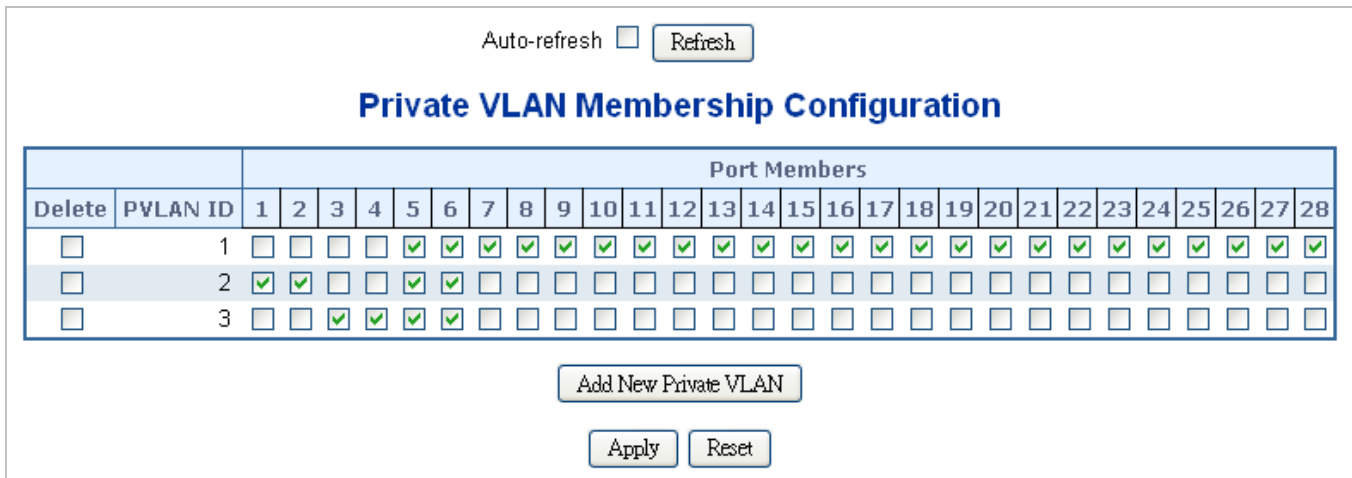
2. Assign VLAN Member :

VLAN 1 : Port-5 and Port-6

VLAN 2 : Port-1,Port-2 ,Port-5 and Port-6

VLAN 3: Port-3~Port-6.

The screen in [Figure 4-6-18](#) appears.



The interface shows a table for assigning ports to private VLANs. Three VLANs are configured: VLAN 1 (ports 5, 6), VLAN 2 (ports 1, 2, 5, 6), and VLAN 3 (ports 3, 4, 5, 6). The interface includes an 'Auto-refresh' checkbox, a 'Refresh' button, and 'Add New Private VLAN', 'Apply', and 'Reset' buttons at the bottom.

		Port Members																											
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input type="checkbox"/>	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Auto-refresh ☐ Refresh

Add New Private VLAN

Apply Reset

Figure 4-6-18: Private VLAN Port Setting

4.6.11 MAC-based VLAN

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries. The MAC-based VLAN screen in [Figure 4-6-17](#) appears.

MAC-based VLAN Membership Configuration

Auto-refresh ☐ Refresh << >>

Delete	MAC Address	VLAN ID	Port Members																											
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Currently no entries present																														

Add New Entry

Save Reset

Figure 4-6-19: MAC-based VLAN Membership Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Delete	To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted in the stack.
<ul style="list-style-type: none">• MAC Address	Indicates the MAC address.
<ul style="list-style-type: none">• VLAN ID	Indicates the VLAN ID.
<ul style="list-style-type: none">• Port Members	A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

Add new entry: Click to add a new MAC-based VLAN entry.

Save: Click to save changes.

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

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the table starting from the first entry in the MAC-based VLAN Table.



: Updates the table, starting with the entry after the last entry currently displayed.

4.6.12 MAC-based VLAN Status

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. The MAC-based VLAN Status screen in [Figure 4-6-18](#) appears.

MAC-based VLAN Membership Status for User Static

Static Auto-refresh ☐

MAC Address	VLAN ID	Port Members																											
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No data exists for the user																													

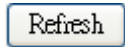
Figure 4-6-20: MAC-based VLAN Membership Configuration for User Static Page Screenshot

The page includes the following fields:

Object	Description
• MAC Address	Indicates the MAC address.
• VLAN ID	Indicates the VLAN ID.
• Port Members	Port members of the MAC-based VLAN entry.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.



: Click to refresh the page immediately.

4.6.13 Protocol-based VLAN

This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the switch. The Protocol-based VLAN screen in [Figure 4-6-21](#) appears.

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
No Group entry found!			

Auto-refresh ☐

Figure 4-6-21: Protocol to Group Mapping Table Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Delete 	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.
<ul style="list-style-type: none"> Frame Type 	<p>Frame Type can have one of the following values:</p> <ol style="list-style-type: none"> Ethernet LLC SNAP <p>Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you select..</p>
<ul style="list-style-type: none"> Value 	<p>Valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu.</p> <p>Below is the criteria for three different Frame Types:</p> <ol style="list-style-type: none"> For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff For LLC: Valid value in this case is comprised of two different sub-values. <ol style="list-style-type: none"> DSAP: 1-byte long string (0x00-0xff) SSAP: 1-byte long string (0x00-0xff) For SNAP: Valid value in this case also is comprised of two different sub-values. <ol style="list-style-type: none"> OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges

	<p>from 0x00-0xff.</p> <p>b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.</p>
<ul style="list-style-type: none"> • Group Name 	<p>A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9). Note: special character and underscore(_) are not allowed.</p>

Buttons

Add New Entry

: Click to add a new entry in mapping table.

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh

: Click to refresh the page immediately.

4.6.14 Protocol-based VLAN Membership

This page allows you to map a already configured Group Name to a VLAN for the switch. The Group Name to VLAN Mapping Table screen in [Figure 4-6-22](#) appears.

Group Name to VLAN Mapping Table

			Port Members																											
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No Group entries																														

Add New Entry

Save

Reset

Auto-refresh ☐

Refresh

Figure 4-6-22: Group Name to VLAN Mapping Table Page Screenshot

The page includes the following fields:

Object	Description
• Delete	To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save
• Group Name	A valid Group Name is a string of atmost 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. Whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be preused by any other existing mapping entry on this page.
• VLAN ID	Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.
• Port Members	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

: Click to add a new entry in mapping table.

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

4.7 Spanning Tree Protocol

4.7.1 Theory

The Spanning Tree protocol 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 your network to ensure that only one route exists between any two stations on the network, and provide backup links which 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 Spanning Tree Protocol 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

It is to make the root port a fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become 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 instance, 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 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

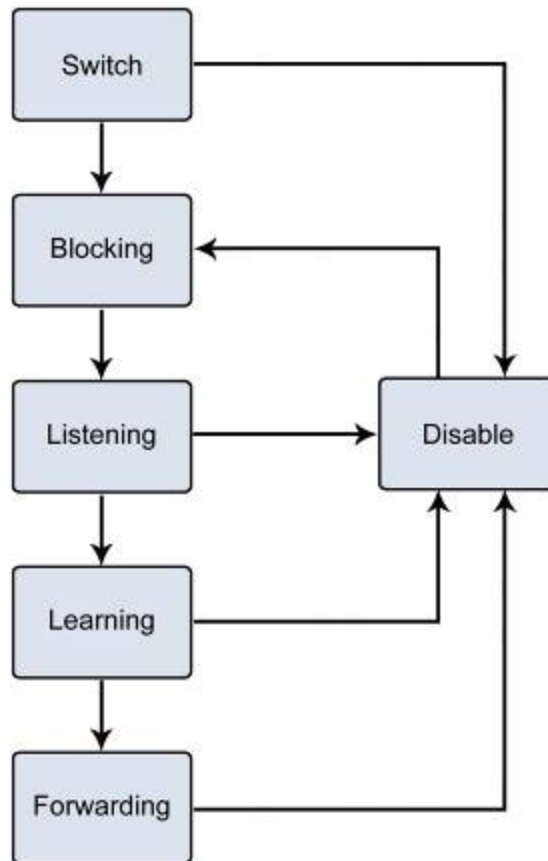


Figure 4-7-1: STP Port State Transitions

You can modify each port state by using management software. When you enable STP, 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.

2. STP Parameters

STP Operation Levels

The 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.



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 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 Switch's factory default setting should cover the majority of installations. However, 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 your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.



The Hello Time cannot be longer than the Max. Age. Otherwise, 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, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your 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.



Observe the following formulas when setting the above parameters:

Max. Age $\geq 2 \times (\text{Forward Delay} - 1 \text{ second})$

Max. Age $\geq 2 \times (\text{Hello Time} + 1 \text{ second})$

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.

3. Illustration of STP

A simple illustration of three switches connected in a loop is depicted in the below 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 will broadcast it to switch C, and switch C will broadcast it to 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 will drop the packet at port 2 and the broadcast will end 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 straight forward.

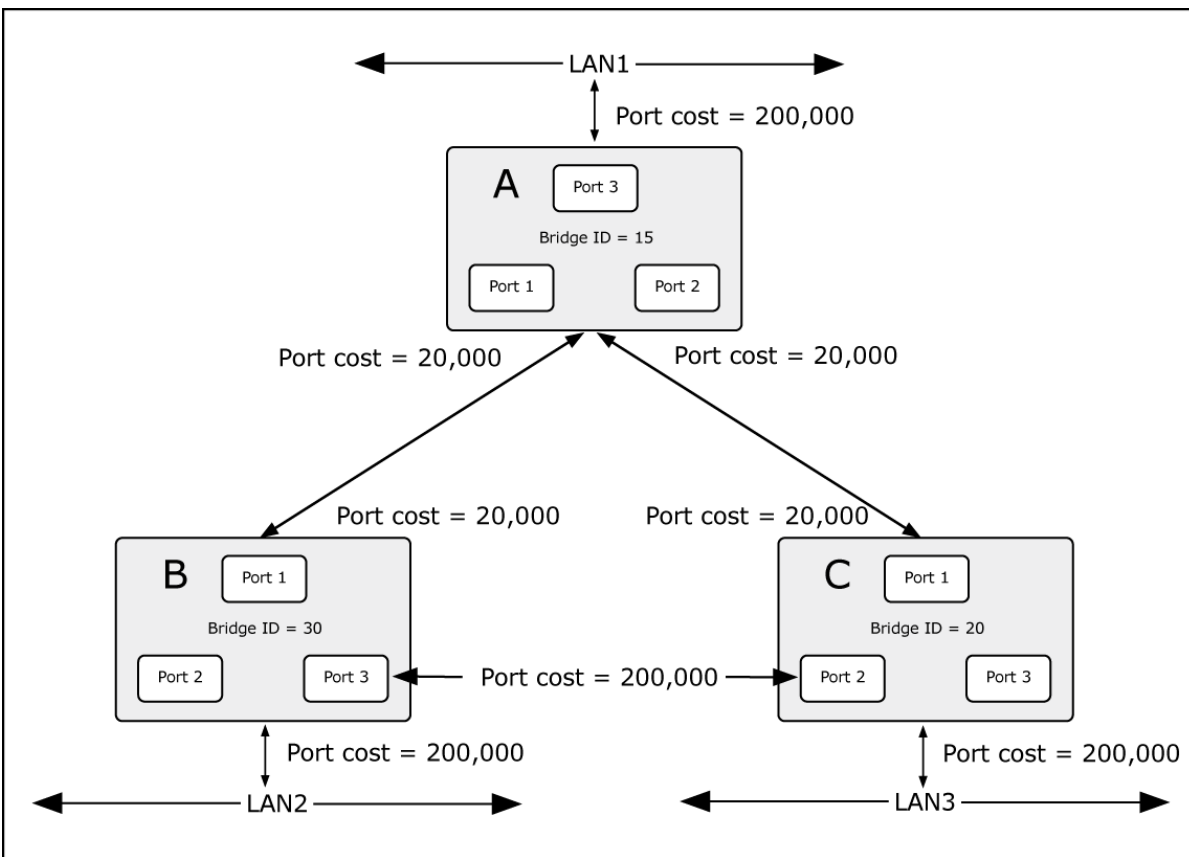


Figure 4-7-2: Before Applying the STA Rules

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

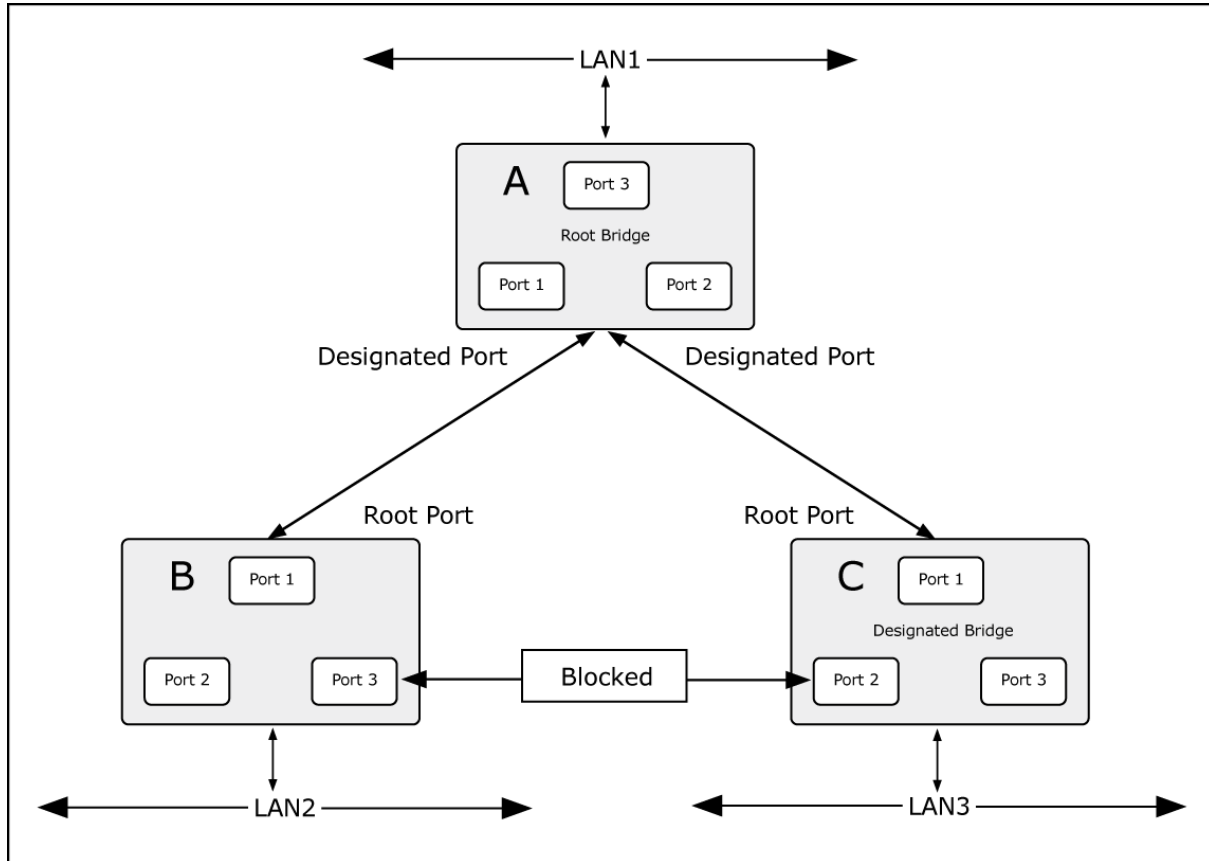


Figure 4-7-3: After Applying the STA Rules

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.

4.7.2 STP System Configuration

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch or switch Stack. The Managed Switch support 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 of 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" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

The STP System Configuration screen in [Figure 4-7-4](#) appears.

STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	128
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

Save

Reset

Figure 4-7-4: STP Bridge Configuration Page Screenshot

The page includes the following fields:

Basic Settings

Object	Description
• Protocol Version	The STP protocol version setting. Valid values are STP , RSTP and MSTP .
• Bridge Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
• Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds -Default: 15 -Minimum: The higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$ -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 $[2 \times (\text{Hello Time} + 1)]$. -Maximum: The lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$
• 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 will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Object	Description
• Edge Port BPDU Filtering	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
• Edge Port BPDU Guard	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
• Port Error Recovery	Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
• Port Error Recovery Timeout	The time that has to pass before a port in the <i>error-disabled</i> state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).



The **Managed Switch** implements the Rapid Spanning Protocol as the default spanning tree protocol. While selecting “**Compatibles**” mode, the system uses the RSTP (802.1w) to compatible and co work with another STP (802.1D)’s BPDU control packet.

Buttons



: Click to save changes.



: Click to undo any changes made locally and revert to previously saved values.

4.7.3 Bridge Status

This page provides a status overview for all STP bridge instances.

The displayed table contains a row for each STP bridge instance, where the column displays the following information: The Bridge Status screen in [Figure 4-7-5](#) appears.

STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00-00:6F:10:30:00	80:00-00:6F:10:30:00	-	0	Steady	-

Auto-refresh ☐ Refresh

Figure 4-7-5: STP Bridge Status Page Screenshot

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 <i>root</i> 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 last Topology Change occurred.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.7.4 CIST Port Configuration

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. The CIST Port Configuration screen in [Figure 4-7-6](#) appears.

STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	<input type="checkbox"/>	<All>		<All>	<All>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<All>
1	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
11	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
12	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
13	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
14	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
15	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
16	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
17	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
18	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
19	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
20	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
21	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
22	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
23	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
24	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
25	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
26	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
27	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
28	<input type="checkbox"/>	Auto		128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto


Figure 4-7-6 : STP CIST Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical STP port.
• STP Enabled	Controls whether RSTP is enabled on this switch port, * means to select all ports of Managed Switch.
• Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. All means all ports will have one specific setting.
• 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 All means all ports will have one specific setting.
• operEdge (state flag)	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having <i>operEdge</i> true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.
• Admin Edge	Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized). All means all ports will have one specific setting.
• Auto Edge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.
• Restricted Role	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard .
• Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network

	administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.
• BPDU Guard	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
• Point-to-Point	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. A transition to the forwarding state is faster for point-to-point LANs than for shared media. All means all ports will have one specific setting.

Buttons

: Click to save changes.

: Click 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 values shown below. 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 802.1w standard exceeds 65,535, the default is set to 65,535.

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

Table 4-7-1: Recommended STP Path Cost Range

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

Table 4-7-2: Recommended 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

Table 4-7-3: Default STP Path Costs

4.7.5 MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Priority screen in [Figure 4-7-7](#) appears.

MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<All>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

Save

Reset

Figure 4-7-7: MSTI Priority Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">MSTI	The bridge instance. The CIST is the default instance, which is always active.
<ul style="list-style-type: none">Priority	<p>The Configuration All with available values will assign to whole items.</p> <p>Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier, * means all MSTI items will have one priority setting.</p>

Buttons

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.7.6 MSTI Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Configuration screen in [Figure 4-7-8](#) appears.

MSTI Configuration

Add VLANs separated by spaces or comma.

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

Configuration Identification

Configuration Name	00-30-6f-20-10-00
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Save

Reset

Figure 4-7-8: MSTI Configuration Page Screenshot

The page includes the following fields:

Configuration Identification

Object	Description
<ul style="list-style-type: none">• Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters.
<ul style="list-style-type: none">• Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

Object	Description
<ul style="list-style-type: none">• MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
<ul style="list-style-type: none">• VLANs Mapped	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to <i>one</i> MSTI. A unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.7.7 MSTI Ports Configuration

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

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 MSTI Port Configuration screen in [Figure 4-7-9](#) & [Figure 4-7-10](#) appears.



Figure 4-7-9: MSTI Port Configuration Page Screenshot

The page includes the following fields:

MSTI Port Configuration

Object	Description
<ul style="list-style-type: none">Select MSTI	Select the bridge instance and set more detail configuration.

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto <input type="button" value="v"/>	<input type="text" value="128"/> <input type="button" value="v"/>

MSTI Normal Ports Configuration

Port	Path Cost	Priority
*	<All> <input type="button" value="v"/>	<All> <input type="button" value="v"/>
1	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
2	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
3	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
4	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
5	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
6	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
7	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
8	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
9	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
10	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
11	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
12	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
13	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
14	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
15	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
16	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
17	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
18	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
19	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
20	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
21	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
22	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
23	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
24	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
25	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
26	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
27	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>
28	Auto <input type="button" value="v"/>	128 <input type="button" value="v"/>


Figure 4-7-10: MST1 MSTI Port Configuration Page Screenshot


The page includes the following fields:


MSTx MSTI Port Configuration

Object	Description
• Port	The switch port number of the corresponding STP CIST (and MSTI) port.
• Path Cost	The Configuration All with available values will assign to whole items. Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. All means all ports will have one specific setting.
• Priority	The Configuration All with available values will assign to whole items. Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). All means all ports will have one specific setting.

Buttons

: Click to set MSTx configuration

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.7.8 Port Status

This page displays the STP CIST port status for port physical ports in the currently selected switch.
The STP Port Status screen in [Figure 4-7-11](#) appears.

STP Port Status			
Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-
13	Non-STP	Forwarding	-
14	Non-STP	Forwarding	-
15	Non-STP	Forwarding	-
16	Non-STP	Forwarding	-
17	Non-STP	Forwarding	-
18	Non-STP	Forwarding	-
19	Non-STP	Forwarding	-
20	Non-STP	Forwarding	-
21	Non-STP	Forwarding	-
22	Non-STP	Forwarding	-
23	Non-STP	Forwarding	-
24	Non-STP	Forwarding	-
25	Non-STP	Forwarding	-
26	Non-STP	Forwarding	-
27	Non-STP	Forwarding	-
28	Non-STP	Forwarding	-

Auto-refresh ☐ Refresh

Figure 4-7-11: STP Port Status Page Screenshot

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

	<ul style="list-style-type: none"> ■ BackupPort ■ RootPort ■ DesignatedPort
<ul style="list-style-type: none"> • CIST State 	<p>The current STP port state of the CIST port . The port state can be one of the following values:</p> <ul style="list-style-type: none"> ■ Disabled ■ Blocking ■ Learning ■ Forwarding ■ Non-STP
<ul style="list-style-type: none"> • Uptime 	<p>The time since the bridge port was last initialized.</p>

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

4.7.9 Port Statistics

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

The STP Port Statistics screen in [Figure 4-7-12](#) appears.

STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

Auto-refresh ☐ Refresh Clear

Figure 4-7-12: STP Statistics Page Screenshot

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

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Click to clear the information immediately.

4.8 Multicast

4.8.1 IGMP Snooping

The **Internet Group Management Protocol (IGMP)** lets host 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 the Internet Group Management Protocol (IGMP) Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (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 the '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 if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.

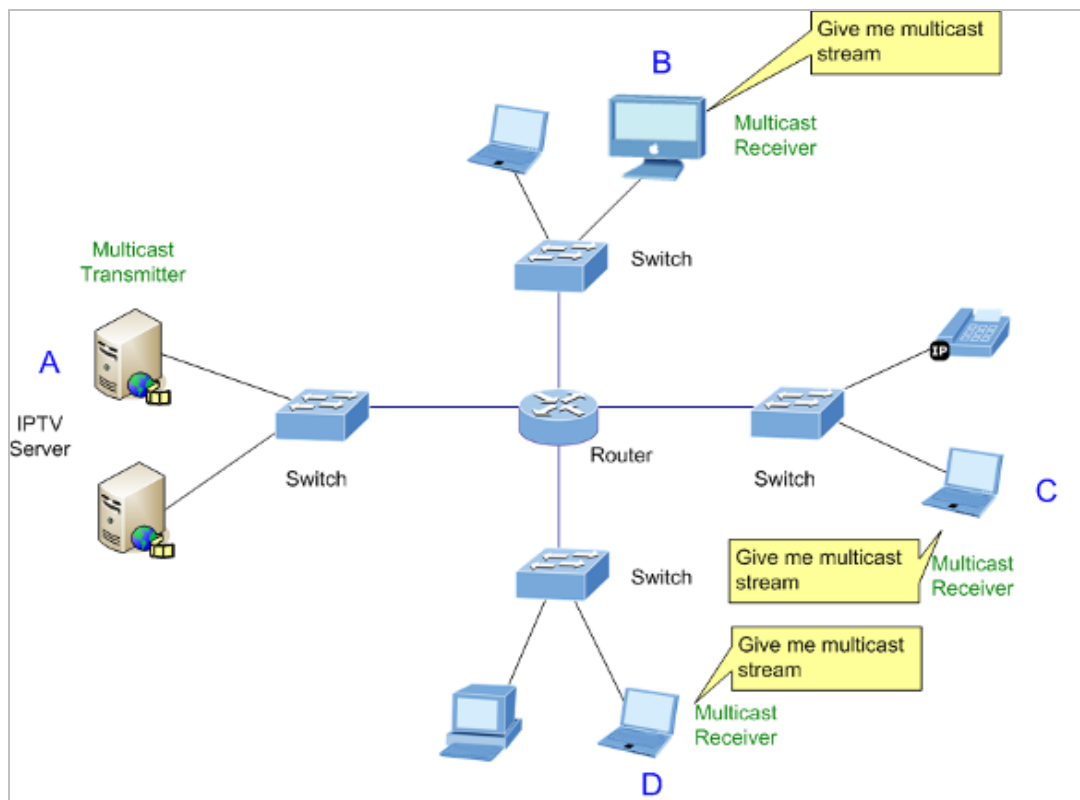


Figure 4-8-1: Multicast Service

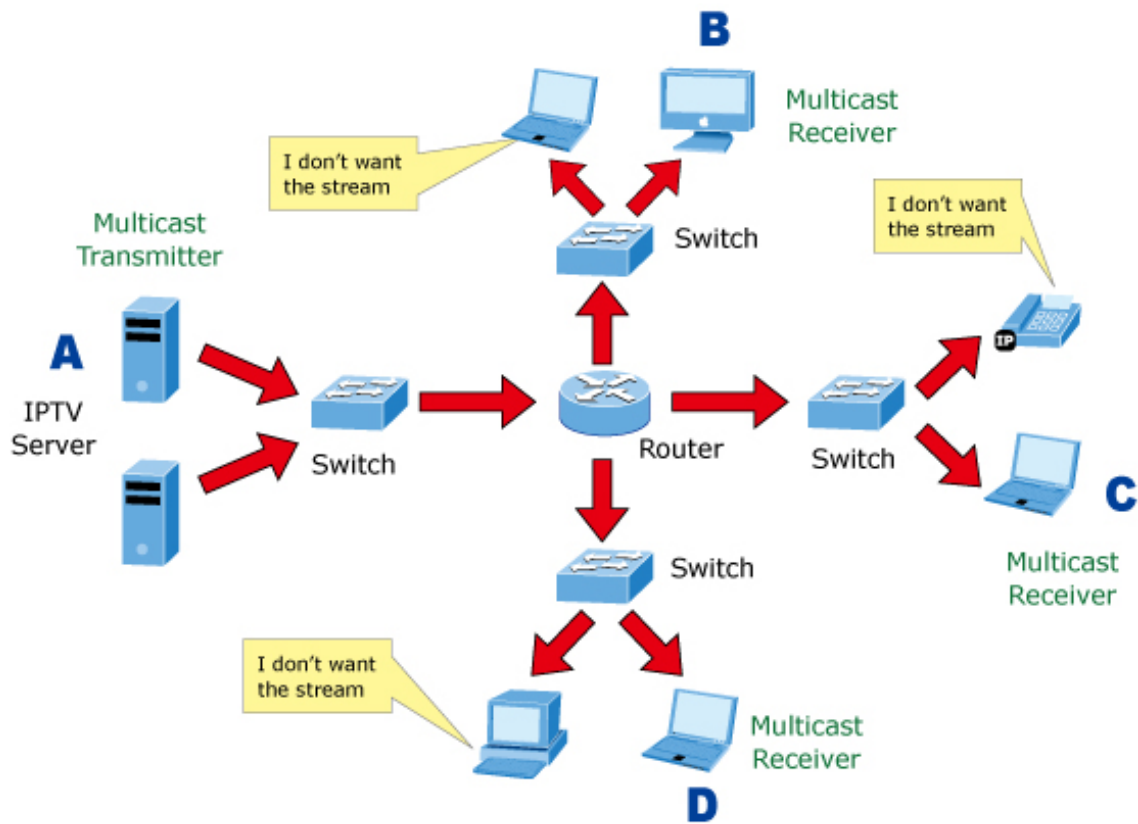


Figure 4-8-2: Multicast Flooding

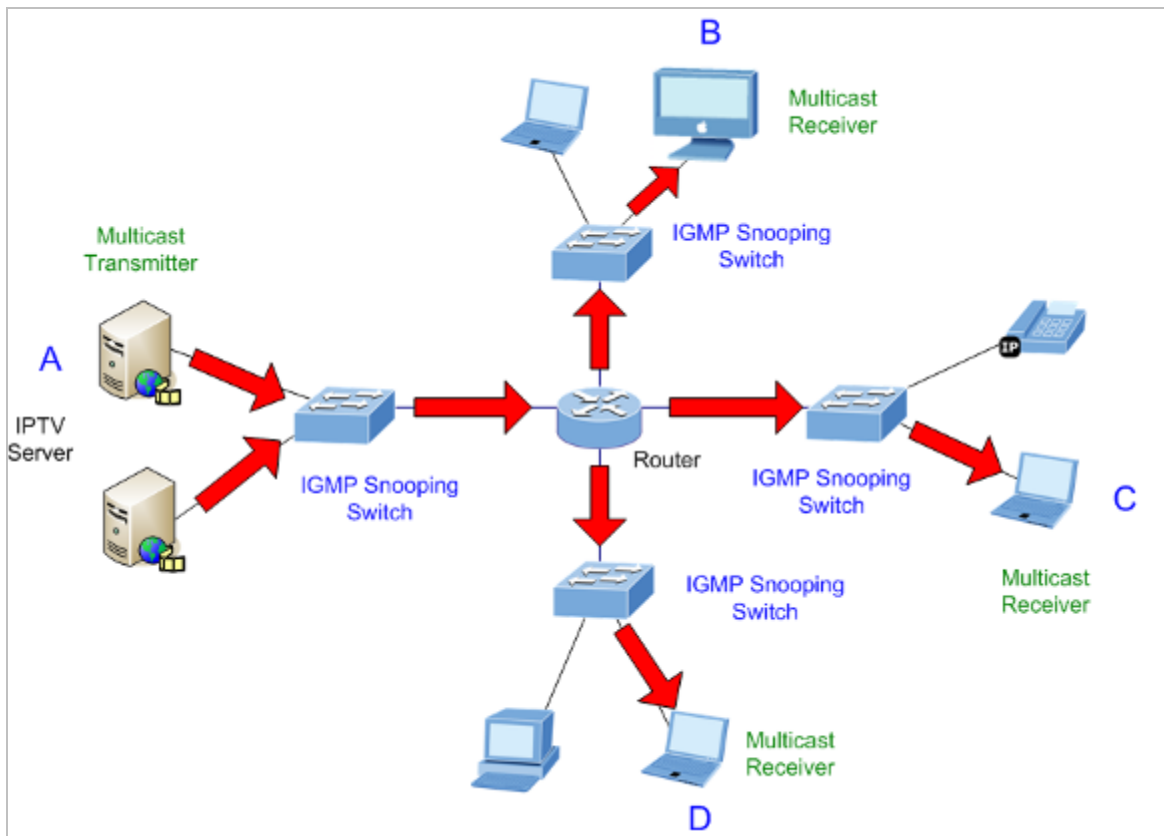


Figure 4-8-3: IGMP Snooping Multicast Stream Control

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

0	8	16	31
Type	Response Time	Checksum	
Group Address (all zeros if this is a query)			

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 enable 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 shown below:

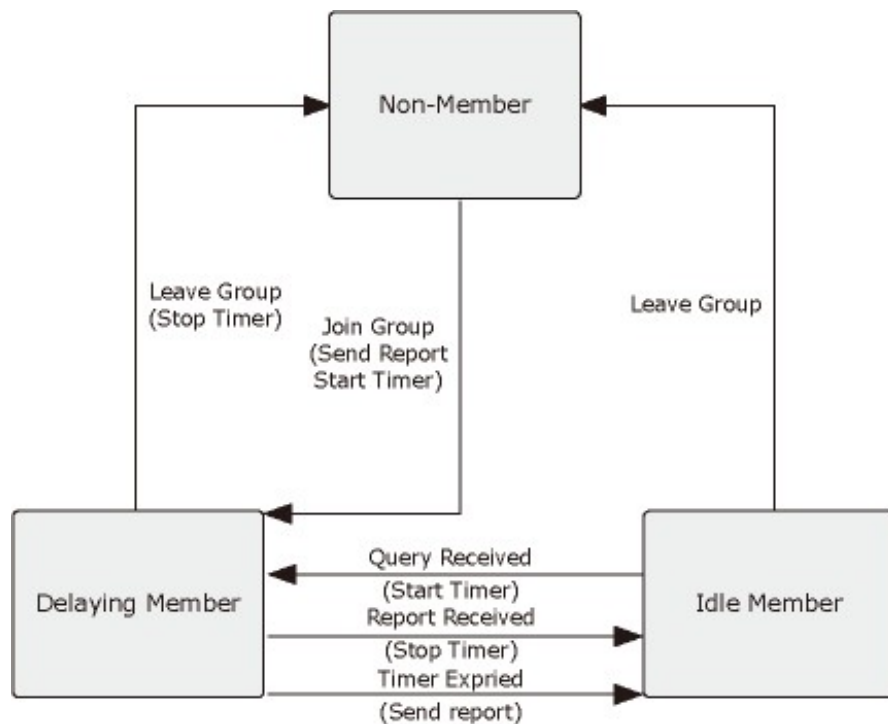
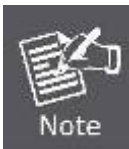


Figure 4-8-4: IGMP State Transitions

■ 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 on 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.



4.8.2 Profile Table

This page provides IPMC Profile related configurations. The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each. The Profile Table screen in Figure 4-8-5 appears.

IPMC Profile Configurations

Global Profile Mode Disabled

IPMC Profile Table Setting



Delete	Profile Name	Profile Description	Rule
Delete			 

Add New IPMC Profile

Apply Reset

Figure 4-8-5: IPMC Profile Configuration Page

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Global Profile Mode	Enable/Disable the Global IPMC Profile. System starts to do filtering based on profile settings only when the global profile mode is enabled.
<ul style="list-style-type: none">• Delete	Check to delete the entry. The designated entry will be deleted during the next save.
<ul style="list-style-type: none">• Profile Name	The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.
<ul style="list-style-type: none">• Profile Description	Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.
<ul style="list-style-type: none">• 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

Add New IPMC Profile : Click to add new IPMC profile. Specify the name and configure the new entry. Click "Save".

Apply : Click to apply changes

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

4.8.3 Address Entry

This page provides address range settings used in IPMC profile. The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create at maximum 128 address entries in the system. The Profile Table screen in [Figure 4-8-6](#) appears.

IGMP Snooping VLAN Configuration

Refresh << >>

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
--------	---------	------------------	--------------	---------------	----	----------	---------------	----------------	-----------

Add New IGMP VLAN

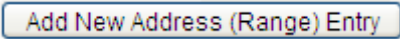
Save Reset


Figure 4-8-6: IPMC Profile Address Configuration Page

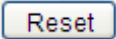
The page includes the following fields:

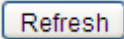
Object	Description
<ul style="list-style-type: none">Delete	<p>Check to delete the entry.</p> <p>The designated entry will be deleted during the next save.</p>
<ul style="list-style-type: none">Entry Name	<p>The name used for indexing the address entry table.</p> <p>Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.</p>
<ul style="list-style-type: none">Start Address	<p>The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.</p>
<ul style="list-style-type: none">End Address	<p>The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.</p>


Buttons


: Click to add new address range. Specify the name and configure the addresses. Click "Save".

: Click to apply changes

: Click to undo any changes made locally and revert to previously saved values.

: Refreshes the displayed table starting from the input fields.

: Updates the table starting from the first entry in the IPMC Profile Address Configuration.

: Updates the table, starting with the entry after the last entry currently displayed.

4.8.4 IGMP Snooping Configuration

This Page provides IGMP Snooping related configuration. The IGMP Snooping Configuration screen in [Figure 4-8-7](#) appears.

IGMP Snooping Configuration

Global Configuration

Snooping Enabled	<input checked="" type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<All> ▾	<input type="checkbox"/>	<All> ▾
1	Auto ▾	<input type="checkbox"/>	Unlimited ▾
2	Auto ▾	<input type="checkbox"/>	Unlimited ▾
3	Auto ▾	<input type="checkbox"/>	Unlimited ▾
4	Auto ▾	<input type="checkbox"/>	Unlimited ▾
5	Auto ▾	<input type="checkbox"/>	Unlimited ▾
6	Auto ▾	<input type="checkbox"/>	Unlimited ▾
7	Auto ▾	<input type="checkbox"/>	Unlimited ▾
8	Auto ▾	<input type="checkbox"/>	Unlimited ▾
21	Auto ▾	<input type="checkbox"/>	Unlimited ▾
22	Auto ▾	<input type="checkbox"/>	Unlimited ▾
23	Auto ▾	<input type="checkbox"/>	Unlimited ▾
24	Auto ▾	<input type="checkbox"/>	Unlimited ▾
25	Auto ▾	<input type="checkbox"/>	Unlimited ▾
26	Auto ▾	<input type="checkbox"/>	Unlimited ▾
27	Auto ▾	<input type="checkbox"/>	Unlimited ▾
28	Auto ▾	<input type="checkbox"/>	Unlimited ▾

Apply

Reset

Figure 4-8-7: IGMP Snooping Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Snooping Enabled	Enable the Global IGMP Snooping.
• Unregistered IPMCv4 Flooding Enabled	<p>Enable unregistered IPMCv4 traffic flooding.</p> <p>The flooding control takes effect only when IGMP Snooping is enabled.</p> <p>When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.</p>
• 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.
• Router Port	<p>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.</p> <ul style="list-style-type: none"> ■ Auto: Select "Auto" to have 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 you connect an IGMP multicast server or IP camera which applied with multicast protocol to the port. ■ None: The Managed Switch will not use the specified port as an IGMP Router port. The Managed Switch will not keep any record of an IGMP router being connected to this port. Use this mode when you connect other IGMP multicast servers directly on the non-querier Managed Switch and don't want the multicast stream be flood to 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.

Buttons

Apply : Click to apply changes

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

4.8.5 IGMP Snooping VLAN Configuration

Each Page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per Page" input field.

When first visited, the web Page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. The IGMP Snooping VLAN Configuration screen in [Figure 4-8-8](#) appears.

IGMP Snooping VLAN Configuration

Refresh << >>

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
--------	---------	------------------	------------------	-----------------	---------------	-----	----	----------	---------------	----------------	-----------

Add New IGMP VLAN

Apply Reset

Figure 4-8-8: IGMP Snooping VLAN ConfigurationPage Screenshot


The page includes the following fields:

Object	Description
• Delete	Check to delete the entry. The designated entry will be deleted during the next save.
• VLAN ID	The VLAN ID of the entry.
• IGMP Snooping 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. <div><div>■ When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.</div><div>■ When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value.</div></div>

	By default, this value will be 192.0.2.1
<ul style="list-style-type: none"> • Compatibility 	<p>Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3.</p> <p>Default compatibility value is IGMP-Auto.</p>
<ul style="list-style-type: none"> • PRI 	<p>(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.</p> <p>The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0</p>
<ul style="list-style-type: none"> • RV 	<p>Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network.</p> <p>The allowed range is 1 to 255, default robustness variable value is 2.</p>
<ul style="list-style-type: none"> • QI 	<p>Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.</p>
<ul style="list-style-type: none"> • QRI 	<p>Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries.</p> <p>The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).</p>
<ul style="list-style-type: none"> • LLQI (LMQI for IGMP) 	<p>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.</p> <p>The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).</p>
<ul style="list-style-type: none"> • URI 	<p>Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group.</p> <p>The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.</p>

Buttons

: Refreshes the displayed table starting from the "VLAN" input fields.

: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

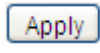


: Updates the table, starting with the entry after the last entry currently displayed.

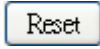


: Click to add new IGMP VLAN. Specify the VID and configure the new entry.

Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.



: Click to apply changes



: Click to undo any changes made locally and revert to previously saved values.

4.8.6 IGMP Group Port Group Filtering

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. 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.

IGMP filtering enables you to assign 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; but 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 IGMP Snooping Port Group Filtering Configuration screen in [Figure 4-8-9](#) appears.

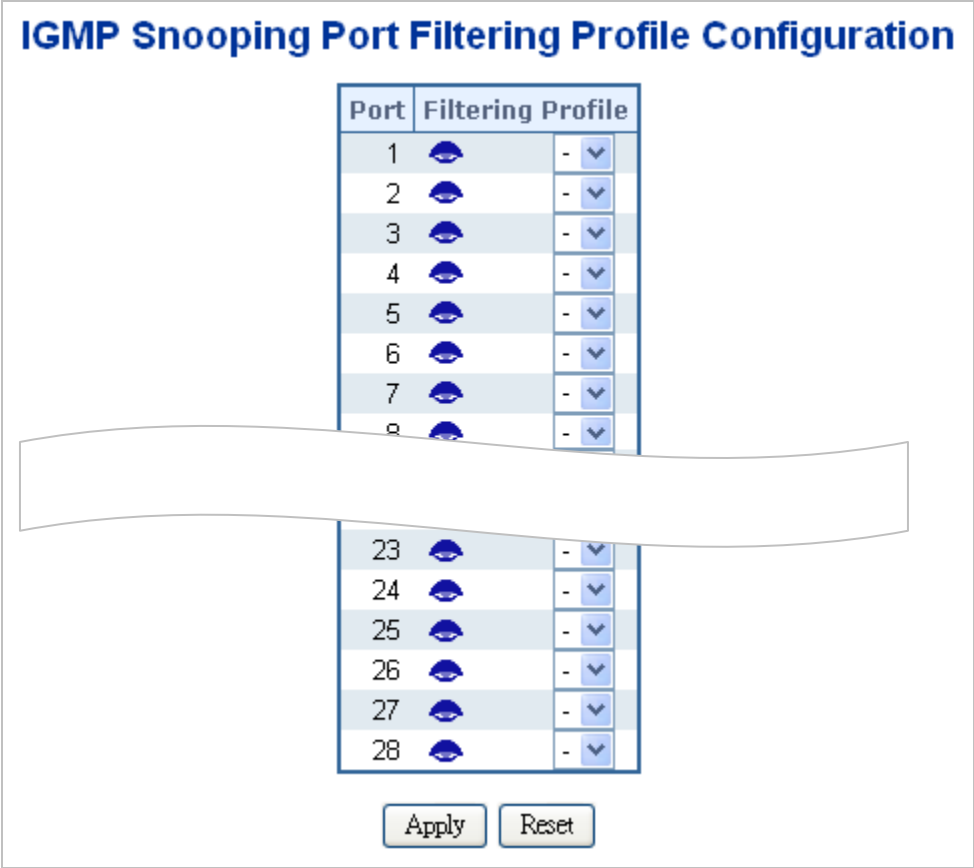
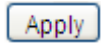


Figure 4-8-9: IGMP Snooping Filtering Profile Configuration Page Screenshot

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 to apply changes



: Click to undo any changes made locally and revert to previously saved values.

4.8.7 IGMP Snooping Status

This Page provides IGMP Snooping status. The IGMP Snooping Status screen in [Figure 4-8-10](#) appears.

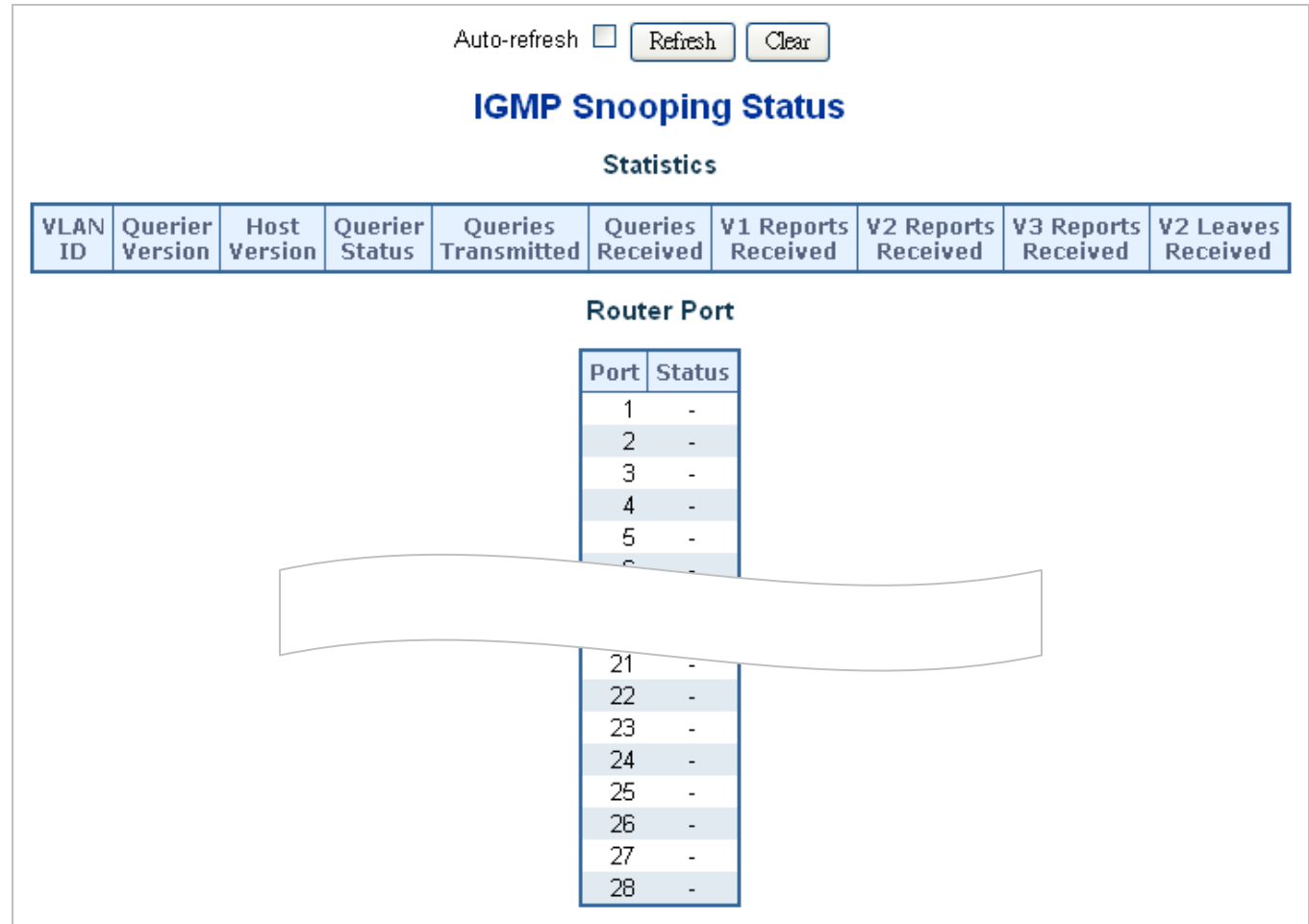


Figure 4-8-10: IGMP Snooping Status Page Screenshot


The Page includes the following fields:

Object	Description
<ul style="list-style-type: none">VLAN ID	The VLAN ID of the entry.
<ul style="list-style-type: none">Querier Version	Working Querier Version currently.
<ul style="list-style-type: none">Host Version	Working Host Version currently.
<ul style="list-style-type: none">Querier Status	Show the Querier status is "ACTIVE" or "IDLE".
<ul style="list-style-type: none">Querier Transmitted	The number of Transmitted Querier.
<ul style="list-style-type: none">Querier Received	The number of Received Querier.
<ul style="list-style-type: none">V1 Reports Received	The number of Received V1 Reports.
<ul style="list-style-type: none">V2 Reports Received	The number of Received V2 Reports.

• V3 Reports Received	The number of Received V3 Reports.
• V2 Leave Received	The number of Received V2 Leave.
• Router Port	<p>Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.</p> <p>Static denotes the specific port is configured to be a router port.</p> <p>Dynamic denotes the specific port is learnt to be a router port.</p> <p>Both denote the specific port is configured or learnt to be a router port.</p>
• Port	Switch port number.
• Status	Indicate whether specific port is a router port or not.

Buttons

: Click to refresh the Page immediately.

: Clears all Statistics counters.

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

4.8.8 IGMP Group Information

Entries in the IGMP Group Table are shown on this Page. The IGMP Group Table is sorted first by VLAN ID, and then by group. Each Page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per Page" input field. When first visited, the web Page will show the first 20 entries from the beginning of the IGMP Group Table. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table. The IGMP Groups Information screen in [Figure 4-8-11](#) appears.

IGMP Snooping Group Information

Auto-refresh ☐ Refresh << >>

Start from VLAN and group Address with entries per page.

		Port Members																											
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No more entries																													

Figure 4-8-9: IGMP Snooping Groups Information Page Screenshot

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

- Auto-refresh ☐: Automatic refresh occurs every 3 seconds.
- Refresh: Refreshes the displayed table starting from the input fields.
- <<: Updates the table, starting with the first entry in the IGMP Group Table.
- >>: Updates the table, starting with the entry after the last entry currently displayed.

4.8.9 IGMPv3 Information

Entries in the IGMP SSM Information Table are shown on this Page. The IGMP SSM Information Table is sorted first by VLAN ID, then by group, and then by Port No. Different source addresses belong to the same group are treated as single entry.

Each Page shows up to 99 entries from the IGMP SSM (Source Specific Multicast) Information table, default being 20, selected through the "entries per Page" input field. When first visited, the web Page will show the first 20 entries from the beginning of the IGMP SSM Information Table.

The "**Start from VLAN**", and "**Group**" input fields allow the user to select the starting point in the IGMP SSM Information Table. The IGMPv3 Information screen in [Figure 4-8-12](#) appears.

IGMP SSM Information

Auto-refresh ☐

Start from VLAN and Group with entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Figure 4-8-12: IGMP SSM Information Page Screenshot


The Page includes the following fields:


Object	Description
• VLAN ID	VLAN ID of the group.
• Group	Group address of the group displayed.
• Port	Switch port number.
• Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
• Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
• Type	Indicates the Type. It can be either Allow or Deny.
• Hardware Filter/Switch	Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Buttons

Auto-refresh ☐: Check this box to enable an automatic refresh of the Page at regular intervals.

: Click to refresh the Page immediately.

: Updates the table, starting with the first entry in the IGMP Group Table.

: Updates the table, starting with the entry after the last entry currently displayed.

4.8.10 MLD Snooping Configuration

This Page provides MLD Snooping related configuration. The MLD Snooping Configuration screen in [Figure 4-8-13](#) appears.

MLD Snooping Configuration

Global Configuration	
Snooping Enabled	<input checked="" type="checkbox"/>
Unregistered IPMCv6 Flooding Enabled	<input type="checkbox"/>
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<All>	<input type="checkbox"/>	<All>
1	Auto	<input type="checkbox"/>	Unlimited
2	Auto	<input type="checkbox"/>	Unlimited
3	Auto	<input type="checkbox"/>	Unlimited
4	Auto	<input type="checkbox"/>	Unlimited
5	Auto	<input type="checkbox"/>	Unlimited
6	Auto	<input type="checkbox"/>	Unlimited
7	Auto	<input type="checkbox"/>	Unlimited
8	Auto	<input type="checkbox"/>	Unlimited
23	Auto	<input type="checkbox"/>	Unlimited
24	Auto	<input type="checkbox"/>	Unlimited
25	Auto	<input type="checkbox"/>	Unlimited
26	Auto	<input type="checkbox"/>	Unlimited
27	Auto	<input type="checkbox"/>	Unlimited
28	Auto	<input type="checkbox"/>	Unlimited

ApplyReset

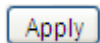
Figure 4-8-13: MLD Snooping Configuration Page Screenshot

The Page includes the following fields:

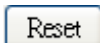
Object	Description
• Snooping Enabled	Enable the Global MLD Snooping.
• Unregistered IPMCv6 Flooding enabled	Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled.

	When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.
• MLD SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
• Leave Proxy 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 will act as a router port. The allowed selection is Auto , Fix , Fone , default compatibility value is Auto.
• 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.

Buttons



: Click to apply changes



: Click to undo any changes made locally and revert to previously saved values.

4.8.11 MLD Snooping VLAN Configuration

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

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. The MLD Snooping VLAN Configuration screen in [Figure 4-8-14](#) appears.

MLD Snooping VLAN Configuration

Refresh |<< >>

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
--------	---------	------------------	------------------	---------------	-----	----	----------	---------------	----------------	-----------

Add New MLD VLAN

Apply Reset

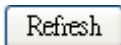
Figure 4-8-14: IGMP Snooping VLAN Configuration Page Screenshot

The Page includes the following fields:

Object	Description
• Delete	Check to delete the entry. The designated entry will be deleted during the next save.
• VLAN ID	The VLAN ID of the entry.
• MLD Snooping Enable	Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.
• Querier Election	Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.
• Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto , Forced MLDv1 , Forced MLDv2 , default compatibility value is MLD-Auto.
• PRI	(PRI) Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0
• RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255 , default robustness variable value is 2 .

<ul style="list-style-type: none"> • QI 	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.
<ul style="list-style-type: none"> • QRI 	Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
<ul style="list-style-type: none"> • 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).
<ul style="list-style-type: none"> • 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



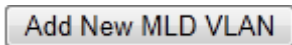
: Refreshes the displayed table starting from the "VLAN" input fields.



: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.




: Updates the table, starting with the entry after the last entry currently displayed.




: Click to add new MLD VLAN. Specify the VID and configure the new entry.

Click "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.



: Click to apply changes



: Click to undo any changes made locally and revert to previously saved values.

4.8.12 MLD Snooping Port Group Filtering

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. 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.

MLD filtering enables you to assign 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; but 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 MLD Snooping Port Group Filtering Configuration screen in [Figure 4-8-15](#) appears.

Port	Filtering Profile
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

23	-
24	-
25	-
26	-
27	-
28	-

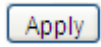
Apply Reset

Figure 4-8-15: MLD Snooping Port Group Filtering Configuration Page Screenshot

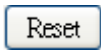
The Page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	The logical port for the settings.
<ul style="list-style-type: none"> • Filtering Group 	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 to apply changes



: Click to undo any changes made locally and revert to previously saved values.

4.8.13 MLD Snooping Status

This Page provides MLD Snooping status. The IGMP Snooping Status screen in [Figure 4-8-16](#) appears.

Auto-refresh ☐ Refresh Clear

MLD Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
---------	-----------------	--------------	----------------	---------------------	------------------	---------------------	---------------------	--------------------

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
23	-
24	-
25	-
26	-
27	-
28	-

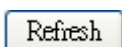
Figure 4-8-16: MLD Snooping Status Page Screenshot

The Page includes the following fields:

Object	Description
• VLAN ID	The VLAN ID of the entry.
• Querier Version	Working Querier Version currently.
• Host Version	Working Host Version currently.
• Querier Status	Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
• Querier Transmitted	The number of Transmitted Querier.
• Querier Received	The number of Received Querier.

• V1 Reports Received	The number of Received V1 Reports.
• V2 Reports Received	The number of Received V2 Reports.
• V1 Leave Received	The number of Received V1 Leaves.
• Router Port	<p>Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.</p> <p>Static denotes the specific port is configured to be a router port.</p> <p>Dynamic denotes the specific port is learnt to be a router port.</p> <p>Both denote the specific port is configured or learnt to be a router port.</p>
• Port	Switch port number.
• Status	Indicates whether specific port is a router port or not.


Buttons



: Click to refresh the Page immediately.



: Clears all Statistics counters.

Auto-refresh : Automatic refresh occurs every 3 seconds.

4.8.14 MLD Group Information

Entries in the MLD Group Table are shown on this Page. The MLD Group Table is sorted first by VLAN ID, and then by group. Each Page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per Page" input field. When first visited, the web Page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. The MLD Groups Informatino screen in [Figure 4-8-17](#) appears.

MLD Snooping Group Information

Auto-refresh ☐

Refresh << >>

Start from VLAN and group Address with entries per page.

		Port Members																											
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No more entries																													

Figure 4-8-17: MLD Snooping Groups Information Page Screenshot

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

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

Refresh

: Click to refresh the Page immediately.

<<

: Updates the table, starting with the first entry in the IGMP Group Table.

>>

: Updates the table, starting with the entry after the last entry currently displayed.

4.8.15 MLDv2 Information

Entries in the MLD SFM Information Table are shown on this Page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry. Each Page shows up to 99 entries from the MLD SFM Information table, default being 20, selected through the "entries per Page" input field. When first visited, the web Page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD SFM Information Table.

The MLDv2 Information screen in [Figure 4-8-18](#) appears.

MLD SFM Information

Auto-refresh ☐

Start from VLAN and Group with entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Figure 4-8-18: MLD SSM Information Page Screenshot

The Page includes the following fields:

Object	Description
• VLAN ID	VLAN ID of the group.
• Group	Group address of the group displayed.
• Port	Switch port number.
• Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
• Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
• Type	Indicates the Type. It can be either Allow or Deny.
• Hardware Filter/Switch	Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

: Refreshes the displayed table starting from the input fields.

: Updates the table starting from the first entry in the MLD SFM Information Table.



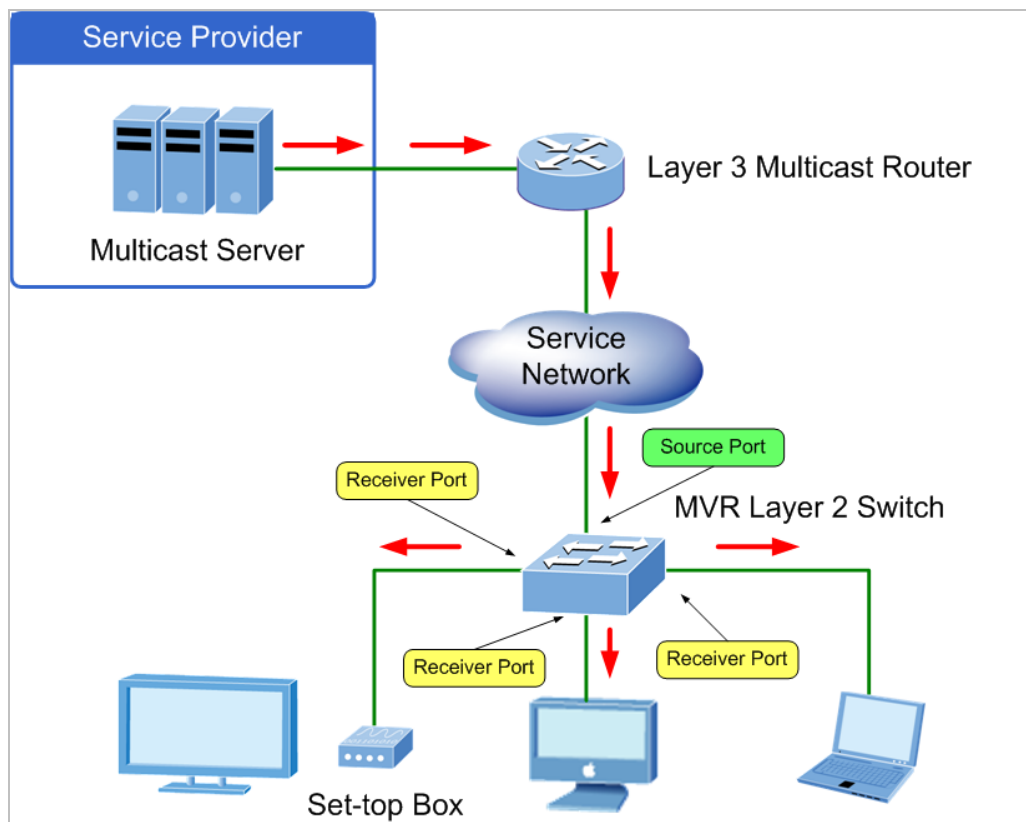
: Updates the table, starting with the entry after the last entry currently displayed.

4.8.16 MVR (Multicast VLAN Registration)

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

- In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream.
- Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address.
- Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

It is allowed to create at maximum 8 MVR VLANs with corresponding channel settings for each Multicast VLAN. There will be totally at maximum 256 group addresses for channel settings.



This Page provides MVR related configuration. The MVR screen in [Figure 4-8-19](#) appears.

MVR Configurations

MVR Mode Disabled ▾

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
--------	---------	----------	--------------	------	---------	----------	------	---------------------------

Add New MVR VLAN

Immediate Leave Setting

Port	Immediate Leave
*	<All> ▾
1	Disabled ▾
2	Disabled ▾
3	Disabled ▾
4	Disabled ▾
5	Disabled ▾
6	Disabled ▾
7	Disabled ▾
8	Disabled ▾

23	Disabled ▾
24	Disabled ▾
25	Disabled ▾
26	Disabled ▾
27	Disabled ▾
28	Disabled ▾

Apply

Reset

Figure 4-8-19: MVR Configuration Page Screenshot




The Page includes the following fields:

Object	Description
<ul style="list-style-type: none"> MVR Mode 	<p>Enable/Disable the Global MVR.</p> <p>The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping.</p> <p>It is suggested to enable Unregistered Flooding control when the MVR group table is full.</p>

• Delete	Check to delete the entry. The designated entry will be deleted during the next save.
• MVR VID	Specify the Multicast VLAN ID. Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.
• MVR Name	MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 16. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.
• 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, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.
• Mode	Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.
• Tagging	Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.
• Priority	Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.
• LLQI	Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.
• Interface Channel Setting	When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profile selected for designated interface channel is not allowed to have overlapped permit group address.
• 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 MVR operations.

	<ul style="list-style-type: none"> ■ 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. <p>Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.</p> <p>Select the port role by clicking the Role symbol to switch the setting.</p> <p>I indicates Inactive; S indicates Source; R indicates Receiver</p> <p>The default Role is Inactive.</p>
• Immediate Leave	Enable the fast leave on the port.

Buttons

- : Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Save"
- : Click to apply changes
- : Click to undo any changes made locally and revert to previously saved values.

4.8.17 MVR Status

This Page provides MVR status. The MVR Status screen in [Figure 4-8-20](#) appears.

MVR Statistics						
VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
No more entries						
Auto-refresh <input type="checkbox"/> <input type="button" value="Refresh"/> <input type="button" value="Clear"/>						

Figure 4-8-20: MVR Status Page Screenshot

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 to refresh the Page immediately.

: Clears all Statistics counters.

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

4.8.18 MVR Groups Information

Entries in the MVR Group Table are shown on this Page. The MVR Group Table is sorted first by VLAN ID, and then by group. Each Page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per Page" input field. When first visited, the web Page will show the first 20 entries from the beginning of the MVR Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MVR Group Table. The MVR Groups Information screen in [Figure 4-8-21](#) appears.

MVR Channels (Groups) Information

Auto-refresh ☐ Refresh << >>

Start from VLAN and Group Address with entries per page.

		Port Members																											
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No more entries																													

Figure 4-8-21: MVR Groups Information Page Screenshot

The Page includes the following fields:

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

Buttons

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

<<: Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.8.19 MVR SFM Information

Entries in the MVR SFM Information Table are shown on this Page. The MVR **SFM (Source-Filtered Multicast)** Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Each Page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the "entries per Page" input field. When first visited, the web Page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information Table. The MVR SFM Information screen in [Figure 4-8-22](#) appears.

MVR SFM Information

Auto-refresh ☐

Start from VLAN and Group Address with entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Figure 4-8-22: MVR SFM Information Page Screenshot

The Page includes the following fields:

Object	Description
• VLAN ID	VLAN ID of the group.
• Group	Group address of the group displayed.
• Port	Switch port number.
• Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
• Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.
• Type	Indicates the Type. It can be either Allow or Deny.
• Hardware Filter / Switch	Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

Buttons

Auto-refresh ☐: Automatic refresh occurs every 3 seconds.

: Refreshes the displayed table starting from the input fields.



: Updates the table starting from the first entry in the MVR SFM Information Table.

4.9 Quality of Service

4.9.1 Understand QoS

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

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic. You can use QoS on your system to:

- Control a wide variety of network traffic by:
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage 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 Switch then groups classified traffic in order to schedule them with the appropriate service level.
- **DiffServ Code Point (DSCP)** — is the 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 that will be 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 Switch will treat certain types of traffic. Rules are associated with a QoS Profile (see above).

To implement QoS on your network, you need to carry out 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 Switch.
3. Create a QoS profile which associates a service level and a classifier.

4. Apply a QoS profile to a port(s).

4.9.2 Port Policing

This page allows you to configure the Policer settings for all switch ports. The Port Policing screen in [Figure 4-9-1](#) appears.

QoS Ingress Port Policers


Port	Enabled	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<All> ▼	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps ▼	
6	<input type="checkbox"/>	500	kbps ▼	
7	<input type="checkbox"/>	500	kbps ▼	
8	<input type="checkbox"/>	500	kbps ▼	
9	<input type="checkbox"/>	500	kbps ▼	
10	<input type="checkbox"/>	500	kbps ▼	
11	<input type="checkbox"/>	500	kbps ▼	
12	<input type="checkbox"/>	500	kbps ▼	
13	<input type="checkbox"/>	500	kbps ▼	
14	<input type="checkbox"/>	500	kbps ▼	
15	<input type="checkbox"/>	500	kbps ▼	
16	<input type="checkbox"/>	500	kbps ▼	
17	<input type="checkbox"/>	500	kbps ▼	
18	<input type="checkbox"/>	500	kbps ▼	
19	<input type="checkbox"/>	500	kbps ▼	
20	<input type="checkbox"/>	500	kbps ▼	
21	<input type="checkbox"/>	500	kbps ▼	
22	<input type="checkbox"/>	500	kbps ▼	
23	<input type="checkbox"/>	500	kbps ▼	
24	<input type="checkbox"/>	500	kbps ▼	
25	<input type="checkbox"/>	500	kbps ▼	
26	<input type="checkbox"/>	500	kbps ▼	
27	<input type="checkbox"/>	500	kbps ▼	
28	<input type="checkbox"/>	500	kbps ▼	


Figure 4-9-1: QoS Ingress Port Policers Page Screenshot

The page includes the following fields:

Object	Description
• Port	The port number for which the configuration below applies.
• Enabled	Controls whether the policer is enabled on this switch port, * means selection all ports of Managed Switch.
• 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	The Configuration All with available options will assign to whole ports. Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps. The default value is "kbps". All means all ports will have one specific setting.
• 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 to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.9.3 Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports. The Port Shapping screen in [Figure 4-9-2](#) appears.

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
11	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
14	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
16	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
17	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
18	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
19	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
20	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
21	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
22	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
23	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
24	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
25	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
26	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
27	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
28	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

Figure 4-9-2: QoS Egress Port Shapers Page Screenshot

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 in order to configure the shapers. For more detail, please refer to chapter 4.9.3.1.
• 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".

4.9.3.1 QoS Egress Port Schedule and Shapers

The Port Scheduler and Shapers for a specific port are configured on this page. The QoS Egress Port Schedule and Shaper screen in [Figure 4-9-3](#) appears.

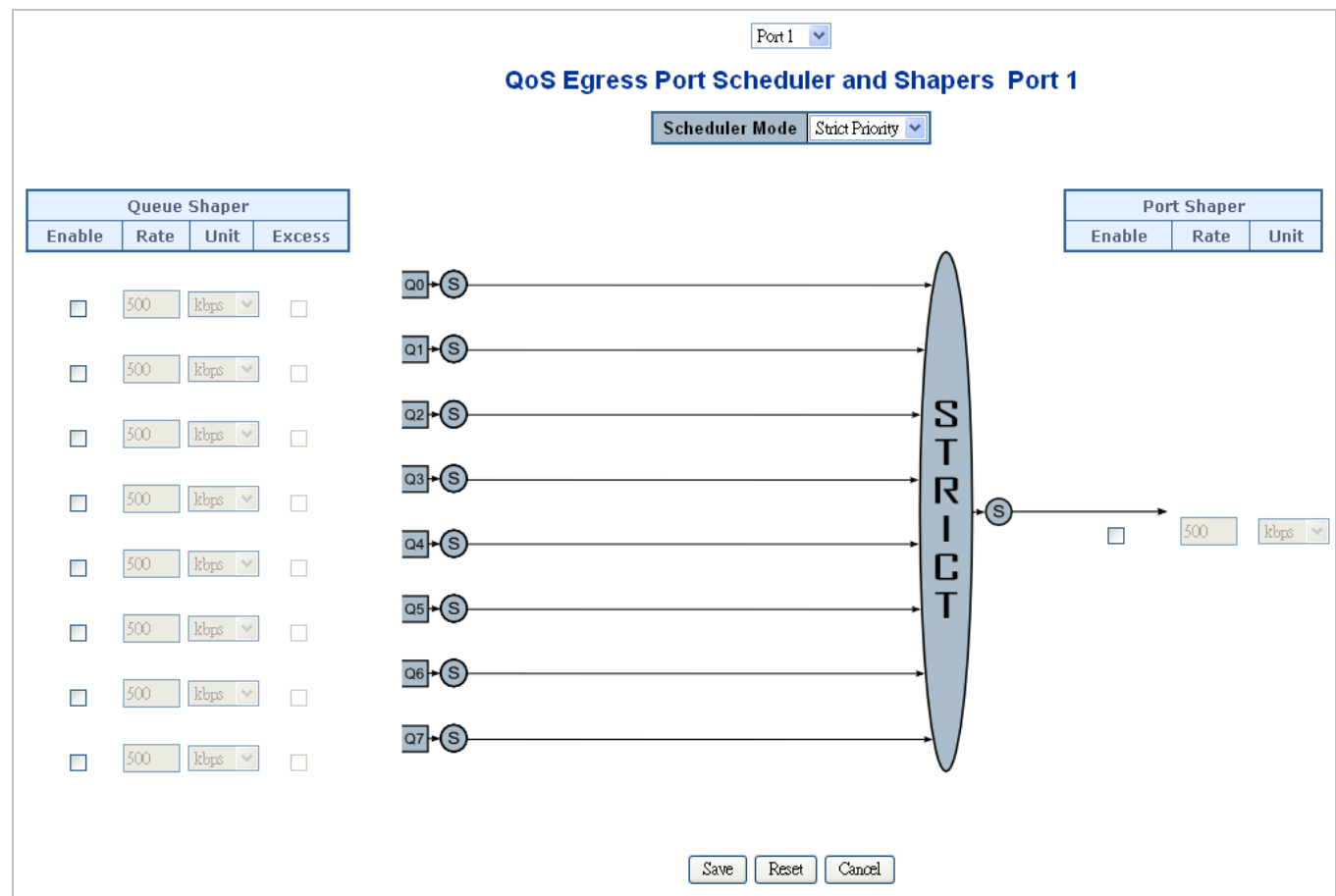


Figure 4-9-3: QoS Egress Port Schedule and Shapers Page Screenshot

The page includes the following fields:

Object	Description
• Schedule 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 1-3300 when the " Unit " is " Mbps ".
• Queue Shaper Unit	Controls the unit of measure for the queue shaper rate as " kbps " or " Mbps ". The default value is " kbps ".
• Queue Shaper Excess	Controls whether the queue is allowed to use excess bandwidth.

• Queue Scheduler Weight	Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if " Scheduler Mode " is set to " Weighted ".
• Queue Scheduler Percent	Shows the weight in percent for this queue. This parameter is only shown if " Scheduler Mode " is set to " Weighted ".
• Port Shaper Enable	Controls whether the port shaper is enabled for this switch port.
• Port Shaper Rate	Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the " Unit " is " kbps ", and it is restricted to 1-3300 when the " Unit " is " Mbps ".
• Port Shaper Unit	Controls the unit of measure for the port shaper rate as " kbps " or " Mbps ". The default value is " kbps ".

Buttons

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

Cancel

: Click to undo any changes made locally and return to the previous page.

4.9.4 Port Classification

This page allows you to configure the basic QoS Ingress Classification settings for all switch ports. The Port Classification screen in [Figure 4-9-4](#) appears.

QoS Ingress Port Classification


Port	QoS Class	DP Level	PCP	DEI	Tag Class.	DSCP Based
*	<All> ▼	<All> ▼	<All> ▼	<All> ▼		<input type="checkbox"/>
1	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
2	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
3	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
4	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
5	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
6	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
7	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
8	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
9	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
10	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
11	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
12	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
13	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
14	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
15	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
16	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
17	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
18	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
19	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
20	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
21	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
22	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
23	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
24	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
25	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
26	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
27	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
28	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>

Figure 4-9-4 : QoS Ingress Port Classification Page Screenshot

The page includes the following fields:

Object	Description
• Port	The port number for which the configuration below applies.
• QoS Class	<p>The Configuration All with available values will assign to whole ports.</p> <p>Controls the default QoS class, i.e., the QoS class for frames not classified in any other way. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.</p> <p>All means all ports will have one specific setting.</p>
• DP Level	<p>The Configuration All with available values will assign to whole ports.</p> <p>Controls the default DP level, i.e., the DP level for frames not classified in any other way.</p> <p>All means all ports will have one specific setting.</p>
• PCP	<p>The Configuration All with available values will assign to whole ports.</p> <p>Controls the default PCP for untagged frames.</p> <p>All means all ports will have one specific setting.</p>
• DEI	<p>The Configuration All with available values will assign to whole ports.</p> <p>Controls the default DEI for untagged frames.</p> <p>All means all ports will have one specific setting.</p>
• Tag Class	<p>Shows the classification mode for tagged frames on this port.</p> <ul style="list-style-type: none">■ Disabled: Use default QoS class and DP level for tagged frames.■ Enabled: Use mapped versions of PCP and DEI for tagged frames. <p>Click on the mode in order to configure the mode and/or mapping.</p> <p>For more detail information, please refer to chapter 4.9.3.1.</p>
• DSCP Based	Click to Enable DSCP Based QoS Ingress Port Classification.

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.9.4.1 QoS Ingress Port Tag Classification

The clasification modes for tagged frames are configured on this page. The QoS Ingress Port Tag Classification screen in [Figure 4-9-5](#) appears.

Port 1

QoS Ingress Port Tag Classification Port 1

Tagged Frames Settings

Tag Classification Disabled

(PCP, DEI) to (QoS Class, DP Level) Mapping

PCP	DEI	QoS Class	DP Level
*	*	<All>	<All>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

SaveResetCancel

Figure 4-9-5 : QoS Ingress Port Tag Classification Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">Tag Classification	Controls the classification mode for tagged frames on this port. <ul style="list-style-type: none">■ Disabled: Use default QoS class and DP level for tagged frames.■ Enabled: Use mapped versions of PCP and DEI for tagged frames.
<ul style="list-style-type: none">(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

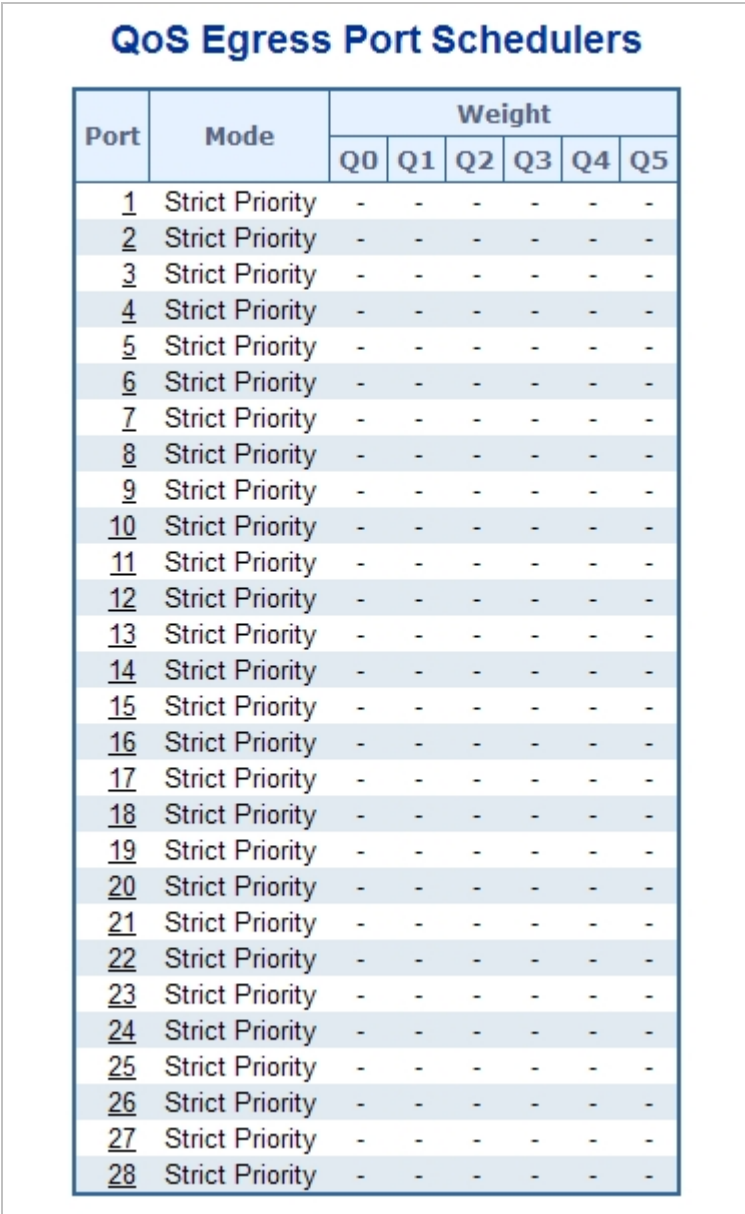
Save: Click to save changes.

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

Cancel: Return to the previous page.

4.9.5 Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports. The Port Scheduler screen in [Figure 4-9-6](#) appears.



Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
<u>1</u>	Strict Priority	-	-	-	-	-	-
<u>2</u>	Strict Priority	-	-	-	-	-	-
<u>3</u>	Strict Priority	-	-	-	-	-	-
<u>4</u>	Strict Priority	-	-	-	-	-	-
<u>5</u>	Strict Priority	-	-	-	-	-	-
<u>6</u>	Strict Priority	-	-	-	-	-	-
<u>7</u>	Strict Priority	-	-	-	-	-	-
<u>8</u>	Strict Priority	-	-	-	-	-	-
<u>9</u>	Strict Priority	-	-	-	-	-	-
<u>10</u>	Strict Priority	-	-	-	-	-	-
<u>11</u>	Strict Priority	-	-	-	-	-	-
<u>12</u>	Strict Priority	-	-	-	-	-	-
<u>13</u>	Strict Priority	-	-	-	-	-	-
<u>14</u>	Strict Priority	-	-	-	-	-	-
<u>15</u>	Strict Priority	-	-	-	-	-	-
<u>16</u>	Strict Priority	-	-	-	-	-	-
<u>17</u>	Strict Priority	-	-	-	-	-	-
<u>18</u>	Strict Priority	-	-	-	-	-	-
<u>19</u>	Strict Priority	-	-	-	-	-	-
<u>20</u>	Strict Priority	-	-	-	-	-	-
<u>21</u>	Strict Priority	-	-	-	-	-	-
<u>22</u>	Strict Priority	-	-	-	-	-	-
<u>23</u>	Strict Priority	-	-	-	-	-	-
<u>24</u>	Strict Priority	-	-	-	-	-	-
<u>25</u>	Strict Priority	-	-	-	-	-	-
<u>26</u>	Strict Priority	-	-	-	-	-	-
<u>27</u>	Strict Priority	-	-	-	-	-	-
<u>28</u>	Strict Priority	-	-	-	-	-	-

Figure 4-9-6: QoS Egress Port Schedule Page Screenshot

The page includes the following fields:

Object	Description
--------	-------------

• Port	<p>The logical port for the settings contained in the same row.</p> <p>Click on the port number in order to configure the schedulers.</p> <p>For more detail, please refer to chapter 4.9.5.1.</p>
• Mode	Shows the scheduling mode for this port.
• Q0 ~ Q5	Shows the weight for this queue and port.

4.9.6 Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports. The Port Tag Remarking screen in [Figure 4-9-7](#) appears.

QoS Egress Port Tag Remarking	
Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified
15	Classified
16	Classified
17	Classified
18	Classified
19	Classified
20	Classified
21	Classified
22	Classified
23	Classified
24	Classified
25	Classified
26	Classified
27	Classified
28	Classified

Figure 4-9-7: QoS Egress Port Tag Remarking Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	<p>The logical port for the settings contained in the same row.</p> <p>Click on the port number in order to configure tag remarking.</p> <p>For more detail, please refer to chapter 4.9.6.1.</p>
<ul style="list-style-type: none"> • Mode 	<p>Shows the tag remarking mode for this port.</p> <ul style="list-style-type: none"> ■ Classified: Use classified PCP/DEI values. ■ Default: Use default PCP/DEI values. ■ Mapped: Use mapped versions of QoS class and DP level.

4.9.6.1 QoS Egress Port Tag Remarking


The QoS Egress Port Tag Remarking for a specific port are configured on this page. The QoS Egress Port Tag Remarking screen in [Figure 4-9-8](#) appears.

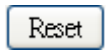
Figure 4-9-8: QoS Egress Port Tag Remarking Page Screenshot

The page includes the following fields:

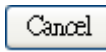
Object	Description
<ul style="list-style-type: none"> • Mode 	<p>Controls the tag remarking mode for this port.</p> <ul style="list-style-type: none"> ■ Classified: Use classified PCP/DEI values. ■ Default: Use default PCP/DEI values. ■ Mapped: Use mapped versions of QoS class and DP level.
<ul style="list-style-type: none"> • PCP/DEI Configuration 	Controls the default PCP and DEI values used when the mode is set to Default .
<ul style="list-style-type: none"> • (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 to save changes.



: Click to undo any changes made locally and revert to previously saved values.



: Click to undo any changes made locally and return to the previous page.

4.9.7 Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports. The Port DSCP screen in [Figure 4-9-9](#) appears.

QoS Port DSCP Configuration


Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<All> ▼	<All> ▼
1	<input type="checkbox"/>	Disable ▼	Disable ▼
2	<input type="checkbox"/>	Disable ▼	Disable ▼
3	<input type="checkbox"/>	Disable ▼	Disable ▼
4	<input type="checkbox"/>	Disable ▼	Disable ▼
5	<input type="checkbox"/>	Disable ▼	Disable ▼
6	<input type="checkbox"/>	Disable ▼	Disable ▼
7	<input type="checkbox"/>	Disable ▼	Disable ▼
8	<input type="checkbox"/>	Disable ▼	Disable ▼
9	<input type="checkbox"/>	Disable ▼	Disable ▼
10	<input type="checkbox"/>	Disable ▼	Disable ▼
11	<input type="checkbox"/>	Disable ▼	Disable ▼
12	<input type="checkbox"/>	Disable ▼	Disable ▼
13	<input type="checkbox"/>	Disable ▼	Disable ▼
14	<input type="checkbox"/>	Disable ▼	Disable ▼
15	<input type="checkbox"/>	Disable ▼	Disable ▼
16	<input type="checkbox"/>	Disable ▼	Disable ▼
17	<input type="checkbox"/>	Disable ▼	Disable ▼
18	<input type="checkbox"/>	Disable ▼	Disable ▼
19	<input type="checkbox"/>	Disable ▼	Disable ▼
20	<input type="checkbox"/>	Disable ▼	Disable ▼
21	<input type="checkbox"/>	Disable ▼	Disable ▼
22	<input type="checkbox"/>	Disable ▼	Disable ▼
23	<input type="checkbox"/>	Disable ▼	Disable ▼
24	<input type="checkbox"/>	Disable ▼	Disable ▼
25	<input type="checkbox"/>	Disable ▼	Disable ▼
26	<input type="checkbox"/>	Disable ▼	Disable ▼
27	<input type="checkbox"/>	Disable ▼	Disable ▼
28	<input type="checkbox"/>	Disable ▼	Disable ▼


Figure 4-9-9: QoS Port DSCP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
• Ingress	<p>In Ingress settings you can change ingress translation and classification settings for individual ports.</p> <p>There are two configuration parameters available in Ingress:</p> <ul style="list-style-type: none"> ■ Translate ■ Classify
• Translate	To Enable the Ingress Translation click the checkbox. * means to select all ports of Managed Switch.
• Classify	<p>The Configuration All with available options will assign to whole ports.</p> <p>Classification for a port has 4 different values. All means all ports will have one specific setting.</p> <ul style="list-style-type: none"> ■ Disable: No Ingress DSCP Classification. ■ DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0. ■ Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP. ■ All: Classify all DSCP.
• Egress	<p>The Configuration All with available options will assign to whole ports.</p> <p>Port Egress Rewriting can be one of –. All means all ports will have one specific setting.</p> <ul style="list-style-type: none"> ■ Disable: No Egress rewrite. ■ Enable: Rewrite enabled without remapping. ■ Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. ■ Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with 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 to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.9.8 DSCP-Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches. The DSCP-Based QoS screen in [Figure 4-9-10](#) appears.

DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	<input type="checkbox"/>	<All>	<All>
0 (BE)	<input type="checkbox"/>	0	0
1	<input type="checkbox"/>	0	0
2	<input type="checkbox"/>	0	0
3	<input type="checkbox"/>	0	0
4	<input type="checkbox"/>	0	0
5	<input type="checkbox"/>	0	0
6	<input type="checkbox"/>	0	0
7	<input type="checkbox"/>	0	0
8 (CS1)	<input type="checkbox"/>	0	0
9	<input type="checkbox"/>	0	0
...			
58	<input type="checkbox"/>	0	0
59	<input type="checkbox"/>	0	0
60	<input type="checkbox"/>	0	0
61	<input type="checkbox"/>	0	0
62	<input type="checkbox"/>	0	0
63	<input type="checkbox"/>	0	0

Save

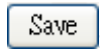
Reset

Figure 4-9-10: DSCP-Based QoS Ingress Classification Page Screenshot

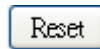
The page includes the following fields:

Object	Description
• DSCP	Maximum number of supported DSCP values are 63.
• Trust	Click to check if the DSCP value is trusted. * means to select all ports of Managed Switch.
• QoS Class	The Configuration All with available values will assign to whole DSCP values. QoS Class value can be any of (0-7)
• DPL	The Configuration All with available values will assign to whole DSCP values. Drop Precedence Level (0-1)

Buttons



: Click to save changes.



: Click to undo any changes made locally and revert to previously saved values.

4.9.9 DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress. The DSCP Translation screen in [Figure 4-9-11](#) appears.

DSCP Translation

DSCP	Ingress		Egress
	Translate	Classify	Remap
*	<All>	<input type="checkbox"/>	<All>
0 (BE)	0 (BE)	<input type="checkbox"/>	0 (BE)
1	1	<input type="checkbox"/>	1
2	2	<input type="checkbox"/>	2
3	3	<input type="checkbox"/>	3
4	4	<input type="checkbox"/>	4
5	5	<input type="checkbox"/>	5
6	6	<input type="checkbox"/>	6
7	7	<input type="checkbox"/>	7
8 (CS1)	8 (CS1)	<input type="checkbox"/>	8 (CS1)
9	9	<input type="checkbox"/>	9
56 (CS7)	56 (CS7)	<input type="checkbox"/>	54
57	57	<input type="checkbox"/>	57
58	58	<input type="checkbox"/>	58
59	59	<input type="checkbox"/>	59
60	60	<input type="checkbox"/>	60
61	61	<input type="checkbox"/>	61
62	62	<input type="checkbox"/>	62
63	63	<input type="checkbox"/>	63

Save

Reset

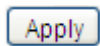
Figure 4-9-11: DSCP Translation Page Screenshot

The Page includes the following fields:

Object	Description
<ul style="list-style-type: none">DSCP	Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

• Ingress	<p>Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.</p> <p>There are two configuration parameters for DSCP Translation –</p> <ul style="list-style-type: none"> ■ Translate ■ Classify
• Translate	DSCP at Ingress side can be translated to any of (0-63) DSCP values.
• Classify	Click to enable Classification at Ingress side.
• Egress	<p>There is following configurable parameter for Egress side -</p> <ul style="list-style-type: none"> ■ Remap
• Remap DP	<p>Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.</p>

Buttons



: Click to apply changes



: Click to undo any changes made locally and revert to previously saved values.

4.9.10 DSCP Classification

This Page allows you to map DSCP value to a QoS Class and DPL value. The DSCP Classification screen in [Figure 4-9-11](#) appears.

DSCP Classification

QoS Class	DSCP
*	<All> ▼
0	0 (BE) ▼
1	0 (BE) ▼
2	0 (BE) ▼
3	0 (BE) ▼
4	0 (BE) ▼
5	0 (BE) ▼
6	0 (BE) ▼
7	0 (BE) ▼


Apply
Reset


Figure 4-9-11: DSCP Classification Page Screenshot

The Page includes the following fields:

Object	Description
• QoS Class	Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to followed parameters.
• DSCP	Select DSCP value (0-63) from DSCP menu to map DSCP to corresponding QoS Class and DPL value

Buttons

 : Click to apply changes

 : Click to undo any changes made locally and revert to previously saved values.

4.9.11 QoS Control List

This page shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.

Click on the lowest plus sign to add a new QCE to the list.

The QoS Control List screen in [Figure 4-9-12](#) appears.







QoS Control List Configuration

QCE#	Port	Frame Type	SMAC	DMAC	VID	PCP	DEI	Action			
								Class	DPL	DSCP	
											<div></div>

Figure 4-9-12: QoS Control List Configuration Page Screenshot

The page includes the following fields:

Object	Description
• 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: <ul style="list-style-type: none"> ■ Any: The QCE will match all frame type. ■ Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

	<ul style="list-style-type: none"> ■ LLC: Only (LLC) frames are allowed. ■ SNAP: Only (SNAP) frames are allowed. ■ IPv4: The QCE will match only IPV4 frames. ■ IPv6: The QCE will match only IPV6 frames.
• SMAC	Displays the OUI field of Source MAC address, i.e. first three octet (byte) of MAC address.
• DMAC	<p>Specify the type of Destination MAC addresses for incoming frame. Possible values are:</p> <ul style="list-style-type: none"> ■ Any: All types of Destination MAC addresses are allowed. ■ Unicast: Only Unicast MAC addresses are allowed. ■ Multicast: Only Multicast MAC addresses are allowed. ■ Broadcast: Only Broadcast MAC addresses are allowed. <p>The default value is 'Any'.</p>
• VID	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
• PCP	Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
• DEI	Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.
• Action	<p>Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.</p> <p>There are three action fields: Class, DPL and DSCP.</p> <ul style="list-style-type: none"> ■ Class: Classified QoS Class; if a frame matches the QCE it will be put in the queue. ■ DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column. ■ DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.
• Modification Buttons	<p>You can modify each QCE in the table using the following buttons:</p> <ul style="list-style-type: none"> : 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.

4.9.11.1 QoS Control Entry Configuration

The QCE Configuration screen in [Figure 4-9-13](#) appears.

QCE Configuration

Port Members																											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Key Parameters

Tag	Any
VID	Any
PCP	Any
DEI	Any
SMAC	Any
DMAC Type	Any
Frame Type	Any

Action Parameters

Class	0
DPL	Default
DSCP	Default

Figure 4-9-13: QCE Configuration Page Screenshot


The page includes the following fields:


Object	Description
<ul style="list-style-type: none"> Port Members 	Check the checkbox button in case you want to make any port member of the QCL entry. By default all ports will be checked
<ul style="list-style-type: none"> Key Parameters 	<p>Key configuration is described as below:</p> <ul style="list-style-type: none"> ■ 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'; user can enter either a specific value or a range of VLANs. ■ PCP Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'. ■ DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'. ■ SMAC Source MAC address: 24 MS bits (OUI) or 'Any'. ■ DMAC Type Destination MAC type: possible values are unicast(UC), multicast(MC), broadcast(BC) or 'Any'.


	<p>■ Frame Type Frame Type can have any of the following values:</p> <ol style="list-style-type: none"> 1. Any 2. Ethernet 3. LLC 4. SNAP 5. IPv4 6. IPv6 <p>Note: All frame types are explained below.</p>
• Any	Allow all types of frames.
• Ethernet	Ethernet Type Valid ethernet type can have value within 0x600-0xFFFF or 'Any' but excluding 0x800(IPv4) and 0x86DD(IPv6), default value is 'Any'.
• LLC	<p>■ SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'</p> <p>■ DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'</p> <p>■ Control Address Valid Control Address can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'</p>
• SNAP	PID Valid PID(a.k.a ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'
• IPv4	<p>■ Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'</p> <p>■ 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 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</p> <p>DSCP Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43</p> <p>■ IP Fragment IPv4 frame fragmented option: yes no any</p> <p>■ Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP</p> <p>■ Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP</p>
• IPv6	<p>■ Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'</p> <p>■ Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits</p> <p>■ DSCP Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43</p>

	<ul style="list-style-type: none"> ■ 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
<ul style="list-style-type: none"> • Action Parameters 	<ul style="list-style-type: none"> ■ Class QoS class: (0-7) or 'Default'. ■ DP Valid Drop Precedence Level can be (0-1) or 'Default'. ■ DSCP Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'. <p>'Default' means that the default classified value is not modified by this QCE.</p>

Buttons

: Click to save the configuration and move to main QCL page

: Click to undo any changes made locally and revert to previously saved values

: Return to the previous page without saving the configuration change

4.9.12 QoS Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is **256** on each switch. The QoS Control List Status screen in [Figure 4-9-14](#) appears.

Combined ▼ Auto-refresh ☐ Resolve Conflict Refresh

QoS Control List Status

User	QCE#	Frame Type	Port	Action			Conflict
				Class	DPL	DSCP	
No entries							


Figure 4-9-14: QoS Control List Status Page Screenshot

The page includes the following fields:

Object	Description
• User	Indicates the QCL user.
• QCE#	Indicates the index of QCE.
• Frame Type	<p>Indicates the type of frame to look for incoming frames. Possible frame types are:</p> <ul style="list-style-type: none"> ■ Any: The QCE will match all frame type. ■ Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. ■ LLC: Only (LLC) frames are allowed. ■ SNAP: Only (SNAP) frames are allowed. ■ IPv4: The QCE will match only IPV4 frames. ■ IPv6: The QCE will match only IPV6 frames.
• Port	Indicates the list of ports configured with the QCE
• Action	<p>Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.</p> <p>There are three action fields: Class, DPL and DSCP.</p> <ul style="list-style-type: none"> ■ Class: Classified QoS Class; if a frame matches the QCE it will be put in the queue. ■ DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.

	<ul style="list-style-type: none"> ■ DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.
<ul style="list-style-type: none"> • Conflict 	<p>Displays QCE status. It may happen that resources required to add a QCE may not available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the resource required by the QCE and pressing 'Refresh' button.</p>

Buttons

: Select the QCL status from this drop down list.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to release the resources required to add QCL entry, in case conflict status for any QCL entry is 'yes'.

: Click to refresh the page immediately.

4.9.13 Storm Control Configuration

Storm control for the switch is configured on this 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 Storm Control Configuration screen in [Figure 4-9-15](#) appears.

QoS Port Storm Control

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enabled	Rate	Unit	Enabled	Rate	Unit	Enabled	Rate	Unit
*	<input type="checkbox"/>	500	<All> ▾	<input type="checkbox"/>	500	<All> ▾	<input type="checkbox"/>	500	<All> ▾
1	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
2	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
3	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
4	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
5	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
6	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
7	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
8	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
9	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
10	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
11	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
12	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
13	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
14	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
15	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
16	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
17	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
18	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
19	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
20	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
21	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
22	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
23	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
24	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
25	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
26	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
27	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
28	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾

Figure 4-9-15: Storm Control Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Frame Type	The settings in a particular row apply to the frame type listed here: <ul style="list-style-type: none">■ unicast■ multicast■ Broadcast
<ul style="list-style-type: none">• Enable	Enable or disable the storm control status for the given frame type.
<ul style="list-style-type: none">• Rate	The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K , 1024K, 2048K, 4096K, 8192K, 16384K or 32768K.

Buttons

: Click to save changes.

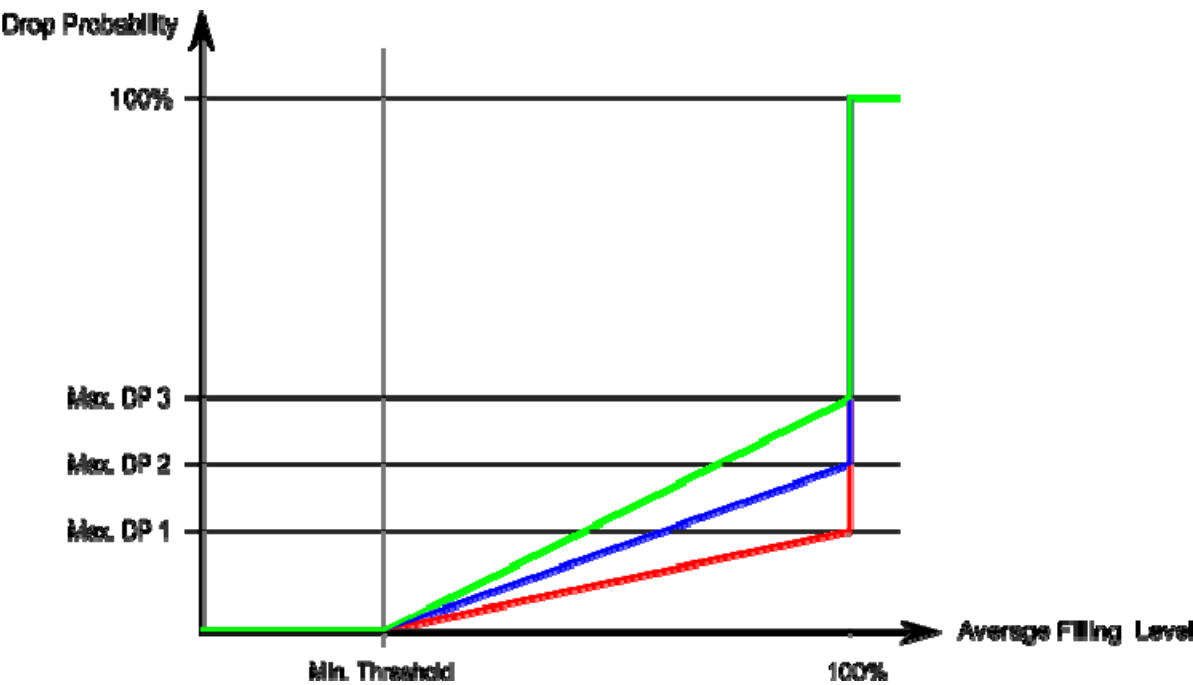
: Click to undo any changes made locally and revert to previously saved values.

4.9.14 WRED

RED Drop Probability Function

Max. DP 1-3 is the drop probability when the average queue filling level is 100%. Frames marked with Drop Precedence Level 0 are never dropped. Min. Threshold is the average queue filling level where the queues randomly start dropping frames. The drop probability for frames marked with Drop Precedence Level n increases linearly from zero (at Min. Threshold average queue filling level) to Max. DP n (at 100% average queue filling level).

The following illustration shows the drop probability function with associated parameters.



This page allows you to configure the Random Early Detection (RED) settings for queue 0 to 5. RED cannot be applied to queue 6 and 7. Through different RED configuration for the queues (QoS classes) it is possible to obtain Weighted Random Early Detection (WRED) operation between queues. The settings are global for all ports in the switch. The QoS Statistics screen in [Figure 4-9-16](#) appears.

Queue	Enable	Min. Threshold	Max. DP 1	Max. DP 2	Max. DP 3
0	<input type="checkbox"/>	0	1	5	10
1	<input type="checkbox"/>	0	1	5	10
2	<input type="checkbox"/>	0	1	5	10
3	<input type="checkbox"/>	0	1	5	10
4	<input type="checkbox"/>	0	1	5	10
5	<input type="checkbox"/>	0	1	5	10

Save Reset

Figure 4-9-16: WRED Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Queue	The queue number (QoS class) for which the configuration below applies.
• Enable	Controls whether RED is enabled for this queue.
• Min. Threshold	Controls the lower RED threshold. If the average queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100.
• Max. DP1	Controls the drop probability for frames marked with Drop Precedence Level 1 when the average queue filling level is 100%. This value is restricted to 0-100.
• Max. DP2	Controls the drop probability for frames marked with Drop Precedence Level 2 when the average queue filling level is 100%. This value is restricted to 0-100.
• Max. DP3	Controls the drop probability for frames marked with Drop Precedence Level 3 when the average queue filling level is 100%. This value is restricted to 0-100.

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.9.15 QoS Statistics

This page provides statistics for the different queues for all switch ports. The QoS Statistics screen in [Figure 4-9-17](#) appears.

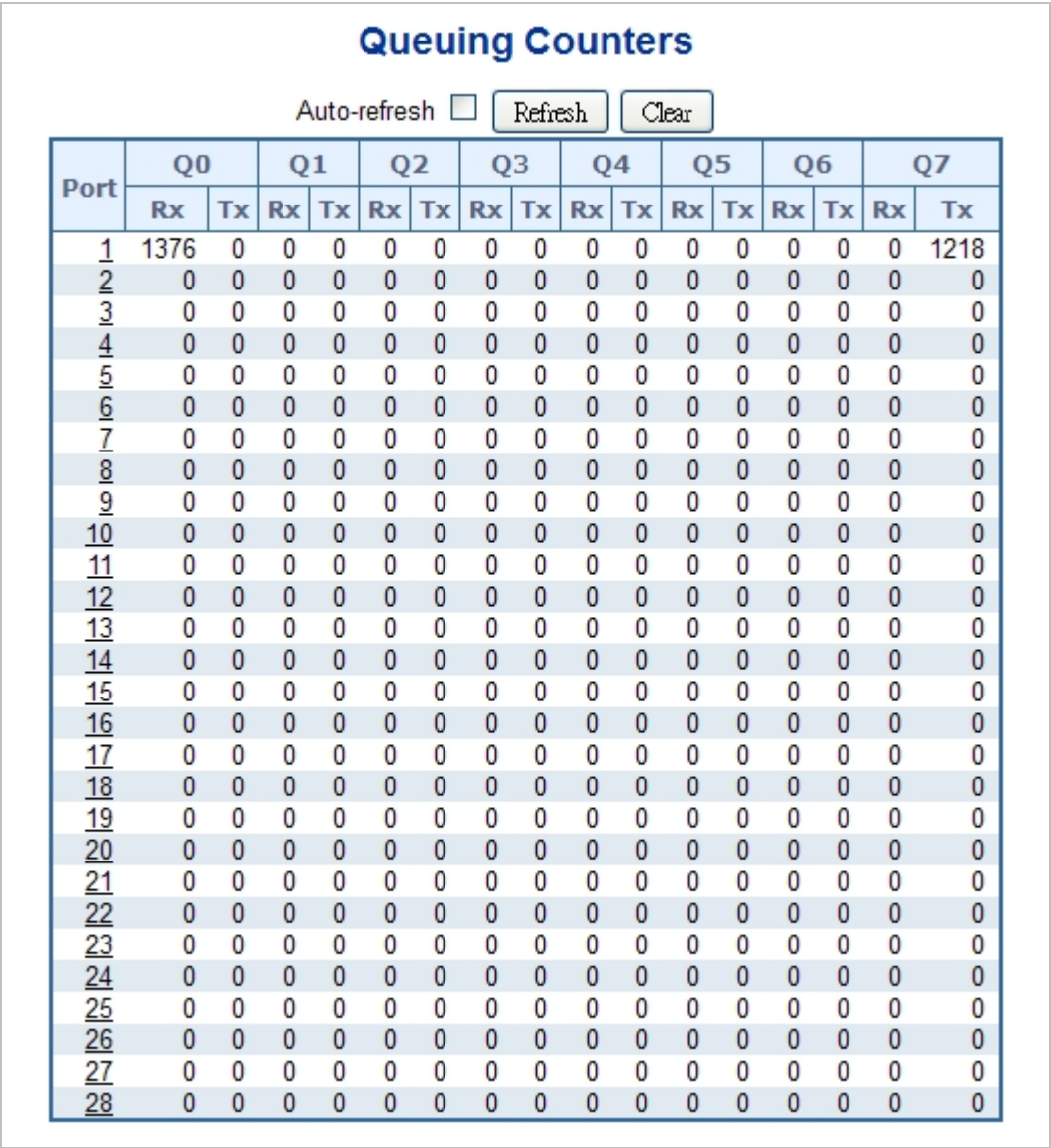


Figure 4-9-17: Queuing Counters Page Screenshot

The page includes the following fields:

Object	Description
• Port	The logical port for the settings contained in the same row.
• Q0 ~ Q7	There are 8 QoS queues per port. Q0 is the lowest priority queue.
• Rx/Tx	The number of received and transmitted packets per queue.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

: Clears the counters for all ports.

4.9.16 Voice VLAN Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI. The Voice VLAN Configuration screen in [Figure 4-9-18](#) appears.

Voice VLAN Configuration

Mode	Disabled
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High)

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<All>	<All>	<All>
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
11	Disabled	Disabled	OUI
12	Disabled	Disabled	OUI
13	Disabled	Disabled	OUI
14	Disabled	Disabled	OUI
15	Disabled	Disabled	OUI
16	Disabled	Disabled	OUI
17	Disabled	Disabled	OUI
18	Disabled	Disabled	OUI
19	Disabled	Disabled	OUI
20	Disabled	Disabled	OUI
21	Disabled	Disabled	OUI
22	Disabled	Disabled	OUI
23	Disabled	Disabled	OUI
24	Disabled	Disabled	OUI
25	Disabled	Disabled	OUI
26	Disabled	Disabled	OUI
27	Disabled	Disabled	OUI
28	Disabled	Disabled	OUI

Save

Reset

Figure 4-9-18: Voice VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Mode	<p>Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter. Possible modes are:</p> <ul style="list-style-type: none"> ■ Enabled: Enable Voice VLAN mode operation. ■ Disabled: Disable Voice VLAN mode operation.
• VLAN ID	<p>Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is conflict configuration if the value equal management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.</p>
• Age Time	<p>Indicates the Voice VLAN secure learning age time. The allowed range is 10 to 10000000 seconds. It used when security mode or auto detect mode is enabled. In other cases, it will based hardware age time. The actual age time will be situated in the [age_time; 2 * age_time] interval.</p>
• Traffic Class	<p>Indicates the Voice VLAN traffic class. All traffic on Voice VLAN will apply this class.</p>
• Port Mode	<p>Indicates 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. Possible port modes are:</p> <ul style="list-style-type: none"> ■ Disabled: Disjoin from Voice VLAN. ■ Auto: Enable auto detect mode. It detects whether there is VoIP phone attached on the specific port and configure the Voice VLAN members automatically. ■ Forced: Forced join to Voice VLAN. ■ All means all ports will have one specific setting.
• Port Security	<p>Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephone MAC address in Voice VLAN will be blocked 10 seconds. Possible port modes are:</p> <ul style="list-style-type: none"> ■ Enabled: Enable Voice VLAN security mode operation. ■ Disabled: Disable Voice VLAN security mode operation. ■ All means all ports will have one specific setting.
• Port Discovery Protocol	<p>Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:</p> <ul style="list-style-type: none"> ■ OUI: Detect telephony device by OUI address.

	<ul style="list-style-type: none"> ■ LLDP: Detect telephony device by LLDP. ■ Both: Both OUI and LLDP. ■ All means all ports will have one specific setting.
--	--

Buttons

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.9.17 Voice VLAN OUI Table

Configure VOICE VLAN OUI table on this page. The maximum entry number is 16. Modifying the OUI table will restart auto detection of OUI process. The Voice VLAN OUI Table screen in [Figure 4-9-19](#) appears.

Voice VLAN OUI Table		
Delete	Telephony OUI	Description
<input type="checkbox"/>	00-03-6b	Cisco phones
<input type="checkbox"/>	00-0f-e2	H3C phones
<input type="checkbox"/>	00-60-b9	Phillips and NEC AG phones
<input type="checkbox"/>	00-d0-1e	Pingtel phones
<input type="checkbox"/>	00-e0-75	Polycom phones
<input type="checkbox"/>	00-e0-bb	3Com phones
<input type="checkbox"/>	00-01-e3	Siemens AG phones

Figure 4-9-19 : Voice VLAN OUI Table Page Screenshot

The page includes the following fields:

Object	Description
• Delete	Check to delete the entry. It will be 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 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
• Description	The description of OUI address. Normaly, it descript which vendor telephony device. The allowed string length is 0 to 32.

Buttons

Add New Entry: Click to add a new access management entry.

Save: Click to save changes.

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

4.10 Access Control Lists

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

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

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

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

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

4.10.1 Access Control List Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is **256** on each switch. The Voice VLAN OUI Table screen in [Figure 4-10-1](#) appears.

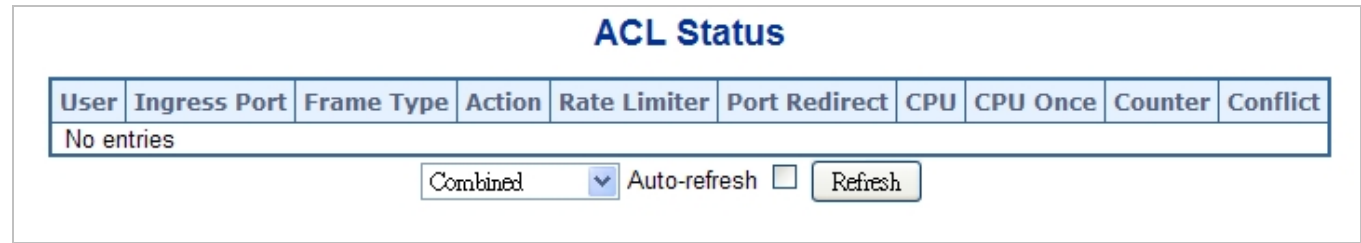



Figure 4-10-1: ACL Status Page Screenshot

The page includes the following fields:

Object	Description
• User	Indicates the ACL user.
• Ingress Port	Indicates the ingress port of the ACE. Possible values are: <ul style="list-style-type: none"> ■ All: The ACE will match all ingress port. ■ Port: The ACE will match a specific ingress port.
• Frame Type	Indicates the frame type of the ACE. Possible values are: <ul style="list-style-type: none"> ■ Any: The ACE will match any frame type. ■ EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ■ ARP: The ACE will match ARP/RARP frames. ■ IPv4: The ACE will match all IPv4 frames. ■ IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. ■ IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. ■ IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. ■ IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. ■ IPv6: The ACE will match all IPv6 standard frames.
• Action	Indicates the forwarding action of the ACE. <ul style="list-style-type: none"> ■ Permit: Frames matching the ACE may be forwarded and learned. ■ Deny: Frames matching the ACE are dropped.
• Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
• Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
• Mirror	Specify the mirror operation of this port. The allowed values are: <ul style="list-style-type: none"> ■ 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

Combined : Select the ACL status from this drop down list.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediate

4.10.2 Access Control List Configuration

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is **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 Access Control List Configuration screen in [Figure 4-10-2](#) appears.



Figure 4-10-2: Access Control List Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Ingress Port	Indicates the ingress port of the ACE. Possible values are: <ul style="list-style-type: none">■ All: The ACE will match all ingress port.■ Port: The ACE will match a specific ingress port.
• Policy / Bitmask	Indicates the policy number and bitmask of the ACE.
• Frame Type	Indicates the frame type of the ACE. Possible values are: <ul style="list-style-type: none">■ Any: The ACE will match any frame type.■ EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.■ ARP: The ACE will match ARP/RARP frames.■ IPv4: The ACE will match all IPv4 frames.■ IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.

	<ul style="list-style-type: none"> ■ IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. ■ IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. ■ IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. ■ IPv6: The ACE will match all IPv6 standard frames.
• Action	<p>Indicates the forwarding action of the ACE.</p> <ul style="list-style-type: none"> ■ Permit: Frames matching the ACE may be forwarded and learned. ■ Deny: Frames matching the ACE are dropped.
• Rate Limiter	<p>Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.</p>
• Port Redirect	<p>Indicates the ingress port of the ACE. Possible values are:</p> <ul style="list-style-type: none"> ■ All: The ACE will match all ingress port. ■ Port: The ACE will match a specific ingress port.
• Mirror	<p>Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:</p> <ul style="list-style-type: none"> ■ Enabled: Frames received on the port are mirrored. ■ Disabled: Frames received on the port are not mirrored. <p>The default value is "Disabled".</p>
• Counter	<p>The counter indicates the number of times the ACE was hit by a frame.</p>
• Modification Buttons	<p>You can modify each ACE (Access Control Entry) in the table using the following buttons:</p> <ul style="list-style-type: none"> : Inserts a new ACE before the current row. : Edits the ACE row. : Moves the ACE up the list. : Moves the ACE down the list. : Deletes the ACE. : The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

: Click to clear the counters.

: Click to remove all ACEs.

4.10.3 ACE Configuration

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

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

A frame that hits this ACE matches the configuration that is defined here. The ACE Configuration screen in [Figure 4-10-3](#) appears.

ACE Configuration

Ingress Port	All
Policy Filter	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Port Redirect	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Save

Reset

Cancel

Figure 4-10-3: ACE Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">Ingress Port	<p>Select the ingress port for which this ACE applies.</p> <ul style="list-style-type: none">All: The ACE applies to all port.Portn: The ACE applies to this port number, where <i>n</i> is the number of the switch port.
<ul style="list-style-type: none">Policy Filter	<p>Specify the policy number filter for this ACE.</p> <ul style="list-style-type: none">Any: No policy filter is specified. (policy filter status is "don't-care".)Specific: If you want to filter a specific policy with this ACE, choose this

	value. Two field for entering an policy value and bitmask appears.
• Policy Value	When " Specific " is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255 .
• Policy Bitmask	When " Specific " is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff .
• Frame Type	Select the frame type for this ACE. These frame types are mutually exclusive. <ul style="list-style-type: none"> ■ Any: Any frame can match this ACE. ■ Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). ■ ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type. ■ IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.
• Action	Specify the action to take with a frame that hits this ACE. <ul style="list-style-type: none"> ■ Permit: The frame that hits this ACE is granted permission for the ACE operation. ■ Deny: The frame that hits this ACE is dropped.
• Rate Limiter	Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.
• EVC Policer	Select whether EVC policer is enabled or disabled. The default value is " Disabled ".
• EVC Policer ID	Select which EVC policer ID to apply on this ACE. The allowed values are Disabled or the values 1 through 128 .
• Port Redirect	Frames that hit the ACE are redirected to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled.
• Mirror	Specify the mirror operation of this port. The allowed values are: <ul style="list-style-type: none"> ■ Enabled: Frames received on the port are mirrored. ■ Disabled: Frames received on the port are not mirrored. The default value is "Disabled".
• Logging	Specify the logging operation of the ACE. The allowed values are: <ul style="list-style-type: none"> ■ Enabled: Frames matching the ACE are stored in the System Log. ■ Disabled: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
• Shutdown	Specify the port shut down operation of the ACE. The allowed values are: <ul style="list-style-type: none"> ■ Enabled: If a frame matches the ACE, the ingress port will be disabled.

	<ul style="list-style-type: none"> ■ Disabled: Port shut down is disabled for the ACE.
<ul style="list-style-type: none"> • Counter 	The counter indicates the number of times the ACE was hit by a frame.

■ MAC Parameters

Object	Description
<ul style="list-style-type: none"> • SMAC Filter 	<p>(Only displayed when the frame type is Ethernet Type or ARP.)</p> <p>Specify the source MAC filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No SMAC filter is specified. (SMAC filter status is "don't-care".) ■ Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.
<ul style="list-style-type: none"> • SMAC Value 	<p>When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SMAC value.</p>
<ul style="list-style-type: none"> • DMAC Filter 	<p>Specify the destination MAC filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No DMAC filter is specified. (DMAC filter status is "don't-care".) ■ MC: Frame must be multicast. ■ BC: Frame must be broadcast. ■ UC: Frame must be unicast. ■ Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.
<ul style="list-style-type: none"> • DMAC Value 	<p>When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DMAC value.</p>

■ VLAN Parameters

Object	Description
<ul style="list-style-type: none"> • 802.1Q Tagged 	<p>Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:</p> <ul style="list-style-type: none"> ■ Any: Any value is allowed ("don't-care"). ■ Enabled: Tagged frame only. ■ Disabled: Untagged frame only. <p>The default value is "Any".</p>
<ul style="list-style-type: none"> • VLAN ID Filter 	<p>Specify the VLAN ID filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) ■ Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.
<ul style="list-style-type: none"> • VLAN ID 	<p>When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN</p>

	ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
• Tag Priority	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

■ ARP Parameters

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

Object	Description
• ARP/RARP	Specify the available ARP/RARP opcode (OP) flag for this ACE. <ul style="list-style-type: none"> ■ Any: No ARP/RARP OP flag is specified. (OP is "don't-care".) ■ ARP: Frame must have ARP/RARP opcode set to ARP. ■ RARP: Frame must have ARP/RARP opcode set to RARP. ■ Other: Frame has unknown ARP/RARP Opcode flag.
• Request/Reply	Specify the available ARP/RARP opcode (OP) flag for this ACE. <ul style="list-style-type: none"> ■ Any: No ARP/RARP OP flag is specified. (OP is "don't-care".) ■ Request: Frame must have ARP Request or RARP Request OP flag set. ■ Reply: Frame must have ARP Reply or RARP Reply OP flag.
• Sender IP Filter	Specify the sender IP filter for this ACE. <ul style="list-style-type: none"> ■ Any: No sender IP filter is specified. (Sender IP filter is "don't-care".) ■ Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears. ■ Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.
• Sender IP Address	When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
• Sender IP Mask	When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
• Target IP Filter	Specify the target IP filter for this specific ACE. <ul style="list-style-type: none"> ■ Any: No target IP filter is specified. (Target IP filter is "don't-care".) ■ Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. ■ Network: Target IP filter is set to Network. Specify the target IP

	address and target IP mask in the Target IP Address and Target IP Mask fields that appear.
• Target IP Address	When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
• Target IP Mask	When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
• ARP SMAC Match	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. <ul style="list-style-type: none"> ■ 0: ARP frames where SHA is not equal to the SMAC address. ■ 1: ARP frames where SHA is equal to the SMAC address. ■ Any: Any value is allowed ("don't-care").
• RARP SMAC Match	Specify whether frames can hit the action according to their target hardware address field (THA) settings. <ul style="list-style-type: none"> ■ 0: RARP frames where THA is not equal to the SMAC address. ■ 1: RARP frames where THA is equal to the SMAC address. ■ Any: Any value is allowed ("don't-care").
• IP/Ethernet Length	Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings. <ul style="list-style-type: none"> ■ 0: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04). ■ 1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04). ■ Any: Any value is allowed ("don't-care").
• IP	Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings. <ul style="list-style-type: none"> ■ 0: ARP/RARP frames where the HLD is equal to Ethernet (1). ■ 1: ARP/RARP frames where the HLD is equal to Ethernet (1). ■ Any: Any value is allowed ("don't-care").
• Ethernet	Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings. <ul style="list-style-type: none"> ■ 0: ARP/RARP frames where the PRO is equal to IP (0x800). ■ 1: ARP/RARP frames where the PRO is equal to IP (0x800). ■ Any: Any value is allowed ("don't-care").

■ IP Parameters

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

Object	Description
<ul style="list-style-type: none"> • IP Protocol Filter 	<p>Specify the IP protocol filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No IP protocol filter is specified ("don't-care"). ■ Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears. ■ ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file. ■ UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file. ■ TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.
<ul style="list-style-type: none"> • IP Protocol Value 	<p>When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.</p>
<ul style="list-style-type: none"> • IP TTL 	<p>Specify the Time-to-Live settings for this ACE.</p> <ul style="list-style-type: none"> ■ zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry. ■ non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry. ■ Any: Any value is allowed ("don't-care").
<ul style="list-style-type: none"> • IP Fragment 	<p>Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.</p> <ul style="list-style-type: none"> ■ No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. ■ Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. ■ Any: Any value is allowed ("don't-care").
<ul style="list-style-type: none"> • IP Option 	<p>Specify the options flag setting for this ACE.</p> <ul style="list-style-type: none"> ■ No: IPv4 frames where the options flag is set must not be able to match this entry. ■ Yes: IPv4 frames where the options flag is set must be able to match this entry. ■ Any: Any value is allowed ("don't-care").

• SIP Filter	Specify the source IP filter for this ACE. <ul style="list-style-type: none"> ■ Any: No source IP filter is specified. (Source IP filter is "don't-care".) ■ Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears. ■ Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.
• SIP Address	When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.
• SIP Mask	When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
• DIP Filter	Specify the destination IP filter for this ACE. <ul style="list-style-type: none"> ■ Any: No destination IP filter is specified. (Destination IP filter is "don't-care".) ■ Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. ■ Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.
• DIP Address	When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.
• DIP Mask	When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

■ ICMP Parameters

Object	Description
• ICMP Type Filter	Specify the ICMP filter for this ACE. <ul style="list-style-type: none"> ■ Any: No ICMP filter is specified (ICMP filter status is "don't-care"). ■ Specific: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.
• ICMP Type Value	When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.
• ICMP Code Filter	Specify the ICMP code filter for this ACE. <ul style="list-style-type: none"> ■ Any: No ICMP code filter is specified (ICMP code filter status is

	<p>"don't-care").</p> <ul style="list-style-type: none"> ■ Specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.
<ul style="list-style-type: none"> • ICMP Code Value 	<p>When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.</p>

■ TCP/UDP Parameters

Object	Description
<ul style="list-style-type: none"> • TCP/UDP Source Filter 	<p>Specify the TCP/UDP source filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care"). ■ Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears. ■ Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.
<ul style="list-style-type: none"> • TCP/UDP Source No. 	<p>When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.</p>
<ul style="list-style-type: none"> • TCP/UDP Source Range 	<p>When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.</p>
<ul style="list-style-type: none"> • TCP/UDP Destination Filter 	<p>Specify the TCP/UDP destination filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care"). ■ Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears. ■ Range: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.
<ul style="list-style-type: none"> • TCP/UDP Destination Number 	<p>When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame</p>

	that hits this ACE matches this TCP/UDP destination value.
<ul style="list-style-type: none"> • TCP/UDP Destination Range 	<p>When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.</p>
<ul style="list-style-type: none"> • TCP FIN 	<p>Specify the TCP "No more data from sender" (FIN) value for this ACE.</p> <ul style="list-style-type: none"> ■ 0: TCP frames where the FIN field is set must not be able to match this entry. ■ 1: TCP frames where the FIN field is set must be able to match this entry. ■ Any: Any value is allowed ("don't-care").
<ul style="list-style-type: none"> • TCP SYN 	<p>Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.</p> <ul style="list-style-type: none"> ■ 0: TCP frames where the SYN field is set must not be able to match this entry. ■ 1: TCP frames where the SYN field is set must be able to match this entry. ■ Any: Any value is allowed ("don't-care").
<ul style="list-style-type: none"> • TCP RST 	<p>Specify the TCP "Reset the connection" (RST) value for this ACE.</p> <ul style="list-style-type: none"> ■ 0: TCP frames where the RST field is set must not be able to match this entry. ■ 1: TCP frames where the RST field is set must be able to match this entry. ■ Any: Any value is allowed ("don't-care").
<ul style="list-style-type: none"> • TCP PSH 	<p>Specify the TCP "Push Function" (PSH) value for this ACE.</p> <ul style="list-style-type: none"> ■ 0: TCP frames where the PSH field is set must not be able to match this entry. ■ 1: TCP frames where the PSH field is set must be able to match this entry. ■ Any: Any value is allowed ("don't-care").
<ul style="list-style-type: none"> • TCP ACK 	<p>Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.</p> <ul style="list-style-type: none"> ■ 0: TCP frames where the ACK field is set must not be able to match this entry. ■ 1: TCP frames where the ACK field is set must be able to match this entry. ■ Any: Any value is allowed ("don't-care").
<ul style="list-style-type: none"> • TCP URG 	<p>Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.</p> <ul style="list-style-type: none"> ■ 0: TCP frames where the URG field is set must not be able to match


	<p>this entry.</p> <ul style="list-style-type: none"> ■ 1: TCP frames where the URG field is set must be able to match this entry. ■ Any: Any value is allowed ("don't-care").
--	--


■ Ethernet Type Parameters


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

Object	Description
<ul style="list-style-type: none"> • EtherType Filter 	<p>Specify the Ethernet type filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No EtherType filter is specified (EtherType filter status is "don't-care"). ■ Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.
<ul style="list-style-type: none"> • Ethernet Type Value 	<p>When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.</p>

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

: Return to the previous page.

4.10.4 ACL Ports Configuration

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

The ACL Ports Configuration screen in [Figure 4-10-4](#) appears.

ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Logging	Shutdown	State	Counter
*	0	<All> ▼	<All> ▼	<All> ▼	<All> ▼	<All> ▼	<All> ▼	*
1	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	1632
2	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
3	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
4	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
5	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
6	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
7	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
8	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
9	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
10	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
11	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
12	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
13	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
14	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
15	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
16	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
17	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
18	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
19	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
20	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
21	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
22	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
23	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
24	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
25	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
26	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
27	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
28	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0

Save
Reset

Refresh
Clear

Figure 4-10-4: ACL Ports Configuration Page Screenshot

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 1 through 8 . The default value is 1 .
• 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 to this port. The allowed values are Disabled or the values 1 through 15 . The default value is " Disabled ". All means all ports will have one specific setting.
• Port Redirect	Select which port frames are redirected on. The allowed values are Disabled or a specific port number. The default value is " Disabled ". 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. The allowed values are: Enabled : Frames received on the port are stored in the System Log. Disabled : Frames received on the port are not logged. The default value is " Disabled ". Please note that the System Log memory size and logging rate is limited. All means all ports will have one specific setting.
• Shutdown	Specify the port shut down operation of this port. The allowed values are: Enabled : If a frame is received on the port, the port will be disabled. Disabled : Port shut down is disabled. The default value is " Disabled ". All means all ports will have one specific setting.
• State	Specify the port state of this port. The allowed values are: Enabled : To reopen ports by changing the volatile port configuration of the ACL user module. Disabled : To close ports by changing the volatile port configuration of the ACL user module. The default value is " Enabled ". All means all ports will have one specific setting.

• Counter	Counts the number of frames that match this ACE.
------------------	--

Buttons

Save: Click to save changes.

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

Refresh: Click to refresh the page; any changes made locally will be undone.

Clear: Click to clear the counters.

4.10.5 ACL Rate Limiter Configuration

Configure the rate limiter for the ACL of the switch.

The ACL Rate Limiter Configuration screen in [Figure 4-10-5](#) appears.

ACL Rate Limiter Configuration

Rate Limiter ID	Rate (pps)
*	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1


Save **Reset**


Figure 4-10-5: ACL Rate Limiter Configuration Page Screenshot

2The page includes the following fields:

Object	Description
• Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
• Rate	The allowed values are: 0-3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.
• Unit	<p>Specify the rate unit. The allowed values are:</p> <ul style="list-style-type: none">■ pps: packets per second.■ kbps: Kbits per second. <p>All means all ports will have one specific setting.</p>

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.11 Authentication

This section is to control the access of the Managed Switch, includes the user access and management control.

The Authentication section contains links to the following main topics:

- **IEEE 802.1X Port-Based Network Access Control**
- **MAC-Based Authentication**
- **User Authentication**

Overview of 802.1X (Port-Based) Authentication

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

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

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, and 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 3rd party switch or a hub) and still require individual authentication, and 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, 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

It is allowed to configure the Managed Switch to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and Web browser. This 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.

4.11.1 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 available any services offered by the switch or the LAN.

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.

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange
- Ports in Authorized and Unauthorized States

■ Device Roles

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

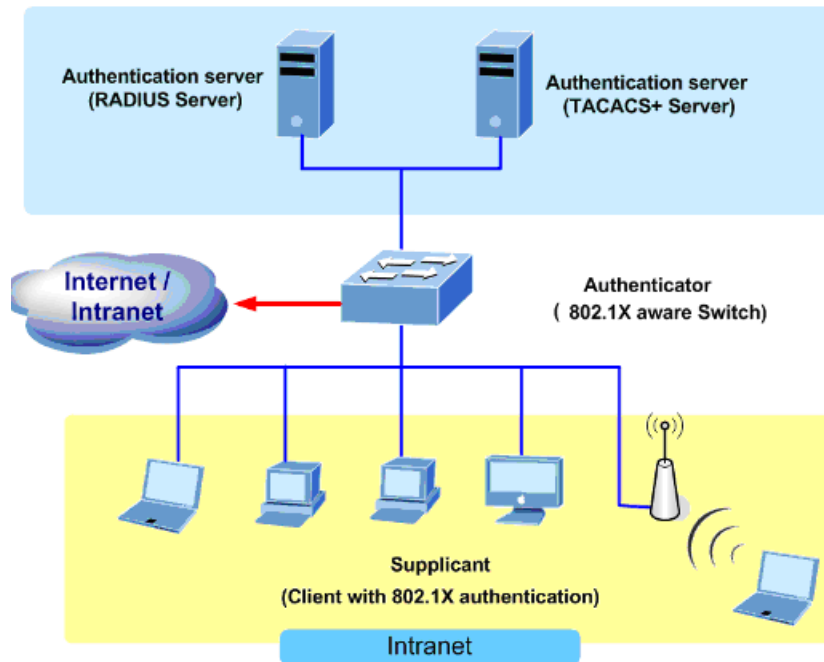


Figure 4-11-1

- **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 Windows XP operating system. (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 whether or not 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; it is available in 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 during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity



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. “[Figure 4-11-2](#)” shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

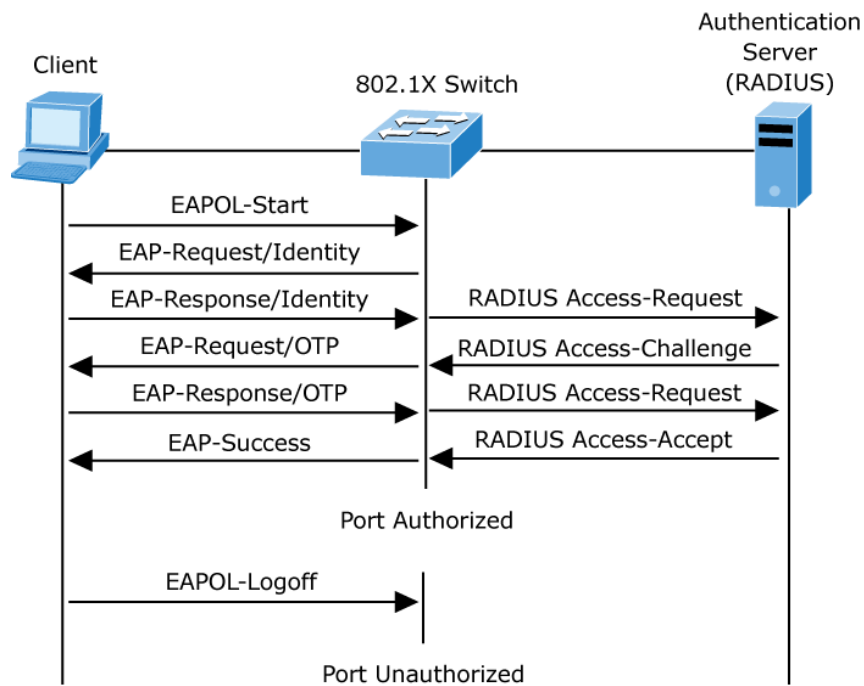


Figure 4-11-2: EAP Message Exchange

■ Ports in Authorized and Unauthorized States

The switch port state determines whether or not 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, causing 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.

4.11.2 Authentication Configuration

This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces. The Authentication Method Configuration screen in [Figure 4-11-3](#) appears.

Client	Authentication Method	Fallback
console	local	<input type="checkbox"/>
telnet	local	<input type="checkbox"/>
ssh	local	<input type="checkbox"/>
web	local	<input type="checkbox"/>

Figure 4-11-3: Authentication Method Configuration Page Screenshot

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: <ul style="list-style-type: none">■ None: authentication is disabled and login is not possible.■ local: use the local user database on the switch stack for authentication.■ RADIUS: use a remote RADIUS server for authentication.■ TACACS+: use a remote TACACS+ server for authentication.
• Fallback	Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to something else than 'none' or 'local'.

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.11.3 Network Access Server Configuration

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

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

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication. The NAS configuration consists of two sections, a system- and a port-wide. The Network Access Server Configuration screen in [Figure 4-11-4](#) appears.

Network Access Server Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	<input type="checkbox"/>
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>
Guest VLAN Enabled	<input type="checkbox"/>
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
* <All>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
11	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
12	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
13	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
14	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
15	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
16	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
17	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
18	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
19	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
20	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
21	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
22	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
23	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
24	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
25	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
26	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
27	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
28	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize

Refresh Save Reset


Refresh 

Figure 4-11-4: Network Access Server Configuration Page Screenshot

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	<p>If checked, 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.</p> <p>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.</p>
• Reauthentication Period	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
• EAPOL Timeout	Determines the time between retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.
• Aging Period	<p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</p> <ul style="list-style-type: none">■ Single 802.1X■ Multi 802.1X■ MAC-Based Auth. <p>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.</p> <p>If reauthentication is enabled and the port is in a 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.</p>

	<p>For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.</p>
<ul style="list-style-type: none"> • Hold Time 	<p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</p> <ul style="list-style-type: none"> ■ Single 802.1X ■ Multi 802.1X ■ MAC-Based Auth. <p>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.</p> <p>In MAC-based Auth. mode, the The switch will ignore new frames coming from the client during the hold time.</p> <p>The Hold Time can be set to a number between 10 and 1000000 seconds.</p>
<ul style="list-style-type: none"> • RADIUS-Assigned QoS Enabled 	<p>RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).</p> <p>The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled for that port. When unchecked, RADIUS-server assigned QoS Class is disabled for all ports.</p>
<ul style="list-style-type: none"> • RADIUS-Assigned VLAN Enabled 	<p>RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).</p> <p>The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When</p>

	checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled for that port. When unchecked, RADIUS-server assigned VLAN is disabled for all ports.
• Guest VLAN Enabled	<p>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.</p> <p>The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled for all ports.</p>
• Guest VLAN ID	<p>This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].</p>
• Max. Reauth. Count	<p>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.</p> <p>Valid values are in the range [1; 255].</p>
• Allow Guest VLAN if EAPOL Seen	<p>The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.</p> <p>The value can only be changed if the Guest VLAN option is globally enabled.</p>

Port Configuration

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

Object	Description
• Port	The port number for which the configuration below applies.
• Admin State	The Configuration All with available options will assign to whole ports.

If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

Force Authorized

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

Force Unauthorized

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

Port-based 802.1X

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

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend

authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Single 802.1X

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

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X

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

Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated

on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

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

MAC-based Auth.

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

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

The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd 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 802.1 X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that

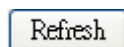
	<p>MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.</p>
<ul style="list-style-type: none"> • RADIUS-Assigned QoS Enabled 	<p>When RADIUS-Assigned QoS is both globally enabled and enabled (checked) 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 or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).</p> <p>This option is only available for single-client modes, i.e.</p> <ul style="list-style-type: none"> • Port-based 802.1X • Single 802.1X <p>RADIUS attributes used in identifying a QoS Class:</p> <p>Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.</p> <p>Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:</p> <p>All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3].</p>
<ul style="list-style-type: none"> • RADIUS-Assigned VLAN Enabled 	<p>When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned</p>

	<p>VLAN ID.</p> <p>If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).</p> <p>This option is only available for single-client modes, i.e.</p> <ul style="list-style-type: none"> • Port-based 802.1X • Single 802.1X <p>For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.</p> <p>RADIUS attributes used in identifying a VLAN ID:</p> <p>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:</p> <ul style="list-style-type: none"> - The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet. - The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag): - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6). - Value of Tunnel-Type must be set to "VLAN" (ordinal 13). - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].
<ul style="list-style-type: none"> • Guest VLAN Enabled 	<p>When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.</p> <p>This option is only available for EAPOL-based modes, i.e.:</p> <ul style="list-style-type: none"> • Port-based 802.1X • Single 802.1X • Multi 802.1X <p>For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN</p>

	<p>Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.</p> <p>Guest VLAN Operation:</p> <p>When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile; the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.</p> <p>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.</p> <p>While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.</p>
<ul style="list-style-type: none"> • Port State 	<p>The current state of the port. It can undertake one of the following values:</p> <ul style="list-style-type: none"> ■ 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.
<ul style="list-style-type: none"> • Restart 	<p>Two buttons are available for each row. The buttons are only enabled when</p>

	<p>authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.</p> <p>Clicking these buttons will not cause settings changed on the page to take effect.</p> <p>Reauthenticate: Schedules a reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.</p> <p>The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.</p> <p>Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.</p>
--	--

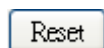
Buttons



: Click to refresh the page.



: Click to save changes.



: Click to undo any changes made locally and revert to previously saved values.

4.11.4 Network Access Overview

This page provides an overview of the current NAS port states for the selected switch. The Network Access Overview screen in [Figure 4-11-5](#) appears.

Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled				
2	Force Authorized	Globally Disabled				
3	Force Authorized	Globally Disabled				
4	Force Authorized	Globally Disabled				
5	Force Authorized	Globally Disabled				
6	Force Authorized	Globally Disabled				
7	Force Authorized	Globally Disabled				
8	Force Authorized	Globally Disabled				
9	Force Authorized	Globally Disabled				
10	Force Authorized	Globally Disabled				
11	Force Authorized	Globally Disabled				
12	Force Authorized	Globally Disabled				
13	Force Authorized	Globally Disabled				
14	Force Authorized	Globally Disabled				
15	Force Authorized	Globally Disabled				
16	Force Authorized	Globally Disabled				
17	Force Authorized	Globally Disabled				
18	Force Authorized	Globally Disabled				
19	Force Authorized	Globally Disabled				
20	Force Authorized	Globally Disabled				
21	Force Authorized	Globally Disabled				
22	Force Authorized	Globally Disabled				
23	Force Authorized	Globally Disabled				
24	Force Authorized	Globally Disabled				
25	Force Authorized	Globally Disabled				
26	Force Authorized	Globally Disabled				
27	Force Authorized	Globally Disabled				
28	Force Authorized	Globally Disabled				

Auto-refresh ☐ [Refresh](#)

Figure 4-11-5: Network Access Server Switch Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number. Click to navigate to detailed NAS statistics for this port.
• Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
• Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
• Last Source	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
• Last ID	The user name (supplicant identity) carried in 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	<p>The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.</p> <p>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.</p> <p>If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.</p>

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

4.11.5 Network Access Statistics

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only. Use the port select box to select which port details to be displayed. The Network Access Statistics screen in [Figure 4-11-6](#) appears.

NAS Statistics Port 1

Port 1
Auto-refresh ☐

Port State

Admin State	Force Authorized
Port State	Globally Disabled

Figure 4-11-6: Network Access Statistics Page Screenshot

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	<p>The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.</p> <p>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.</p> <p>If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.</p>

Port Counters

Object	Description
<ul style="list-style-type: none">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

			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	dot1xAuthEapolLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames)

	that have been transmitted by the switch.			
• Backend Server Counters	These backend (RADIUS) frame counters are available for the following administrative states:			
	<div><div>■</div>Port-based 802.1X</div> <div><div>■</div>Single 802.1X</div> <div><div>■</div>Multi 802.1X</div> <div><div>■</div>MAC-based Auth.</div>			
	Direction	Name	IEEE Name	Description
	Rx	Access Challenges	dot1xAuthBackendAccessChallenges	802.1X-based: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
Rx	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	802.1X-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. MAC-based: Not applicable.	
Rx	Auth.	dot1xAuthBackendAuth	802.1X- and MAC-based:	

	Successes	Successes	Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
Rx	Auth. Failures	dot1xAuthBackendAuth Fails	802.1X- and MAC-based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
Tx	Responses	dot1xAuthBackendResponses	802.1X-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. MAC-based: Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • Selected Counters 	<p>The Selected Counters table is visible when the port is one of the following administrative states:</p> <ul style="list-style-type: none"> ■ Multi 802.1X ■ MAC-based Auth. <p>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.</p>

Attached MAC Address

Object	Description
<ul style="list-style-type: none">• Identity	Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached. This column is not available for MAC-based Auth.
<ul style="list-style-type: none">• MAC Address	For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.
<ul style="list-style-type: none">• VLAN ID	This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.
<ul style="list-style-type: none">• State	The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.
<ul style="list-style-type: none">• Last Authentication	Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

: This button is available in the following modes:

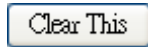
- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X

Click to clear the counters for the selected port.

: This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.



: This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear only the currently selected client's counters.

4.11.6 RADIUS

This Page allows you to configure the RADIUS Servers. The RADIUS Configuration screen in [Figure 4-11-7](#) appears.

RADIUS Server Configuration

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
--------	----------	-----------	-----------	---------	------------	-----

Add New Server

Apply

Reset

Figure 4-11-7: RADIUS Server Configuration Page Screenshot

The Page includes the following fields:

Global Configuration

These setting are common for all of the RADIUS Servers.

Object	Description
<ul style="list-style-type: none">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.
<ul style="list-style-type: none">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.
<ul style="list-style-type: none">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

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

Delete : Click to undo the addition of the new server.

Apply : Click to apply changes

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

4.11.7 TACACS+

This Page allows you to configure the TACACS+ Servers. The TACACS+ Configuration screen in [Figure 4-11-8](#) appears.

TACACS+ Server Configuration

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key		

Server Configuration

Delete	Hostname	Port	Timeout	Key
--------	----------	------	---------	-----

Add New Server

Apply **Reset**

Figure 4-11-8: TACACS+ Server Configuration Page Screenshot

The Page includes the following fields:

Global Configuration

These setting 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	<p>The Dead Time, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.</p> <p>Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.</p>
• Key	The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

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

Object	Description
• Delete	To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.
• Hostname	The IP address or hostname of the TACACS+ server.
• Port	The TCP port to use on the TACACS+ server for authentication.
• Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
• Key	This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

Add New Server

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

Delete

: Click to undo the addition of the new server.

Apply

: Click to apply changes

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.11.8 RADIUS Overview

This Page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration Page. The RADIUS Authentication/Accounting Server Overview screen in [Figure 4-11-9](#) appears.

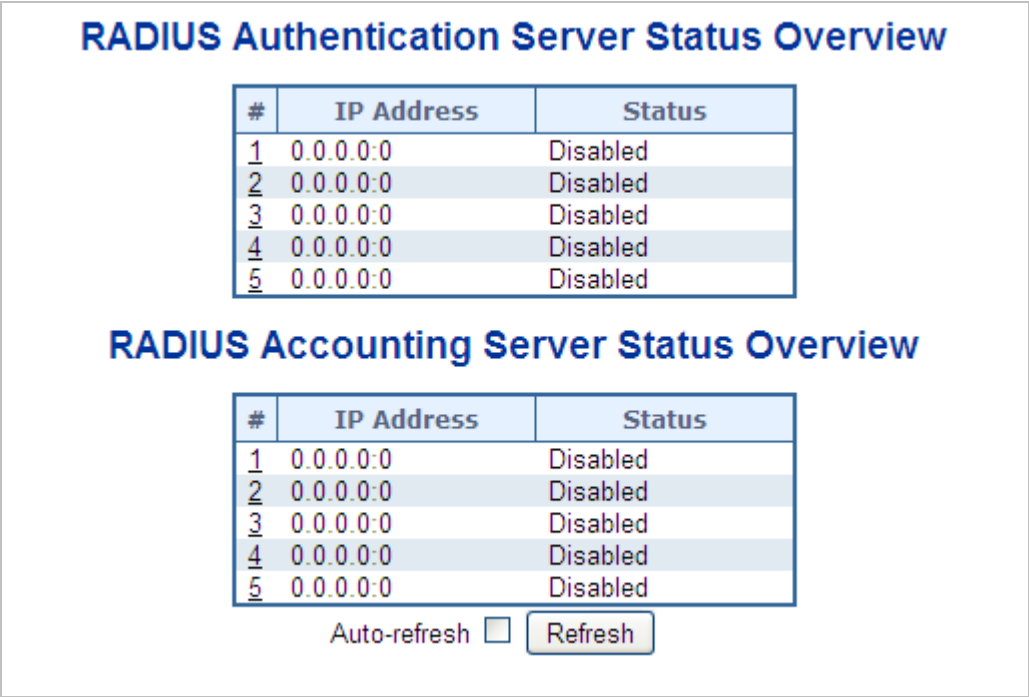


Figure 4-11-9: RADIUS Authentication/Accounting Server Overview Page Screenshot

The Page includes the following fields:

RADIUS Authentication Server Status Overview

Object	Description
<ul style="list-style-type: none">#	The RADIUS server number. Click to navigate to detailed statistics for this server.
<ul style="list-style-type: none">IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
<ul style="list-style-type: none">Status	<div>The current state of the server. This field takes one of the following values:<ul style="list-style-type: none">Disabled: The server is disabled.Not Ready: The server is enabled, but IP communication is not yet up and running.Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily</div>

	been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
--	--

RADIUS Accounting 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	<p>The current state of the server. This field takes one of the following values:</p> <ul style="list-style-type: none"> ■ Disabled: The server is disabled. ■ Not Ready: The server is enabled, but IP communication is not yet up and running. ■ Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. <p>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.</p>

Buttons

Auto-refresh ☐: Check this box to refresh the Page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the Page immediately.

4.11.9 RADIUS Details

This Page provides detailed statistics for a particular RADIUS server. The RADIUS Authentication/Accounting for Server Overview screen in [Figure 4-11-10](#) appears.

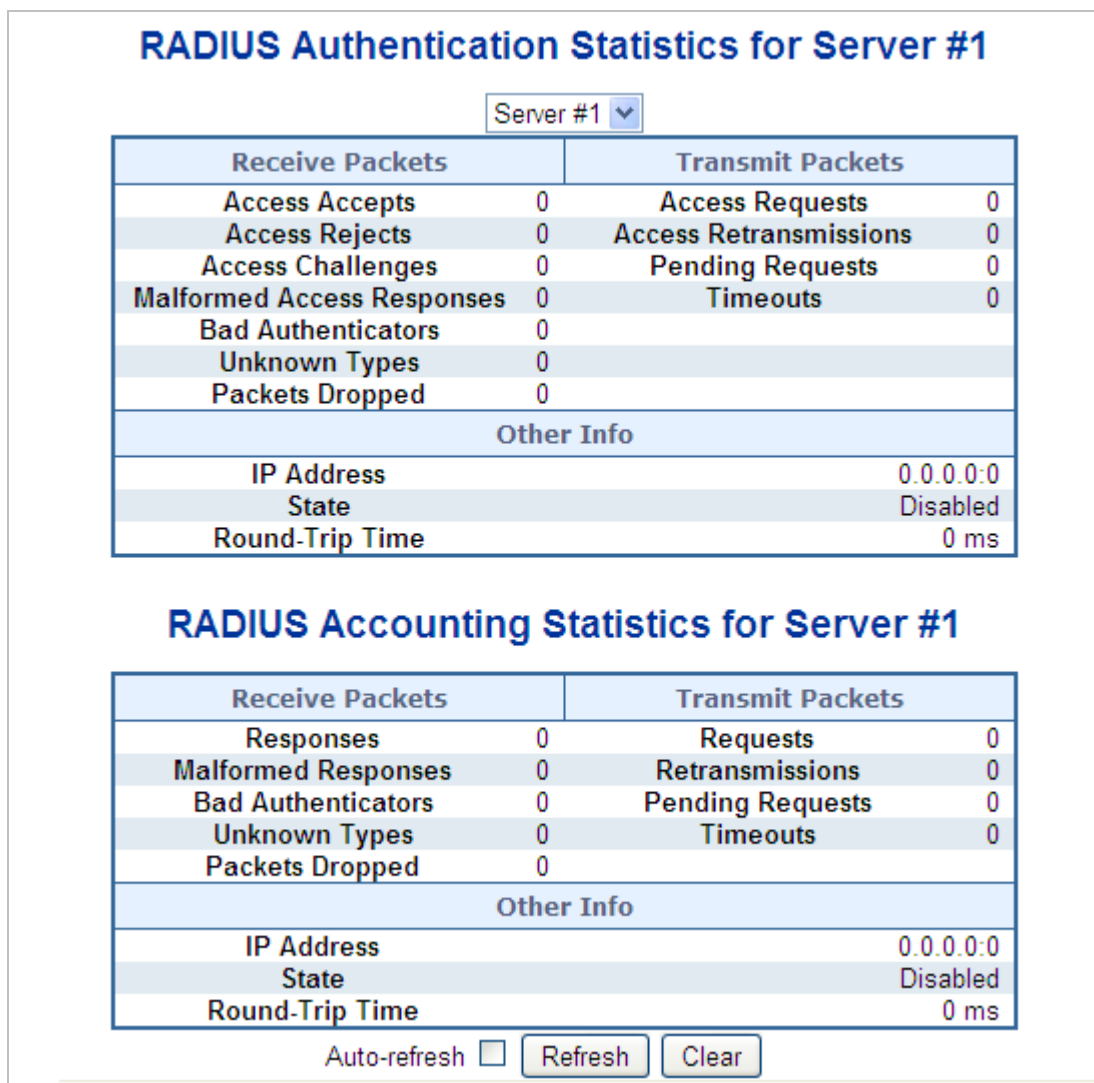


Figure 4-11-10: RADIUS Authentication/Accounting for Server Overview Page Screenshot

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 backend servers to show details for.

Object	Description			
<ul style="list-style-type: none"> Packet Counters 	RADIUS authentication server packet counter. There are seven receive and four transmit counters.			
	Direction	Name	RFC4668 Name	Description
	Rx	Access	radiusAuthClientExtA	The number of RADIUS Access-Accept packets (valid

	Accepts	ccessAccepts	or invalid) received from the server.
Rx	Access Rejects	radiusAuthClientExtA ccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	Access Challenges	radiusAuthClientExtA ccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	Malformed Access Responses	radiusAuthClientExt MalformedAccessRe sponses	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	radiusAuthClientExtB adAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	Unknown Types	radiusAuthClientExtU nknownTypes	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Rx	Packets	radiusAuthClientExtP	The number of RADIUS packets that were received

	Dropped	acketsDropped	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.

<ul style="list-style-type: none"> 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	-	<p>Shows the state of the server. It takes one of the following values:</p> <ul style="list-style-type: none"> ■ 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	RadiusAuthClient ExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

Object	Description
<ul style="list-style-type: none"> Packet Counters 	RADIUS accounting server packet counter. There are five receive and four transmit

counters.

Direction	Name	RFC4670 Name	Description
Rx	Responses	radiusAccClientExt Responses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	radiusAccClientExt MalformedResponses	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.
Rx	Bad Authenticators	radiusAcctClientExt BadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	Unknown Types	radiusAccClientExt UnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radiusAccClientExt PacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	Requests	radiusAccClientExt Requests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	Retransmissions	radiusAccClientExt Retransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.

	Tx	Pending Requests	radiusAccClientExt PendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
	Tx	Timeouts	radiusAccClientExt Timeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
• 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: <ul style="list-style-type: none"> ■ 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

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

Buttons

Auto-refresh ☐: Check this box to refresh the Page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the Page immediately.

: Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

4.12 Security

This section is to control the access of the Managed Switch, includes the user access and management control.

The Security page contains links to the following main topics:

- **Port Limit Control**
- **Access Management**
- **Access Management Statistics**
- **HTTPs**
- **SSH**
- **Port Security Status**
- **Port Security Detail**
- **DHCP Snooping**
- **DHCP Snooping Statistics**
- **IP Source Guard Configuration**
- **IP Source Guard Static Table**
- **ARP Inspection**
- **ARP Inspection Static Table**

4.12.1 Port Limit Control

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

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

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

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

The Port Limit Control Configuration screen in [Figure 4-12-1](#) appears.

Port Security Limit Control Configuration

System Configuration

Mode	Disabled
Aging Enabled	<input type="checkbox"/>
Aging Period	3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<All>	4	<All>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen
13	Disabled	4	None	Disabled	Reopen
14	Disabled	4	None	Disabled	Reopen
15	Disabled	4	None	Disabled	Reopen
16	Disabled	4	None	Disabled	Reopen
17	Disabled	4	None	Disabled	Reopen
18	Disabled	4	None	Disabled	Reopen
19	Disabled	4	None	Disabled	Reopen
20	Disabled	4	None	Disabled	Reopen
21	Disabled	4	None	Disabled	Reopen
22	Disabled	4	None	Disabled	Reopen
23	Disabled	4	None	Disabled	Reopen
24	Disabled	4	None	Disabled	Reopen
25	Disabled	4	None	Disabled	Reopen
26	Disabled	4	None	Disabled	Reopen
27	Disabled	4	None	Disabled	Reopen
28	Disabled	4	None	Disabled	Reopen

Save Reset

Refresh

Figure 4-12-1: Port Limit Control Configuration Overview Page Screenshot

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 checked, secured MAC addresses are subject to aging as discussed under Aging Period.
• Aging Period	<p>If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.</p> <p>The Aging Period can be set to a number between 10 and 10,000,000 seconds. To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.</p>

Port Configuration


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


Object	Description
• Port	The port number for which the configuration below applies.

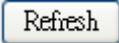
<ul style="list-style-type: none"> • Mode 	<p>The Configuration All with available options will assign to whole ports.</p> <p>Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.</p>
<ul style="list-style-type: none"> • Limit 	<p>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.</p> <p>The stackswitch 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.</p>
<ul style="list-style-type: none"> • Action 	<p>The Configuration All with available options will assign to whole ports.</p> <p>If Limit is reached, the switch can take one of the following actions:</p> <p>None: Do not allow more than Limit MAC addresses on the port, but take no further action.</p> <p>Trap: If Limit + 1 MAC address is seen on the port send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent everytime the limit gets exceeded.</p> <p>Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new 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:</p> <ol style="list-style-type: none"> 1) Boot the stack or elect a new master the switch, 2) Disable and re-enable Limit Control on the port or the stackswitch, 3) Click the Reopen button. <p>Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.</p>
<ul style="list-style-type: none"> • State 	<p>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:</p> <p>Disabled: Limit Control is either globally disabled or disabled on the port.</p> <p>Ready: The limit is not yet reached. This can be shown for all actions.</p> <p>Limit Reached: Indicates that the limit is reached on this port. This state can</p>

	<p>only be shown if Action is set to None or Trap.</p> <p>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.</p>
<ul style="list-style-type: none"> • Reopen Button 	<p>If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section.</p> <p>Note, that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.</p>

Buttons

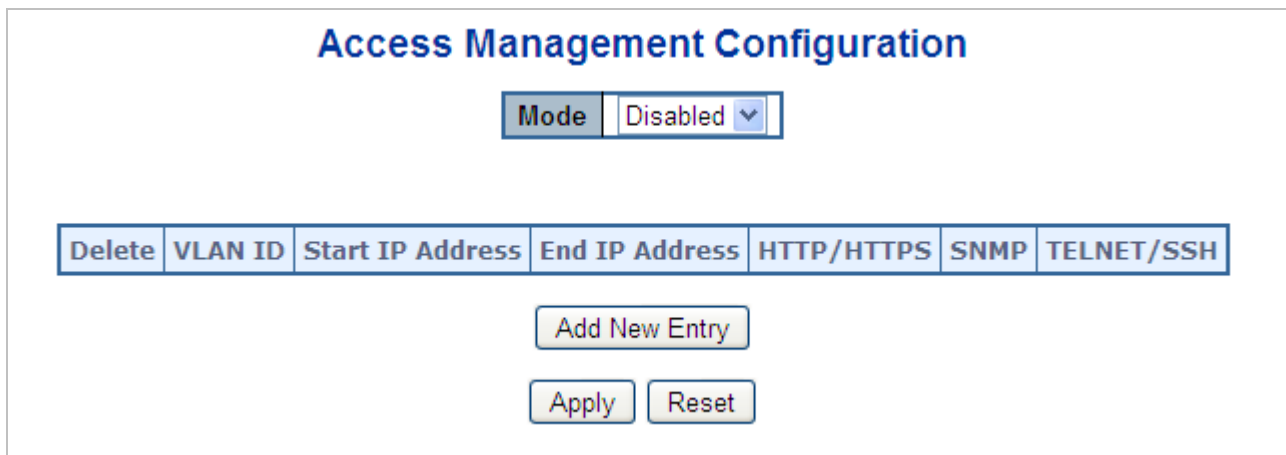
: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

: Click to refresh the page. Note that non-committed changes will be lost.

4.12.2 Access Management

Configure access management table on this 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 Access Management Configuration screen in [Figure 4-12-2](#) appears.



The screenshot shows the 'Access Management Configuration' page. At the top, there is a 'Mode' dropdown menu currently set to 'Disabled'. Below this is a table with columns: 'Delete', 'VLAN ID', 'Start IP Address', 'End IP Address', 'HTTP/HTTPS', 'SNMP', and 'TELNET/SSH'. Under the table, there is an 'Add New Entry' button, and at the bottom, there are 'Apply' and 'Reset' buttons.

Figure 4-12-2: Access Management Configuration Overview Page Screenshot

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.
• End IP address	Indicates the end IP address for the access management entry.
• HTTP/HTTPS	Indicates the host can access the switch from HTTP/HTTPS interface that the host IP address matched the entry.
• SNMP	Indicates the host can access the switch from SNMP interface that the host IP address matched the entry.
• TELNET/SSH	Indicates the host can access the switch from TELNET/SSH interface that the host IP address matched the entry.

Buttons

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

4.12.3 Access Management Statistics

This page provides statistics for access management. The Access Management Statistics screen in [Figure 4-12-3](#) appears.

Access Management Statistics			
Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Auto-refresh ☐ **Refresh** **Clear**

Figure 4-12-3: Access Management Statistics Overview Page Screenshot

The page includes the following fields:

Object	Description
• Interface	The interface that allowed remote host can access the Managed Switch .
• Receive Packets	The received packets number from the interface under access management mode is enabled.
• Allowed 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

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

: Clear all statistics.

4.12.4 HTTPS

Configure HTTPS on this page. The HTTPS Configuration screen in [Figure 4-12-4](#) appears.

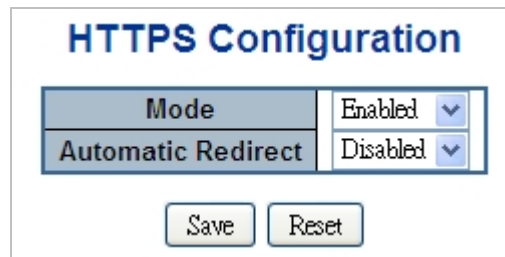


Figure 4-12-4: HTTPS Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Mode	Indicates the HTTPS mode operation. Possible modes are: <ul style="list-style-type: none">■ Enabled: Enable HTTPS mode operation.■ Disabled: Disable HTTPS mode operation.
<ul style="list-style-type: none">• Automatic Redirect	Indicates the HTTPS redirect mode operation. Automatic redirect web browser to HTTPS during HTTPS mode enabled. Possible modes are: <ul style="list-style-type: none">■ Enabled: Enable HTTPS redirect mode operation.■ Disabled: Disable HTTPS redirect mode operation.

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.12.5 SSH

Configure SSH on this page. This page shows the Port Security status. Port Security is a module with no direct configuration.

Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status. The SSH Configuration screen in [Figure 4-12-5](#) appears.





Figure 4-12-5: SSH Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Mode	Indicates the SSH mode operation. Possible modes are: Enabled: Enable SSH mode operation. Disabled: Disable SSH mode operation.

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.12.6 Port Security Status

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status. The Port

Security Status screen in [Figure 4-12-6](#) appears.

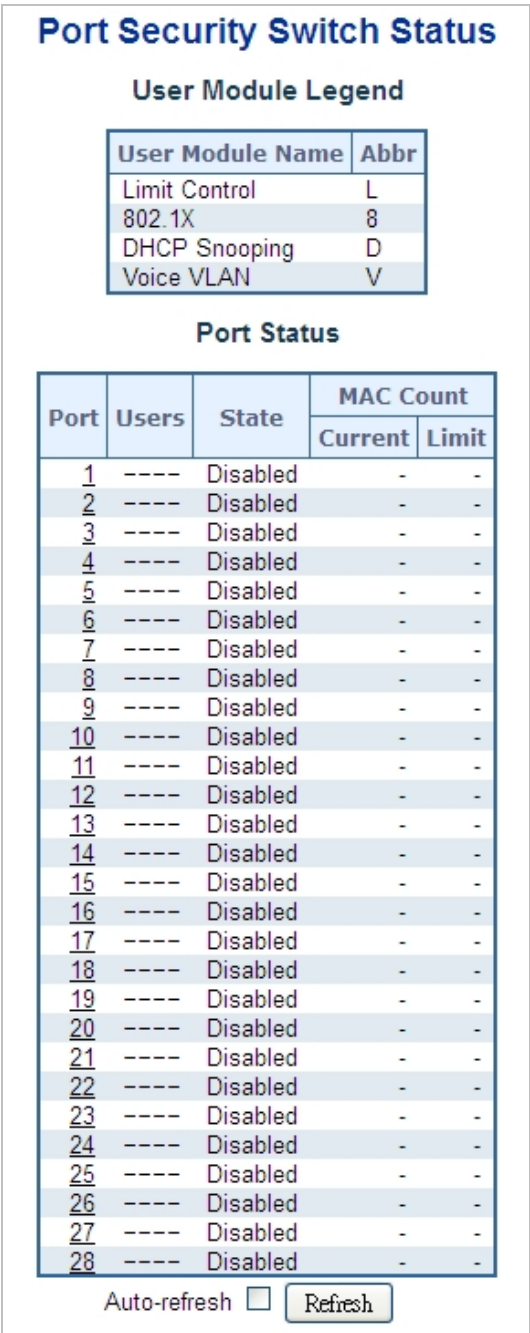


Figure 4-12-6: Port Security Status Screen Page Screenshot

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 whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.
• State	Shows the current state of the port. It can take one of four values: Disabled: No user modules are currently using the Port Security service. Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.
• MAC Count (Current, Limit)	The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh

: Click to refresh the page immediately.

4.12.7 Port Security Detail

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The Port Security Detail screen in [Figure 4-12-7](#) appears.

Port Security Port Status Port 1

Port 1 ▼

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

Auto-refresh ☐ Refresh

Figure 4-12-7: Port Security Detail Screen Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• 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.
<ul style="list-style-type: none">• 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.
<ul style="list-style-type: none">• Time of Addition	Shows the date and time when this MAC address was first seen on the port.
<ul style="list-style-type: none">• Age/Hold	<p>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.</p> <p>If aging is disabled or a user module has decided to hold the MAC address</p>

	indefinitely, a dash (-) will be shown.
--	---

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

4.12.8 DHCP Snooping

DHCP Snooping is used to block intruder 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 this page. The DHCP Snooping Configuration screen in [Figure 4-12-8](#) appears.

DHCP Snooping Configuration

Snooping Mode

Disabled

Port Mode Configuration

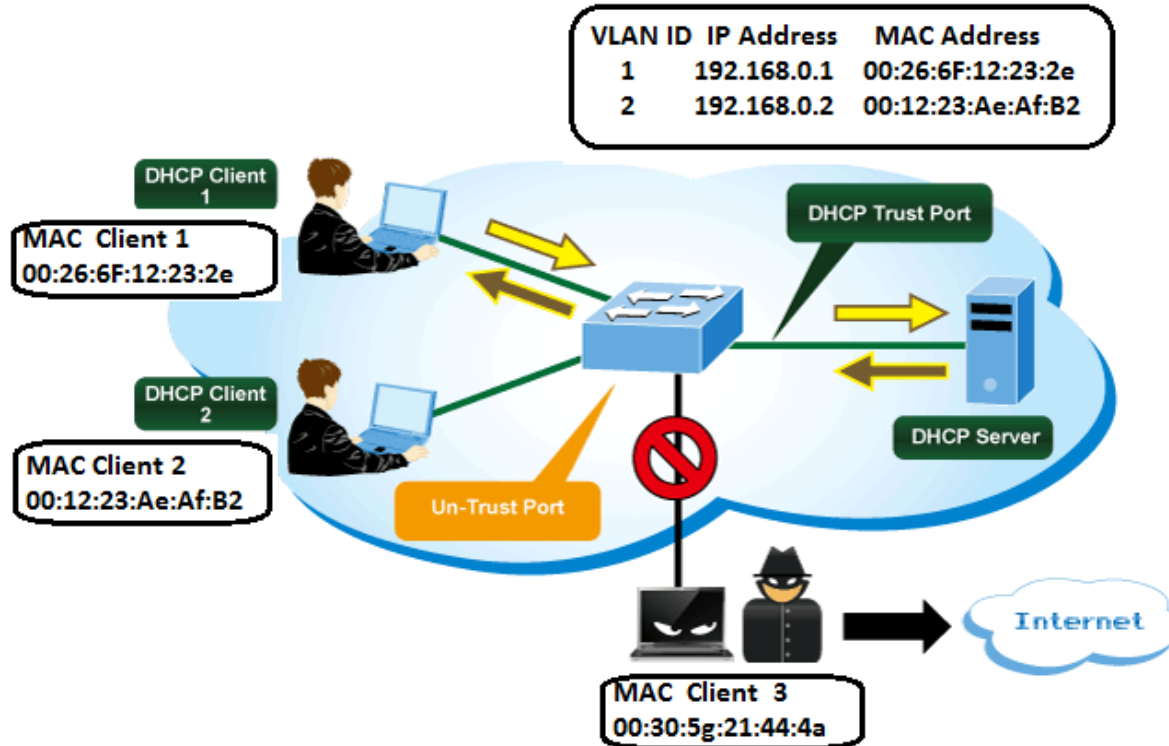
Port	Mode
*	<All>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted
9	Trusted
10	Trusted
11	Trusted
12	Trusted
13	Trusted
14	Trusted
15	Trusted
16	Trusted
17	Trusted
18	Trusted
19	Trusted
20	Trusted
21	Trusted
22	Trusted
23	Trusted
24	Trusted
25	Trusted
26	Trusted
27	Trusted
28	Trusted

Save

Reset

Figure 4-12-8: DHCP Snooping Configuration Screen Page Screenshot


DHCP Snooping Overview




The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Snooping Mode	Indicates the DHCP snooping mode operation. Possible modes are: Enabled : Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. Disabled : Disable DHCP snooping mode operation.
<ul style="list-style-type: none">• Port Mode	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 means all ports will have one specific setting

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.12.9 DHCP Snooping Statistics

This page provides statistics for DHCP snooping. The statistics only counter packet under DHCP snooping mode is enabled and relay mode is disabled. And it doesn't count the DHCP packets for system DHCP client. The DHCP Snooping Port Statistics screen in [Figure 4-12-9](#) appears.

DHCP Snooping Port Statistics Port 1

Port 1 ▼

Receive Packets		Transmit Packets	
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

Auto-refresh ☐
Refresh
Clear

Figure 4-12-9: DHCP Snooping Port Statistics Screen Page Screenshot

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 and Tx NAK	The number of NAK (option 53 with value 6) packets received and transmitted.
• Rx and Tx Release	The number of release (option 53 with value 7) packets received and transmitted.
• Rx and Tx Inform	The number of inform (option 53 with value 8) packets received and transmitted.
• Rx and Tx Lease Query	The number of lease query (option 53 with value 10) packets received and transmitted.
• Rx and Tx Lease Unassigned	The number of lease unassigned (option 53 with value 11) packets received and transmitted.

<ul style="list-style-type: none"> • Rx and Tx Lease Unknown 	The number of lease unknown (option 53 with value 12) packets received and transmitted.
<ul style="list-style-type: none"> • Rx and Tx Lease Active 	The number of lease active (option 53 with value 13) packets received and transmitted.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

: Clears the counters for the selected port.

4.12.10 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. This page provides IP Source Guard related configuration. The IP Source Guard Configuration screen in [Figure 4-12-10](#) appears.

IP Source Guard Configuration

Mode

Disabled

Translate Dynamic to Static

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<All>	<All>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9	Disabled	Unlimited
10	Disabled	Unlimited
11	Disabled	Unlimited
12	Disabled	Unlimited
13	Disabled	Unlimited
14	Disabled	Unlimited
15	Disabled	Unlimited
16	Disabled	Unlimited
17	Disabled	Unlimited
18	Disabled	Unlimited
19	Disabled	Unlimited
20	Disabled	Unlimited
21	Disabled	Unlimited
22	Disabled	Unlimited
23	Disabled	Unlimited
24	Disabled	Unlimited
25	Disabled	Unlimited
26	Disabled	Unlimited
27	Disabled	Unlimited
28	Disabled	Unlimited

Save

Reset

Figure 4-12-10: IP Source Guard Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• Mode of IP Source Guard Configuration	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
• Port Mode Configuration	Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port. All means all ports will have one specific setting.
• Max Dynamic Clients	Specify the maximum number of dynamic clients 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 means only allow the IP packets forwarding that are matched in static entries on the specific port. All means all ports will have one specific setting.

Buttons

Translate dynamic to static : Click to translate all dynamic entries to static entries.

Save : Click to save changes.

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

4.12.11 IP Source Guard Static Table

This page provides Static IP Source Guard Table. The Static IP Source Guard Table screen in [Figure 4-12-11](#) appears.

Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	IP Mask
--------	------	---------	------------	---------

Add New Entry

Save Reset


Figure 4-12-11: Static IP Source Guard Table Screen Page Screenshot


The page includes the following fields:

Object	Description
• Delete	Check to delete the entry. It will be deleted during the next save.
• Port	The logical port for the settings.
• VLAN ID	The VLAN ID for the settings.
• IP Address	Allowed Source IP address.
• MAC address	Allowed Source MAC address.

Buttons

: Click to add a new entry.

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.12.12 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. This page provides ARP Inspection related configuration. The ARP Inspection Configuration screen in [Figure 4-12-12](#) appears.

ARP Inspection Configuration

Mode Disabled ▾

Translate Dynamic to Static

Port Mode Configuration

Port	Mode
*	<All> ▾
1	Disabled ▾
2	Disabled ▾
3	Disabled ▾
4	Disabled ▾
5	Disabled ▾
6	Disabled ▾
7	Disabled ▾
8	Disabled ▾
9	Disabled ▾
10	Disabled ▾
11	Disabled ▾
12	Disabled ▾
13	Disabled ▾
14	Disabled ▾
15	Disabled ▾
16	Disabled ▾
17	Disabled ▾
18	Disabled ▾
19	Disabled ▾
20	Disabled ▾
21	Disabled ▾
22	Disabled ▾
23	Disabled ▾
24	Disabled ▾
25	Disabled ▾
26	Disabled ▾
27	Disabled ▾
28	Disabled ▾

Save

Reset

Figure 4-12-12: ARP Inspection Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• Mode of ARP Inspection Configuration	Enable the Global ARP Inspection or disable the Global ARP Inspection.
• Port Mode Configuration	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. All means all ports will have one specific setting.

Buttons

Translate dynamic to static

: Click to translate all dynamic entries to static entries.

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.12.13 ARP Inspection Static Table

This page provides Static ARP Inspection Table. The Static ARP Inspection Table screen in [Figure 4-12-13](#) appears.

Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
--------	------	---------	-------------	------------

Add New Entry

Save Reset

Figure 4-12-13: Static ARP Inspection Table Screen Page Screenshot


The page includes the following fields:


Object	Description
• Delete	Check to delete the entry. It will be deleted during the next save.
• Port	The logical port for the settings.

• VLAN ID	The VLAN ID for the settings.
• MAC Address	Allowed Source MAC address in ARP request packets.
• IP Address	Allowed Source IP address in ARP request packets.

Buttons

: Click to add a new entry.

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.13 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), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

4.13.1 MAC Address Table Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here. The MAC Address Table Configuration screen in [Figure 4-13-1](#) appears.

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging

☐

Aging Time

300

seconds

MAC Table Learning

	Port Members																											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Static MAC Table Configuration

	Port Members																											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Delete																												
VLAN ID																												
MAC Address																												

Add New Static Entry

Save

Reset

Figure 4-13-1: MAC Address Table Configuration Page Screenshot

The page includes the following fields:

Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Object	Description
• Disable Automatic Aging	Enables/disables the 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	Check to delete the entry. It will be deleted during the next save.
• VLAN ID	The VLAN ID of the entry.
• MAC Address	The MAC address of the entry.
• Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Buttons

Add New Static Entry

: Click to add a new entry.

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.13.2 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. The MAC Address Table screen in [Figure 4-13-2](#) appears.

MAC Address Table

Auto-refresh ☐

Refresh

Clear

<<

>>

Start from VLAN and MAC Address with entries per page.

			Port Members																												
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Static	1	00-55-44-4F-77-30	✓																												
Dynamic	1	00-E0-4C-69-60-84		✓																											
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-55-44-77	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-A8-00-64	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 4-13-2: MAC Address Table Status Page Screenshot

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the **"entries per page"** input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

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

In addition, the two input fields will - upon a **"Refresh"** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

The page includes the following fields:

Object	Description
• Type	Indicates whether 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

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

: Flushes all dynamic entries.

: Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

: Updates the table, starting with the entry after the last entry currently displayed.

4.13.3 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. The Dynamic ARP Inspection Table screen in [Figure 4-13-3](#) appears.

Dynamic ARP Inspection Table

Start from , VLAN , MAC address and IP address with entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			
Auto-refresh <input type="checkbox"/> <input type="button" value="Refresh"/> <input type="button" value="k<"/> <input type="button" value="k>"/>			

Figure 4-13-3: Dynamic ARP Inspection Table Screenshot

Navigating the ARP Inspection Table

Each page shows up to 999 entries from the Dynamic ARP Inspection table, default being 20, selected through the "**entries per page**" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "**Start from port address**", "**VLAN**", "**MAC address**" and "**IP address**" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest

next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a “**Refresh**” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

The page includes the following fields:

Object	Description
• Port	Switch Port Number for which the entries are displayed.
• VLAN ID	VLAN-ID in which the ARP traffic is permitted.
• MAC Address	User MAC address of the entry.
• IP Address	User IP address of the entry.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Refreshes the displayed table starting from the input fields.

: Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

: Updates the table, starting with the entry after the last entry currently displayed.

4.13.4 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 MAC address. The Dynamic IP Source Guard Table screen in [Figure 4-13-4](#) appears.

Dynamic IP Source Guard Table

Start from

Port 1

 , VLAN

1

 and IP address

0.0.0.0

 with

20

 entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

Auto-refresh ☐

Refresh

<<

>>

Figure 4-13-4: Dynamic IP Source Guard Table Screenshot

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "**entries per page**" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table. The "**Start from port address**", "**VLAN**", "**IP address**" and "**IP mask**" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

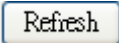
The ">>" will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.


The page includes the following fields:


Object	Description
• Port	Switch Port Number for which the entries are displayed.
• VLAN ID	VLAN-ID in which the IP traffic is permitted.
• IP Address	User IP Address of the entry.
• MAC Address	Source MAC Address.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

: Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

: Updates the table, starting with the entry after the last entry currently displayed.

4.14 LLDP

4.14.1 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 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.

4.14.2 LLDP Configuration

This page allows the user to inspect and configure the current LLDP port settings. The LLDP Configuration screen in [Figure 4-14-1](#) appears.

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> ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
18	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
19	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
21	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
24	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
25	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
26	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
27	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
28	Disabled ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 4-14-1: LLDP Configuration Page Screenshot

The page includes the following fields:

LLDP Parameters

Object	Description
<ul style="list-style-type: none">• Tx Interval	<p>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.</p> <p>Default: 30 seconds</p> <p>This attribute must comply with the following rule:</p> <p>$(\text{Transmission Interval} * \text{Hold Time Multiplier}) \leq 65536$, and $\text{Transmission Interval} \geq (4 * \text{Delay Interval})$</p>
<ul style="list-style-type: none">• Tx Hold	<p>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.</p> <p>TTL in seconds is based on the following rule:</p> <p>$(\text{Transmission Interval} * \text{Holdtime Multiplier}) \leq 65536$.</p> <p>Therefore, the default TTL is $4 * 30 = 120$ seconds.</p>
<ul style="list-style-type: none">• Tx Delay	<p>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.</p> <p>This attribute must comply with the rule:</p> <p>$(4 * \text{Delay Interval}) \leq \text{Transmission Interval}$</p>
<ul style="list-style-type: none">• Tx Reinit	<p>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 isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.</p>

LLDP Port Configuration

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

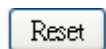
Object	Description
• Port	The switch port number of the logical LLDP port.
• Mode	<p>Select LLDP mode. All means all ports will have one specific setting.</p> <ul style="list-style-type: none">■ Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.■ Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information.■ Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors.■ Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
• CDP Aware	<p>Select CDP awareness.</p> <p>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.</p> <p>Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbours' 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.</p> <p>CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.</p> <p>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.</p> <p>CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.</p> <p>CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.</p> <p>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 neighbours' table.</p> <p>If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbour devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.</p> <p>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.</p>

• Port Description	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
• System Name	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
• System Description	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
• System Capabilities	Optional TLV: When checked 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.
• Management Address	Optional TLV: When checked 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 to save changes.



: Click to undo any changes made locally and revert to previously saved values.

4.14.3 LLDP-MED Configuration

This page allows you to configure the LLDP-MED. The LLDP-MED Configuration screen in [Figure 4-14-2](#) appears.

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count 4

Coordinates Location

Latitude 0 ° North Longitude 0 ° East Altitude 0 Meters Map Datum WGS84

Civic Address Location

Country code		State		County	
City		City district		Block (Neighbourhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

Add New Policy

Figure 4-14-2: LLDP-MED Configuration Page Screenshot

The page includes the following fields:

Fast start repeat count

Object	Description
<ul style="list-style-type: none">• Fast start repeat count	<p>Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPDU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.</p> <p>With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.</p> <p>Because there is a risk that a LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility for that the neighbors has received the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a LLDP frame with new information is received.</p> <p>It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including between Network Connectivity Devices, or to other types of links.</p>

Coordinates Location

Object	Description
<ul style="list-style-type: none"> Latitude 	<p>Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.</p> <p>It is possible to specify the direction to either North of the equator or South of the equator.</p>
<ul style="list-style-type: none"> Longitude 	<p>Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.</p> <p>It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.</p>
<ul style="list-style-type: none"> Altitude 	<p>Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits.</p> <p>It is possible to select between two altitude types (floors or meters).</p> <ul style="list-style-type: none"> ■ Meters: Representing meters of Altitude defined by the vertical datum specified. ■ Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
<ul style="list-style-type: none"> Map Datum 	<p>The Map Datum used for the coordinates given in this Option</p> <ul style="list-style-type: none"> ■ 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, ½
• Landmark	Landmark or vanity address - Example: Columbia University
• Additional location info	Additional location info - Example: South Wing
• Name	Name (residence and office occupant) - Example: Flemming Jahn
• Zip code	Postal/zip code - Example: 2791
• Building	Building (structure) - Example: Low Library
• Apartment	Unit (Apartment, suite) - Example: Apt 42
• Floor	Floor - Example: 4
• Room no.	Room number - Example: 450F
• Place type	Place type - Example: Office
• Postal community name	Postal community name - Example: Leonia
• P.O. Box	Post office box (P.O. BOX) - Example: 12345
• Additional code	Additional code - Example: 1320300003

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

Object	Description
<ul style="list-style-type: none">• Emergency Call Service	Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

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

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

The network policy attributes advertised are:

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

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

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

A large network may support multiple VoIP policies across the entire organization, and different policies per application type.

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

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

Object	Description
• Delete	Check to delete the policy. It will be deleted during the next save.
• Policy ID	ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific ports.
• Application Type	<p>Intended use of the application types:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Video Conferencing</p> <p>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.</p> <p>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.</p>
• Tag	Tag indicating whether the specified application type is using a 'tagged' or an

	<p>'untagged' VLAN.</p> <p>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.</p> <p>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.</p>
• 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.

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

Buttons

Add New Policy: click to add new policy.

Save: Click to save changes.

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

4.14.4 LLDP-MED Neighbor

This page provides a status overview for all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP-MED Neighbor Information screen in [Figure 4-14-3](#) appears. The columns hold the following information:



Figure 4-14-3: LLDP-MED Neighbor Information with no LLDP-MED device detected

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=0-0-046 Voice Signaling=Defined=Untagged=0-0-032					
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 links, Symmetric PAUSE for full-duplex links		100BaseTXFD - 2 pair category 5 UTP, full duplex mode	
Auto-refresh <input type="checkbox"/> <button>Refresh</button>					

Figure 4-14-4: LLDP-MED Neighbor Information with LLDP-MED device detected

The page includes the following fields:

Fast start repeat count

Object	Description
<ul style="list-style-type: none">Port	The port on which the LLDP frame was received.
<ul style="list-style-type: none">Device Type	<p>LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.</p> <p>LLDP-MED Network Connectivity Device Definition</p> <p>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:</p> <ol style="list-style-type: none">1. LAN Switch/Router2. IEEE 802.1 Bridge3. 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. Fore-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP

	<p>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.</p> <p>Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management</p>
<ul style="list-style-type: none"> • LLDP-MED Capabilities 	<p>LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities.</p> <p>The possible capabilities are:</p> <ol style="list-style-type: none"> 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
<ul style="list-style-type: none"> • Application Type 	<p>Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device.</p> <p>The possible application types are shown below.</p> <p>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.</p> <p>Voice Signaling - for use in network topologies that require a different policy for the voice signaling than for the voice media.</p> <p>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.</p> <p>Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.</p> <p>Softphone Voice - for use by softphone applications on typical data centric</p>

	<p>devices, such as PCs or laptops.</p> <p>Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.</p> <p>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.</p> <p>Video Signaling - for use in network topologies that require a separate policy for the video signaling than for the video media.</p>
• Policy	<p>Policy</p> <p>Unknown: The network policy for the specified application type is currently unknown.</p> <p>Defined: The network policy is defined.</p>
• TAG	<p>TAG is indicating whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged</p> <p>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.</p> <p>Tagged: The device is using the IEEE 802.1Q tagged frame format</p>
• VLAN ID	<p>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.</p>
• Priority	<p>Priority is the Layer 2 priority to be used for the specified application type. One of eight priority levels (0 through 7)</p>
• DSCP	<p>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).</p>
• Auto-negotiation	<p>Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.</p>
• Auto-negotiation status	<p>Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.</p>

<ul style="list-style-type: none"> • Auto-negotiation Capabilities 	Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.
--	--

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

4.14.5 Neighbor

This 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 LLDP Neighbor Information screen in [Figure 4-14-4](#) appears.

LLDP Neighbour Information						
Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
Port 1	00-6F-32-A5-E3-4B	1	Realtek Intelligent Switch		Bridge(+)	192.168.0.100 (IPv4)
Port 2	SEP0017E01C9FF9	Port 1			Other(+)	
Port 2	0.0.0.0	0017E01C9FF9:P1	SEP0017E01C9FF9.cisco.com	SW PORT	Bridge(+), Telephone(+)	
Auto-refresh <input type="checkbox"/> <input type="button" value="Refresh"/>						

Figure 4-14-4: LLDP Neighbor Information Page Screenshot

The page includes the following fields:

Object	Description
• Local Port	The port on which the LLDP frame was received.
• Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
• Remote Port ID	The Remote Port ID is the identification of the neighbor port.
• System Name	System Name is the name advertised by the neighbor unit.
• Port Description	Port Description is the port description advertised by the neighbor unit.
• System Capabilities	<p>System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:</p> <ol style="list-style-type: none">1. Other2. Repeater3. Bridge4. WLAN Access Point5. Router6. Telephone7. DOCSIS cable device8. Station only9. Reserved <p>When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).</p>
• Management Address	Management Address is 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

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

4.14.6 Port Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refer to counters for the currently selected switch. The LLDP Statistics screen in [Figure 4-14-5](#) appears.

LLDP Global Counters

Global Counters	
Neighbour entries were last changed 1970-01-01 Thu 00:00:00+00:00 (16628 secs. ago)	
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0

Auto-refresh ☐

Figure 4-14-5: LLDP Statistics Page Screenshot

The page includes the following fields:

Global Counters

Object	Description
• Neighbor entries were last changed at	It also 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 that the entry table was full.
• Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

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.

<ul style="list-style-type: none"> • Age-Outs 	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.
---	--

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

: Clears the local counters. All counters (including global counters) are cleared upon reboot.

4.15 Diagnostics

This section provide the Physical layer and IP layer network diagnostics tools for troubleshoot. The diagnostic tools are designed for network manager to help them quickly diagnose problems between point to point 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:

This section has the following items:

- **Ping**
- **IPv6 Ping**
- **Remote IP Ping**
- **Cable Diagnostics**

PING

The ping and IPv6 ping allow you to issue ICMP PING packets to troubleshoot IP connectivity issues. The Managed Switch transmits ICMP packets, and the sequence number and roundtrip time are displayed upon reception of a reply.

Cable Diagnostics

The Cable Diagnostics is performing 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 statuses as follow:

- 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.
- If the link is established in 100Base-TX or 10Base-T, the Cable Diagnostics cause the link to drop while the diagnostics are running.

After the diagnostics are finished, the link is reestablished. And the following functions are available.

- Coupling between cable pairs.
- Cable pair termination
- Cable Length

4.15.1 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you press “**Start**”, 5 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 ICMP Ping screen in [Figure 4-15-1](#) appears.

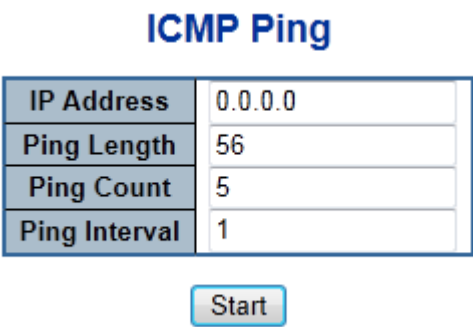


Figure 4-15-1: ICMP Ping Page Screenshot

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.
• Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
• Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.



Be sure the target IP Address is within the same network subnet of the switch, or you have set up the correct gateway IP address.

Button

Start: Click to start transmitting ICMP packets.

New Ping: Click to re-start diagnostics with PING.

4.15.2 IPv6 Ping

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you press “**Start**”, 5 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 ICMPv6 Ping screen in [Figure 4-15-2](#) appears.

ICMPv6 Ping

IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1

Start

Figure 4-15-2: ICMPv6 Ping Page Screenshot

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.
• Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
• Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Button

- Start: Click to start transmitting ICMP packets.
- New Ping: Click to re-start diagnostics with PING.

4.15.3 Remote IP Ping Test

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues on special port.

After you press “**Test**”, 5 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 ICMP Ping screen in [Figure 4-15-3](#) appears.

Remote IP Ping Test


Port	Remote IP Address	Ping Size	Ping Button	Result
1	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
2	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
3	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
4	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
5	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
6	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
7	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
8	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
9	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
10	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
11	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
12	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
13	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
14	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
15	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
16	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
17	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
18	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
19	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
20	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
21	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
22	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
23	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
24	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
25	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
26	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
27	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	
28	<input type="text" value="0.0.0.0"/>	<input type="text" value="64"/>	<input type="button" value="Ping"/>	


Figure 4-15-3: Remote IP Ping Test Page Screenshot


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 to start ping process.

 : Click to save changes.

 : Click to undo any changes made locally and revert to previously saved values.

 : Clears the local counters. All counters (including global counters) are cleared upon reboot.

4.15.4 Cable Diagnostics

This page is used for running the Cable Diagnostics.

Press to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that Cable Diagnostics is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running cable diagnostic. Therefore, running cable diagnostic on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete. The ports belong to the currently selected stack unit, as reflected by the page header. The VeriPHY Cable Diagnostics screen in [Figure 4-15-4](#) appears.

VeriPHY Cable Diagnostics

Port

All

Download

Start

Print

Cable Status									
Port	Description	Pair A(1,2)	Length A	Pair B(3,6)	Length B	Pair C(4,5)	Length C	Pair D(7,8)	Length D
1		--	--	--	--	--	--	--	--
2		--	--	--	--	--	--	--	--
3		--	--	--	--	--	--	--	--
4		--	--	--	--	--	--	--	--

Auto-refresh

☐

Refresh

Figure 4-15-4: VeriPHY Cable Diagnostics Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">Port	The port where you are requesting Cable Diagnostics. Please be noticed that it is only affect to copper port, not fiber port.
<ul style="list-style-type: none">Cable Status	Port : Port number. Pair : The status of the cable pair. Length : The length (in meters) of the cable pair.

Buttons

Start

: Click to run the diagnostics.

4.16 Loop Protection

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

4.16.1 Configuration

This page allows the user to inspect the current Loop Protection configurations,

General Settings

Global Configuration		
Enable Loop Protection	Disable <input type="button" value="v"/>	
Transmission Time	5	seconds
Shutdown Time	180	seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	<input type="checkbox"/>	<All> <input type="button" value="v"/>	<All> <input type="button" value="v"/>
1	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
2	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
3	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
4	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
5	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
6	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
7	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
8	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
9	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
10	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
11	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
12	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
13	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
14	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
15	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
16	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
17	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
18	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
19	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
20	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
21	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
22	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
23	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
24	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
25	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
26	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
27	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>
28	<input checked="" type="checkbox"/>	Shutdown Port <input type="button" value="v"/>	Enable <input type="button" value="v"/>

Figure 4-16-1: Loop Protection Configuration Page Screenshot

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

Port Configuration:

Object	Description
• Port	The switch port number of the port.
• Enable	Controls whether loop protection is enabled on this switch port.
• Action	Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port , Shutdown Port and Log or Log Only .
• Tx Mode	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.16.2 Status

This page displays the loop protection port status the ports from the Managed Switch.

Loop Protection Status

Auto-refresh ☐

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

Figure 4-16-2: Loop Protection Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Action	The currently configured port action.
• Transmit	The currently configured port transmit mode.
• Loops	The number of loops detected on this port.
• Status	The current loop protection status of the port.
• Loop	Whether a loop is currently detected on the port.
• Time of Last Loop	The time of the last loop event detected.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

4.17 RMON

RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

MID of RMON consists of 10 groups. The switch supports the most frequently used group 1, 2, 3 and 9:

- **Statistics:** Maintain basic usage and error statistics for each subnet monitored by the Agent.
- **History:** Record periodical statistic samples available from Statistics.
- **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 RMON Agent.

Alarm depends on the implementation of Event. Statistics and History display some 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).

4.17.1 RMON Alarm Configuration

Configure RMON Alarm table on this page. The entry index key is **ID**; screen in [Figure 4-17-1](#) appears.

RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
--------	----	----------	----------	-------------	-------	---------------	------------------	--------------	-------------------	---------------

Figure 4-18-1: RMON Alarm configuration page screenshot

The page includes the following fields:

Object	Description
• Delete	Check to delete the entry. It will be deleted during the next save.
• ID	Indicates the index of the entry. The range is from 1 to 65535.
• Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.

• Variable	<p>Indicates the particular variable to be sampled, the possible variables are:</p> <ul style="list-style-type: none"> ■ InOctets: The total number of octets received on the interface, including framing characters. ■ InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol. ■ InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. ■ InDiscards: The number of inbound packets that are discarded even the packets are normal. ■ InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. ■ InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol. ■ OutOctets: The number of octets transmitted out of the interface , including framing characters. ■ OutUcastPkts: The number of uni-cast packets that request to transmit. ■ OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit. ■ OutDiscards: The number of outbound packets that are discarded event the packet is normal. ■ OutErrors: The The number of outbound packets that could not be transmitted because of errors. ■ OutQLen: The length of the output packet queue (in packets).
• Sample Type	<p>The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:</p> <ul style="list-style-type: none"> ■ 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	<p>The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:</p> <ul style="list-style-type: none"> ■ 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. ■ RisingOrFalling Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
• Rising Threshold	Rising threshold value (-2147483648-2147483647).
• Rising Index	Rising event index (1-65535).

• Falling Threshold	Falling threshold value (-2147483648-2147483647)
• Falling Index	Falling event index (1-65535).

Buttons

Add New Entry

: Click to add a new community entry.

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.17.2 RMON Alarm Status

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table; screen in [Figure 4-17-2](#) appears.

Port Statistics Overview									
Auto-refresh <input type="checkbox"/> Refresh << >>									
Start from Control Index 0 with 20 entries per page.									
ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

Figure 4-17-2: Port Statistics Overview page screenshot

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

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediate.

: Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

: Updates the table, starting with the entry after the last entry currently displayed.

4.17.3 RMON Event Configuration

Configure RMON Event table on this page. The entry index key is **ID**; screen in [Figure 4-17-3](#) appears.

RMON Event Configuraton

Delete	ID	Desc	Type	Community	Event Last Time
--------	----	------	------	-----------	-----------------

Figure 4-17-3: RMON event configuration page screenshot

The page includes the following fields:

Object	Description
• Delete	Check to delete the entry. It will be deleted during the next save.
• ID	Indicates the index of the entry. The range is from 1 to 65535.
• Desc	Indicates this event, the string length is from 0 to 127, default is a null string.
• Type	Indicates the notification of the event, the possible types are: <ul style="list-style-type: none"> ■ none: The total number of octets received on the interface, including framing characters. ■ log: The number of uni-cast packets delivered to a higher-layer protocol. ■ snmptrap: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. ■ logandtrap: The number of inbound packets that are discarded even the packets are normal.
• Community	Specify the community when trap is sent, the string length is from 0 to 127, default is "public".

• Event Last Time	Indicates the value of sysUpTime at the time this event entry last generated an event.
--------------------------	--

Buttons

Add New Entry: Click to add a new community entry.

Save: Click to save changes.

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

4.17.4 RMON Event Status

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table; screen in [Figure 4-17-4](#) appears.

RMON Event Overview

Auto-refresh ☐ **Refresh** **<<** **>>**

Start from Control Index and Sample Index with entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

Figure 4-17-4: RMON Event Overview page screenshot

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

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediate.

: Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

: Updates the table, starting with the entry after the last entry currently displayed.

4.17.5 RMON History Configuration

Configure RMON History table on this page. The entry index key is **ID**; screen in [Figure 4-17-5](#) appears.

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
--------	----	-------------	----------	---------	-----------------

Figure 4-17-5: RMON history configuration page screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Delete	Check to delete the entry. It will be deleted during the next save.
<ul style="list-style-type: none">• ID	Indicates the index of the entry. The range is from 1 to 65535.
<ul style="list-style-type: none">• Data Source	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005.
<ul style="list-style-type: none">• Interval	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
<ul style="list-style-type: none">• Buckets	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.
<ul style="list-style-type: none">• Buckets Granted	The number of data shall be saved in the RMON.

Buttons

: Click to add a new community entry.

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.17.6 RMON History Status

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table; screen in [Figure 4-17-6](#) appears.

RMON History Overview

Auto-refresh ☐ **Refresh** << >>

Start from Control Index and Sample Index with entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

Figure 4-17-6: RMON history overview page screenshot

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 total number of events in which packets were dropped by the probe due to lack of resources.
• Drops	The total number of events in which packets were dropped by the probe due to lack of resources.
• Octets	The total number of octets of data (including those in bad packets) received on the network.
• Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
• Broadcast	The total number of good packets received that were directed to the broadcast address.
• Multicast	The total number of good packets received that were directed to a multicast address.

• CRCErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.
• Undersize	The total number of packets received that were less than 64 octets.
• Oversize	The total number of packets received that were longer than 1518 octets.
• Frag.	The number of frames which size is less than 64 octets received with invalid CRC.
• Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC.
• Coll.	The best estimate of the total number of collisions on this Ethernet segment.
• Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediate.

: Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

: Updates the table, starting with the entry after the last entry currently displayed.

4.17.7 RMON Statistics Configuration

Configure RMON Statistics table on this page. The entry index key is **ID**; screen in [Figure 4-17-7](#) appears.

RMON Statistics Configuration

Delete	ID	Data Source
Add New Entry	Save	Reset

Figure 4-17-7: RMON Statistics Configuration Page screenshot

The page includes the following fields:

Object	Description
• Delete	Check to delete the entry. It will be deleted during the next save.
• ID	Indicates the index of the entry. The range is from 1 to 65535.

<ul style="list-style-type: none"> • Data Source 	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005
--	---

Buttons

Add New Entry: Click to add a new community entry.

Save: Click to save changes.

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

4.17.8 RMON Statistics Status

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table; screen in [Figure 4-17-8](#) appears.

RMON Statistics Status Overview

Auto-refresh ☐

Refresh

<<

>>

Start from Control Index with entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

Figure 4-17-8: RMON Statistics Status page screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • ID 	Indicates the index of Statistics entry.
<ul style="list-style-type: none"> • Data Source (ifIndex) 	The port ID which wants to be monitored.
<ul style="list-style-type: none"> • Drop 	The total number of events in which packets were dropped by the probe due to lack of resources.
<ul style="list-style-type: none"> • Octets 	The total number of octets of data (including those in bad packets) received on the network.
<ul style="list-style-type: none"> • Pkts 	The total number of packets (including bad packets, broadcast packets, and

	multicast packets) received.
• Broad-cast	The total number of good packets received that were directed to the broadcast address.
• Multi-cast	The total number of good packets received that were directed to a multicast address.
• CRC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
• Under-size	The total number of packets received that were less than 64 octets.
• Over-size	The total number of packets received that were longer than 1518 octets.
• Frag.	The number of frames which size is less than 64 octets received with invalid CRC.
• Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC.
• Coll.	The best estimate of the total number of collisions on this Ethernet segment.
• 64	The total number of packets (including bad packets) received that were 64 octets in length.
• 65~127	The total number of packets (including bad packets) received that were from 65 to 127 octets in length.
• 128~255	The total number of packets (including bad packets) received that were from 128 to 255 octets in length.
• 256~511	The total number of packets (including bad packets) received that were from 256 to 511 octets in length.
• 512~1023	The total number of packets (including bad packets) received that were from 512 to 1023 octets in length.
• 1024~1588	The total number of packets (including bad packets) received that were from 1024 to 1588 octets in length.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 6 seconds.

: Click to refresh the page immediate.

: Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

: Updates the table, starting with the entry after the last entry currently displayed.

4.18 PTP

4.18.1 PTP Configuration

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems. This page allows the user to configure and inspect the current PTP clock settings.

PTP External Clock Mode

One_PPS_Mode	Disable
External Enable	False
VCXO Enable	False
Clock Frequency	1

PTP Clock Configuration

			Port List																											
Delete	Clock Instance	Device Type	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No Clock Instances Present																														

Add New PTP Clock

Save

Reset

Figure 4-18-1: PTP External Clock Mode page screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">One_PPS_Mode	<p>This Selection box will allow you to select the One_pps_mode configuration.</p> <p>The following values are possible:</p> <ol style="list-style-type: none">Output : Enable the 1 pps clock outputInput : Enable the 1 pps clock inputDisable : Disable the 1 pps clock in/out-put
<ul style="list-style-type: none">External Enable	<p>This Selection box will allow you to configure the External Clock output.</p> <p>The following values are possible:</p> <ol style="list-style-type: none">True : Enable the external clock outputFalse : Disable the external clock output
<ul style="list-style-type: none">VCXO_Enable	<p>This Selection box will allow you to configure the External VCXO rate adjustment.</p> <p>The following values are possible:</p>

	1. True : Enable the external VCXO rate adjustment 2. False : Disable the external VCXO rate adjustment
• Clock Frequency	This will allow setting the Clock Frequency. The possible range of values are 1 - 25000000 (1 - 25MHz)

4.18.2 PTP Status

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems. This page allows the user to configure and inspect the current PTP clock settings.

PTP External Clock Mode

One_PPS_Mode	Disable
External Enable	False
VCXO Enable	False
Clock Frequency	1

PTP Clock Configuration

Auto-refresh ☐

		Port List																											
Clock Instance	Device Type	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No Clock Instances Present																													

Figure 4-18-2: PTP Clock configuration page screenshot

The page includes the following fields:

Object	Description
• One_pps_mode	Shows the current One_pps_mode configured. 1. Output : Enable the 1 pps clock output 2. Input : Enable the 1 pps clock input 3. Disable : Disable the 1 pps clock in/out-put
• External Enable	Shows the current External clock output configuration. 1. True : Enable the external clock output 2. False : Disable the external clock output
• VCXO_Enable	Shows the current VCXO rate adjustment configuration.

	1. True : Enable the external VCXO rate adjustment 2. False : Disable the external VCXO rate adjustment
• Clock Frequency	Shows the current clock frequency used by the External Clock. The possible range of values are 1 - 25000000 (1 - 25MHz)
• Clock Instance	Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to monitor the Clock details
• Device Type	Indicates the Type of the Clock Instance. There are five Device Types. <ol style="list-style-type: none"> 1. Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock. 3. E2e Transp - Clock's Device Type is End to End Transparent Clock. 4. Master Only - Clock's Device Type is Master Only. 5. Slave Only - Clock's Device Type is Slave Only.
• Port List	Shows the ports configured for that Clock Instance.

Buttons

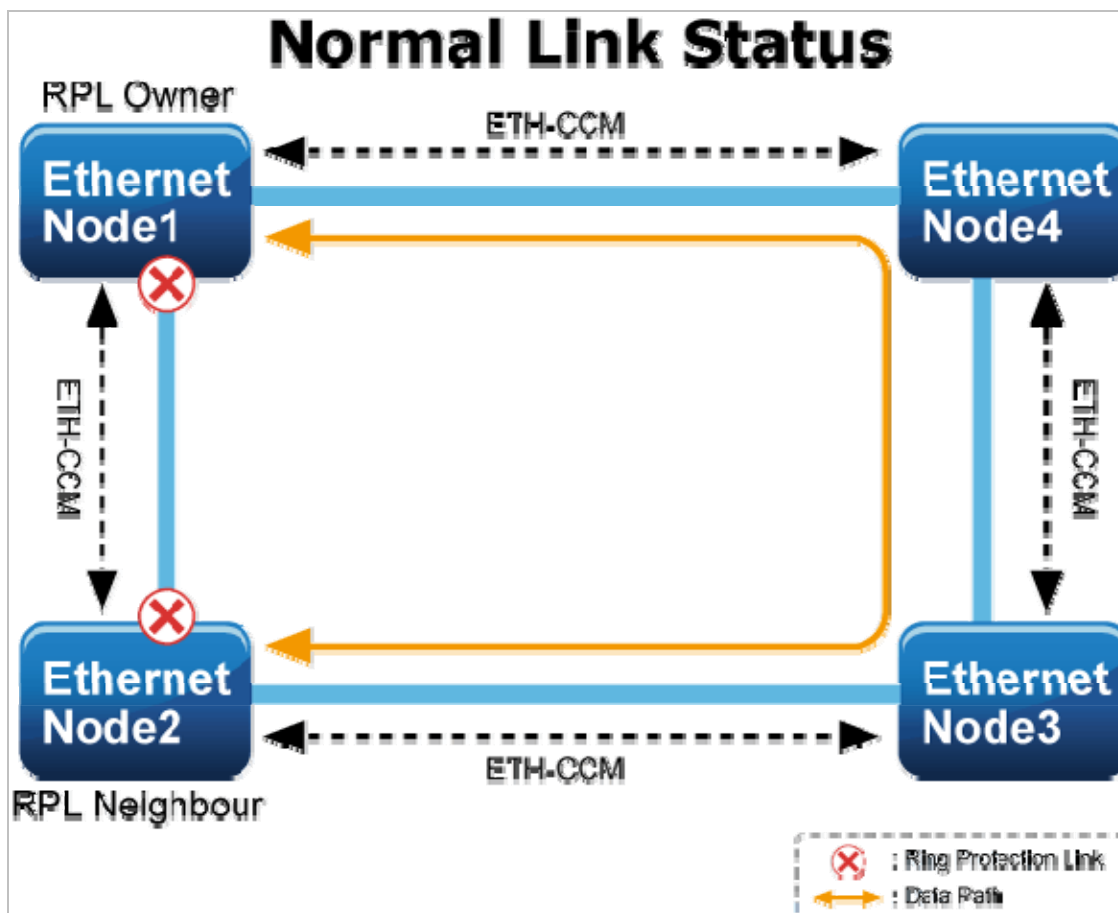
Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 6 seconds.

: Click to refresh the page immediately.

4.19 Ring

ITU-T G.8032 **Ethernet Ring protection switching (ERPS)** is a link layer protocol applied on Ethernet loop protection to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology.

ERPS provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the Ring topology, every switch should be enabled with Ring function and two ports should be assigned as the member ports in the ERPS. Only one switch in the Ring group would be set as the RPL owner switch in which one port, called **owner port**, would be blocked, and PRL neighbour switch has one port in which one port, called **neighbour port**, would be blocked. The **neighbour port** is connected to the owner port directly and this link is called the **Ring Protection Link** or **RPL**. Each switch will send ETH-CCM message to check the link status in the ring group. When the failure of network connection occurs, the nodes block the failed link and report the signal failure message. The RPL owner switch will automatically unblock the PRL to recover from the failure.



• Delete	This box is used to mark an MEP for deletion in next Save operation.
• Instance	The ID of the MEP. Click on the ID of an MEP to enter the configuration page.
• Domain	<p>Port: This is an MEP in the Port Domain. 'Flow Instance' is a Port.</p> <p>Esp: Future use</p> <p>Evc: This is an MEP in the EVC Domain. 'Flow Instance' is an EVC</p> <p>Mpls: Future use</p>
• Mode	<p>MEP: This is a Maintenance Entity End Point.</p> <p>MIP: This is a Maintenance Entity Intermediate Point.</p>
• Direction	<p>Ingress: This is an Ingress (down) MEP - monitoring ingress traffic on 'Residence Port'.</p> <p>Egress: This is an Egress (up) MEP - monitoring egress traffic on 'Residence Port'.</p>
• Residence Port	The port where MEP is monitoring - see 'Direction'.
• Level	The MEG level of this MEP.
• Flow Instance	The MEP is related to this flow - See 'Domain'.
• Tagged VID	<p>Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID.</p> <p>Entering '0' means no TAG added.</p>
• This MAC	The MAC of this MEP can be used by other MEPs when unicast is selected (Info only).
• Alarm	There is an active alarm on the MEP.

Buttons

Add New MEP

: Click to add a new MEP entry

Refresh

: Click to refresh the page immediately.

Save

: Click to save changes.

Reset

: Click to undo any changes made locally and revert to previously saved values.

4.19.2 Detailed MEP Configuration

This page allows the user to inspect and configure the current MEP Instance.; screen in [Figure 4-19-2](#) appears.

MEP Configuration

Refresh

Instance Data

MEP Instance	Domain	Mode	Direction	Residence Port	Flow Instance	Tagged VID	EPS Instance	This MAC
1	Port	Mep	Ingress	1	1	3001	1	00-30-4F-B6-56-8E

Instance Configuration

Level	Format	ICC/Domain Name	MEG ID	MEP ID	Tagged VID		cLevel	cMEG	cMEP	cAIS	cLCK	cSSF	aBLK	aTSF
0	ITU ICC		exp00meg0C	1	3001									

Peer MEP Configuration

Delete	Peer MEP ID	Unicast Peer MAC		cLOC	cRDI	cPeriod	cPriority
<input type="checkbox"/>	6	00-00-00-00-00-00					

Add New Peer MEP

Functional Configuration

Continuity Check				APS Protocol				
Enable	Priority	Frame rate		Enable	Priority	Cast	Type	Last Octet
<input checked="" type="checkbox"/>	0	1 f/sec		<input checked="" type="checkbox"/>	0	Multi	R-APS	1

SaveReset

Figure 4-19-2: Detailed MEP configuration page screenshot

The page includes the following fields:

Instance Data:

Object	Description
• MEP Instance	The ID of the MEP.
• Domain	See help on MEP create WEB.
• Mode	See help on MEP create WEB.
• Direction	See help on MEP create WEB.
• Residence Port	See help on MEP create WEB.
• Flow Instance	See help on MEP create WEB.

• Tagged VID	See help on MEP create WEB.
• This MAC	See help on MEP create WEB.

Instance Configuration:

Object	Description
• Level	See help on MEP create WEB.
• Format	<p>This is the configuration of the two possible Maintenance Association Identifier formats.</p> <p>ITU ICC: This is defined by ITU. 'ICC' can be max. 6 char. 'MEG id' can be max. 7 char.</p> <p>IEEE String: This is defined by IEEE. 'Domain Name' can be max. 8 char. 'MEG id' can be max. 8 char.</p>
• ICC/Domain Name	This is either ITU ICC (MEG ID value[1-6]) or IEEE Maintenance Domain Name - depending on 'Format'. See 'Format'.
• MEG Id	This is either ITU UMC (MEG ID value[7-13]) or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this can be max. 7 char. If only 6 char. is entered the MEG ID value[13] will become NULL.
• MEP Id	This value will become the transmitted two byte CCM MEP ID.
• cLevel	Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.
• cMEG	Fault Cause indicating that a CCM is received with an MEG ID different from configured for this MEP.
• cMEP	Fault Cause indicating that a CCM is received with an MEP ID different from all 'Peer MEP ID' configured for this MEP.
• cAIS	Fault Cause indicating that AIS PDU is received.
• cLCK	Fault Cause indicating that LCK PDU is received.
• cSSF	Fault Cause indicating that server layer is indicating Signal Fail.
• aBLK	The consequent action of blocking service frames in this flow is active.
• aTSF	The consequent action of indicating Trail Signal Fail to-wards protection is active.
• Delete	This box is used to mark a Peer MEP for deletion in next Save operation.
• Peer MEP ID	This value will become an expected MEP ID in a received CCM - see 'cMEP'.

• Unicast Peer MAC	This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.
• cLOC	Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP.
• cRDI	Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.
• cPeriod	Fault Cause indicating that a CCM is received with a period different from what is configured for this MEP - from this peer MEP.
• cPriority	Fault Cause indicating that a CCM is received with a priority different from what is configured for this MEP - from this peer MEP.

Buttons

Add New Peer MEP

: Click to add a new peer MEP.

Functional Configuration

Instance Data:

Object	Description
• Enable	Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.
• Priority	The priority to be inserted as PCP bits in TAG (if any). In case of enabling Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.
• Frame rate	<p>Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has the following uses:</p> <ul style="list-style-type: none"> * The transmission rate of the CCM PDU. * Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'. * Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'. <p>Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enabling</p>

	Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.
--	--

APS Protocol:

Object	Description
• Enable	Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.
• Priority	The priority to be inserted as PCP bits in TAG (if any).
• Cast	Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.
• Type	R-APS: APS PDU is transmitted as R-APS - this is for ERPS. L-APS: APS PDU is transmitted as L-APS - this is for ELPS.
• Last Octet	This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

Buttons

Fault Management: Click to go to Fault Management page.

Performance Monitoring: Click to go to Performance Monitor page.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

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

4.19.3 Ethernet Ring Protocol Switch

The Ethernet Ring Protection Switch instances are configured here; screen in [Figure 4-19-3](#) appears.

Ethernet Ring Protection Switching

Note:

1. Please make sure the DHCP client function has been disabled.
2. Please be noticed that the ring port can not be applied to spanning tree function at the same time.

Refresh

Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type	Major Ring ID	Alarm
--------	---------	--------	--------	----------------	----------------	---------------	---------------	-----------	---------------	-------

Add New Protection Group

Save

Reset

Figure 4-19-3: Ethernet Ring Protocol Switch page screenshot

The page includes the following fields:


Object	Description
• Delete	This box is used to mark an ERPS for deletion in next Save operation.
• Port 0	This will create a Port 0 of the switch in the ring.
• Port 1	This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance
• Port 0 SF MEP	The Port 0 Signal Fail reporting MEP.
• Port 1 SF MEP	The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.
• Port 0 APS MEP	The Port 0 APS PDU handling MEP.
• Port 1 APS MEP	The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.
• Ring Type	Type of Protecting ring. It can be either major ring or sub-ring.
• Major Ring ID	Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.
• Alarm	There is an active alarm on the ERPS.

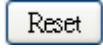
Buttons

Add New Protection Group

: Click to add a new Protection group entry.

: Click to refresh the page immediately.

: Click to save changes.

: Click to undo any changes made locally and revert to previously saved values.

4.19.4 Ethernet Ring Protocol Switch Configuration

This page allows the user to inspect and configure the current ERPS Instance; screen in [Figure 4-19-4](#) appears.

ERPS Configuration 1

Auto-refresh ☐ Refresh

Instance Data

ERPS ID	Port 0	Port 1	Port 0 SF MEP	Port 1 SF MEP	Port 0 APS MEP	Port 1 APS MEP	Ring Type
1	1	2	1	2	1	2	Major Ring

Instance Configuration

Configured	Guard Time	WTR Time	Hold Off Time	Version	Revertive	VLAN config
	500	1min	0	v2	<input checked="" type="checkbox"/>	VLAN Config

RPL Configuration

RPL Role	RPL Port	Clear
None	None	<input type="checkbox"/>

Instance Command

Command	Port
None	None

Instance State

Protection State	Port 0	Port 1	Transmit APS	Port 0 Receive APS	Port 1 Receive APS	WTR Remaining	RPL Un-blocked	No APS Received	Port 0 Block Status	Port 1 Block Status	FOP Alarm
Protected	SF	SF	SF DNF BPRO			0			Blocked	Blocked	

Save Reset

Figure 4-19-4: Ethernet Ring Protocol Switch Configuration page screenshot

The page includes the following fields:

Instant Data:

Object	Description
• ERPS ID	The ID of the Protection group.
• Port 0	See help on ERPS create WEB.
• Port 1	See help on ERPS create WEB.
• Port 0 SF MEP	See help on ERPS create WEB.
• Port 1 SF MEP	See help on ERPS create WEB.
• Port 0 APS MEP	See help on ERPS create WEB.
• Port 1 APS MEP	See help on ERPS create WEB.
• Ring Type	Type of Protected ring. It can be either major ring or sub-ring.

Instant Configuration:

Object	Description
• Configuration	Red: This ERPS is only created and has not yet been configured - is not active. Green: This ERPS is configured - is active.
• Guard Time	Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms
• WTR Time	The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes.
• Hold Off Time	The timing value to be used to make persistent check on Signal Fail before switching. The range of the hold off timer is 0 to 10 seconds in steps of 100 ms
• Version	ERPS Protocol Version - v1 or v2
• Revertive	In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL. In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.
• VLAN Config	VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group.

PRL Configuration:

Object	Description
• PRL Role	It can be either RPL owner or RPL Neighbour.
• PRL Port	This allows to select the east port or west port as the RPL block.
• Clear	If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.

Instant Command:

Object	Description
• Command	Administrative command. A port can be administratively configured to be in either manual switch or forced switch state.
• Port	Port selection - Port0 or Port1 of the protection Group on which the command is applied.

Instant State:

Object	Description
• Protection State	ERPS state according to State Transition Tables in G.8032.
• Port 0	OK: State of East port is ok SF: State of East port is Signal Fail
• Port 1	OK: State of West port is ok SF: State of West port is Signal Fail
• Transmit APS	The transmitted APS according to State Transition Tables in G.8032.
• Port 0 Receive APS	The received APS on Port 0 according to State Transition Tables in G.8032.
• Port 1 Receive APS	The received APS on Port 1 according to State Transition Tables in G.8032.
• WTR Remaining	Remaining WTR timeout in milliseconds.
• RPL Un-blocked	APS is received on the working flow.
• No APS Received	RAPS PDU is not received from the other end.
• Port 0 Block Status	Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
• Port 1 Block Status	Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
• FOP Alarm	Failure of Protocol Defect(FOP) status. If FOP is detected, red LED glows; else green LED glows.

Buttons

Save: Click to save changes.

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 6 seconds.

Refresh: Click to refresh the page immediately.

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

4.19.5 Ring Wizard

This page allows the user to configure the ERPS by wizard; screen in [Figure 4-19-4](#) appears.

Ring Wizard

Note:


1. Please make sure the DHCP client function has been disabled.
2. Please be noticed that the ring port can not be applied to spanning tree function at the same time.

ALL Switch Number (3 ~ 30):

Number ID:


Next

Configuration


Switch-3


Mep:6

Port
Mep:1

(Owner)
Switch-1

Vlan

Port
Mep:2

(Neighbour)
Switch-2


Mep:3

Set

Show Topology

Figure 4-19-5: Ring Wizard page screenshot

The page includes the following fields:

Object	Description
• All Switch Numbers	Set all the switch numbers for the ring group. The default number is 3 and maximum number is 30.
• Number ID	The switch where you are requesting ERPS.
• Port	Configures the port number for the MEP.
• VLAN	Set the ERPS VLAN.

Buttons

Next: Click to configure ERPS.

Set: Click to save changes.

Show Topology: Click to show the ring topology.

4.19.6 Ring Wizard Example:

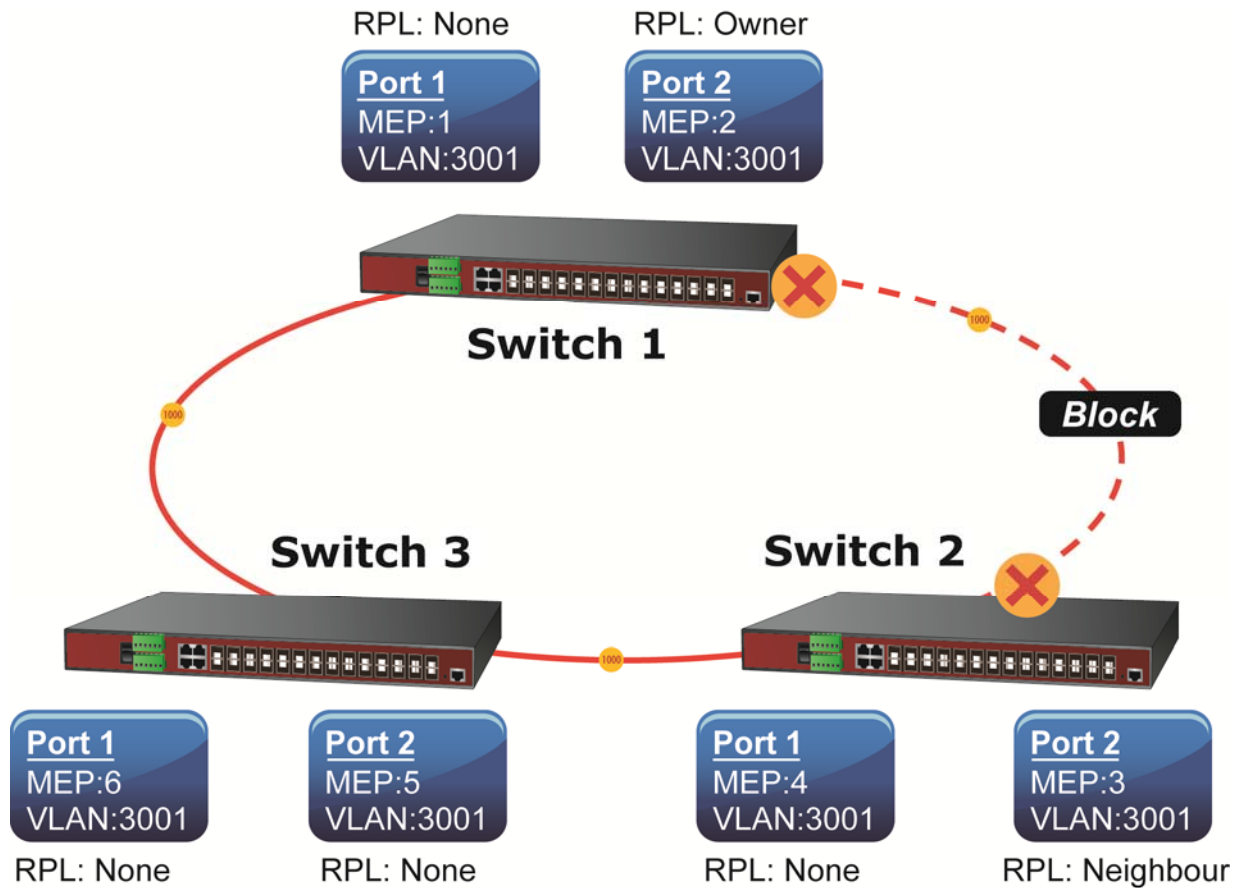


Figure 4-19-6: Ring Example Diagram

The above topology often occurs on using ERPS protocol. The multi switch constitutes a single ERPS ring; all of the switches only are configured as an ERPS in VLAN 3001, thereby constituting a single MRPP ring.

Switch ID	Port	MEP ID	RPL Type	VLAN Group
Switch 1	Port 1	1	None	3001
	Port 2	2	Owner	3001

Switch 2	Port 1	4	None	3001
	Port 2	3	Neighbour	3001
Switch 3	Port 1	6	None	3001
	Port 2	5	None	3001

Table 4-2: ERPS Configuration Table

The scenario is described as follows:

1. Disable DHCP client and set proper static IP for Switch 1, 2 & 3. In this example, switch 1 is 192.168.0.101; switch 2 is 192.168.0.102 and switch 3 is 192.168.0.103.
2. On switch 1, 2 & 3, disable spanning tree protocol to avoid confliction with ERPS.

Setup steps

Set ERPS Configuration on Switch 1

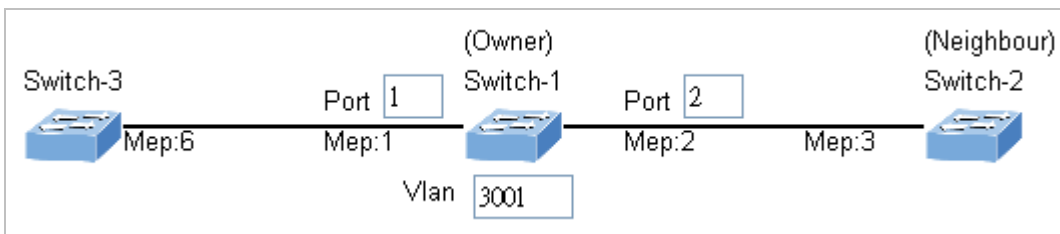
Connect PC to switch 1 directly; don't connect to port 1 & 2

Log-in on the Switch 1 and click "Ring > Ring Wizard"

Set "All Switch Number" = 3 and "Number ID" = 1; click "Next" button to set the ERPS configuration for Switch 1.

ALL Switch Number (3 ~ 30):
Number ID:

Set "MEP1" = Port1, "MEP2" = Port2 and VLAN ID = 3001; click "Set" button to save the ERPS configuration for Switch 1.



Set ERPS Configuration on Switch 2

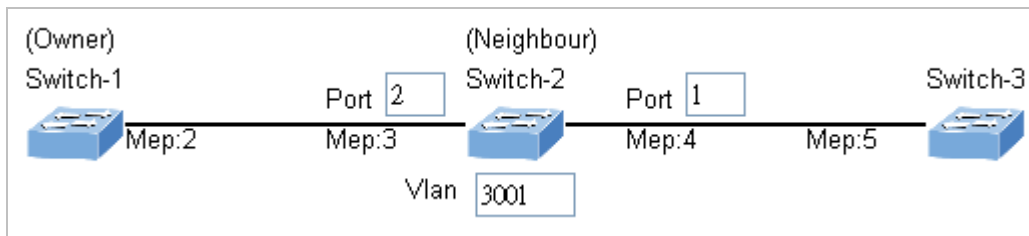
Connect PC to switch 2 directly; don't connect to port 1 & 2

Log-in on the Switch 2 and click "Ring > Ring Wizard"

Set "All Switch Number" = 3 and "Number ID" = 2; click "Next" button to set the ERPS configuration for Switch 2.

ALL Switch Number (3 ~ 30):
Number ID:

Set "MEP3" = Port2, "MEP4" = Port1 and VLAN ID = 3001; click "Set" button to save the ERPS configuration for Switch 2.



Set ERPS Configuration on Switch 3

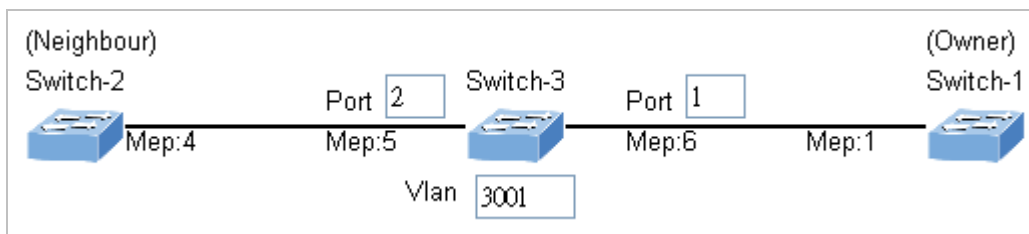
Connect PC to switch 3 directly; don't connect to port 1 & 2

Log-in on the Switch 3 and click "Ring > Ring Wizard"

Set "All Switch Number" = 3 and "Number ID" = 3; click "Next" button to set the ERPS configuration for Switch 3.

ALL Switch Number (3 ~ 30):	<input type="text" value="3"/>	Number ID:	<input type="text" value="3"/>	<input type="button" value="Next"/>
------------------------------	--------------------------------	------------	--------------------------------	-------------------------------------

Set "MEP5" = Port2, "MEP6" = Port1 and VLAN ID = 3001; click "Set" button to save the ERPS configuration for Switch 3.



To avoid loop, please don't connect switch 1, 2 & 3 together in the ring topology before configuring the end of ERPS .

Follow the configuration or ERPS wizard to connect the Switch 1, 2 & 3 together to establish ERPS application:

MEP2 ↔ MEP3 = Switch1 / Port2 ↔ Switch2 / Port2

MEP4 ↔ MEP5 = Switch2 / Port1 ↔ Switch3 / Port2

MEP1 ↔ MEP6 = Switch1 / Port1 ↔ Switch3 / Port1

5. SWITCH OPERATION

5.1 Address Table

The **Managed Switch** is implemented with an address table. This address table composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port no, etc. This in-formation comes from the learning process of **Managed Switch**.

5.2 Learning

When one packet comes in from any port, the **Managed Switch** will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

5.3 Forwarding & Filtering

When one packet comes from some port of the **Managed Switch**, it will also check the destination address besides the source address learning. The **Managed Switch** will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, 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 with this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability

5.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward **Managed Switch** stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets occurrence, it is the best choice when a network needs efficiency and stability.

The **Managed Switch** scans the destination address from the packet-header, searches the routing table pro-vided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. How-ever, the switch is most commonly used to segment existence hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to signifi-cantly boost bandwidth using conventional cabling and adapters.

Due 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 reduce the overall load on the network.

The **Managed Switch** performs "**Store and Forward**" therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

5.5 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 at which both devices are connected and capable of, both 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.

6. TROUBLESHOOTING

This chapter contains information to help you solve problems. If the **Managed Switch** is not functioning properly, make sure the Ethernet Switch was set up according to instructions in this manual.

The per port LED is not lit

Solution:

Check the cable connection of the **Managed Switch**.

Performance is bad

Solution:

Check the speed duplex mode of the partner device. The **Managed Switch** is run at Auto-negotiation mode and if the partner is set to half duplex, then the performance will be poor.

Per port LED is lit, but the traffic is irregular

Solution:

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.

Why the Managed Switch doesn't connect to the network

Solution:

Check per port LED on the **Managed Switch**. Try another port on the **Managed Switch** Make sure the cable is installed properly Make sure the cable is the right type Turn off the power. After a while, turn on power again.

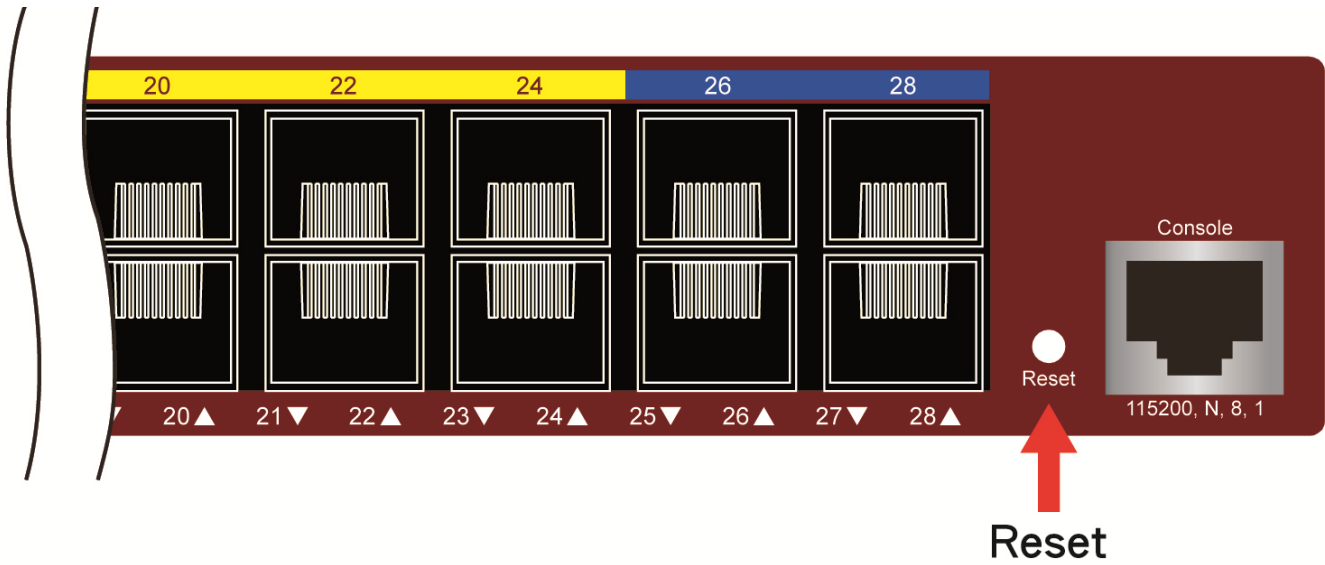
Can I install MGB-SX or other non wide temperature SFP module into SFP slot of Managed Switch?

Solution:

Yes, it does. However, since the MGB-SX and other non wide temperature SFP module cannot operate under -40 to 75 Degree C. Please pay attention to this point and consider use INTERLOGIX wide temperature SFP module for **Managed Switch**.

■ **Changed IP address or forgotten admin password –**

To reset the IP address to the default IP Address “**192.168.0.100**” or reset the password to default value. Press the hardware **reset button** at the front panel about **5 seconds**. After the device is rebooted, you can login the management WEB interface within the same subnet of 192.168.0.xx.



APPENDIX A

A.1 Switch's Data RJ-45 Pin Assignments - 1000Mbps, 1000Base-T

PIN NO	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-

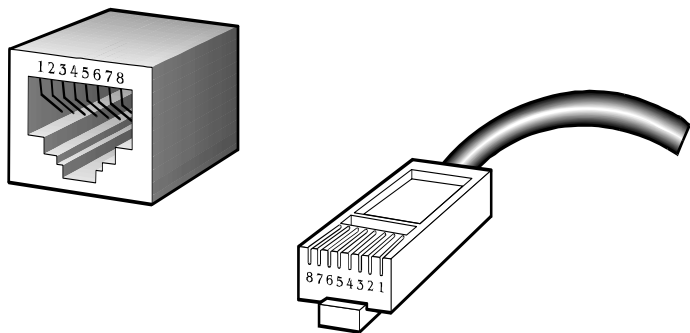
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100Base-TX

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/connector and their pin assignments:

RJ-45 Connector pin assignment		
Contact	MDI Media Dependent Interface	MDI-X Media Dependent Interface-Cross
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 cable, RJ-45 pin assignment



The standard RJ-45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

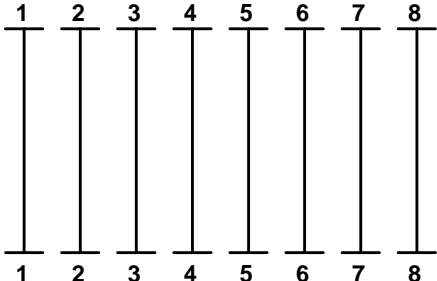
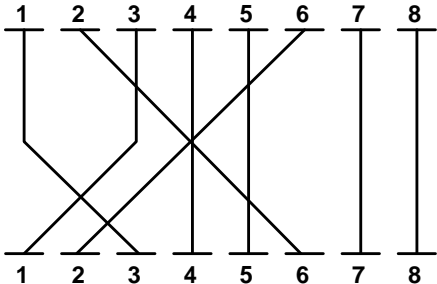
Straight Cable		SIDE 1	SIDE2
	SIDE 1	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown
	SIDE 2		
Crossover Cable		SIDE 1	SIDE2
	SIDE 1	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
	SIDE 2		

Figure A-1: Straight-through and Crossover Cable

Please make sure your connected cables are with same pin assignment and color as the above picture before deploying the cables into your network.

APPENDIX B: GLOSSARY

A

ACE

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

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

ACL

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

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

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

There are 3 web-pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is

incremented. See the Web page help text for each specific port property.

ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for **A**dvanced **E**ncryption **S**tandard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS

AMS is an acronym for **A**uto **M**edia **S**elect. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and cu cables are inserted, the port will select the preferred media.

APS

APS is an acronym for **A**utomatic **P**rotection **S**witching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation

Using multiple ports in parallel is to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(Also *Port Aggregation*, *Link Aggregation*).

ARP

ARP is an acronym for **A**ddress **R**esolution **P**rotocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for Cisco Discovery Protocol.

D

DEI

DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

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

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for **D**omain **N**ame **S**ystem. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for **D**enial of **S**ervice. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.

An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

Drop Precedence Level

Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 corresponds to 'Discard Eligible' (Yellow) frames.

DSCP

DSCP is an acronym for **D**ifferentiated **S**ervices **C**ode **P**oint. It is a field in the header of IP packets for packet classification purposes.

E

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

ERPS

Ethernet Ring Protection Switching, or **ERPS**, is an effort at [ITU-T](#) under G.8032 Recommendation to provide sub-50ms protection and recovery switching for [Ethernet](#) traffic in a [ring topology](#) and at the same time ensuring that there are no loops formed at the Ethernet layer.

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

FTP is an acronym for **F**ile **T**ransfer **P**rotocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

H

HTTP

HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use

the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for **IP Multicast**.

IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

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.

LLC

The IEEE 802.2 **Logical Link Control** (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The **Link Layer Discovery Protocol** (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LLQI

LLQI (Last Listener Query Interval) is the maximum response time used to calculate the Maximum Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC

LOC is an acronym for Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if there's no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MSTP

In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by

IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them(Wikipedia).

N

NAS

NAS is an acronym for **N**etwork **A**ccess **S**erver. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for **N**etwork **B**asic **I**nput/**O**utput **S**ystem. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for **N**etwork **F**ile **S**ystem. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

Optional TLVs.

A LLDP frame contains multiple TLVs

For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for Powered Device. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implements the Ethernet physical layer (IEEE-802.3).

PING

ping 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 e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for Point-to-Point Protocol over Ethernet.

It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a private VLAN, PVLANS provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

Q

QCE

QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

R

RARP

RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

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, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

SHA

SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack Protocol using Routing Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for Secure Shell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for **T**ransmission **C**ontrol **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for **TEL**etype **NET**work. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for **T**rivial **F**ile **T**ransfer **P**rotocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS

ToS is an acronym for **T**ype **o**f **S**ervice. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for **T**ype **L**ength **V**alue. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

TKIP is an acronym for **T**emporal **K**ey **I**ntegrity **P**rotocol. 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

UDP is an acronym for **U**ser **D**atagram **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for **U**niversal **P**lug and **P**lay. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN

It is Virtual LAN. It is a method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

W

WEP

WEP is an acronym for Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

WiFi

WiFi is an acronym for Wireless Fidelity. It is meant to be used generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

WPA-PSK is an acronym for Wi-Fi Protected Access - Pre Shared Key. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

WPA-Radius is an acronym for Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPS

WPS is an acronym for Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WRED

WRED is an acronym for Weighted Random Early Detection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR

WTR is an acronym for Wait To Restore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is