

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

Copyright © **Error! Unknown document property name.** United Technologies Corporation,
Interlogix is part of UTC Climate, Controls & Security, a unit of United Technologies Corporation.
All rights reserved.

Trademarks and patents Trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer Interlogix
2955 Red Hill Avenue, Costa Mesa, CA 92626-5923, USA

Authorized EU manufacturing representative:
UTC Fire & Security B.V.
Kelvinstraat 7, 6003 DH Weert, The Netherlands

Certification



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

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

- (1) This device may not cause harmful interference.
- (2) This Device must accept any interference received, including interference that may cause undesired operation.

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

European Union directives Therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU.



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



2013/56/EU (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

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 Description	11
1.3 How to Use This Manual	13
1.4 Product Features	14
1.5 Product Specifications	17
2. INSTALLATION	20
2.1 Hardware Description	20
2.1.1 Switch Front Panel	20
2.1.2 LED Indications	21
2.1.3 Switch Rear Panel	22
2.2 Installing the Switch.....	24
2.2.1 Desktop Installation	24
2.2.2 Rack Mounting	25
2.2.3 Installing the SFP/SFP+ Transceiver	26
3. SWITCH MANAGEMENT	30
3.1 Requirements	30
3.2 Management Access Overview.....	31
3.3 Administration Console	32
3.4 Web Management.....	33
3.5 SNMP-based Network Management	34
3.6 IFS Smart Discovery Utility	35
4. WEB CONFIGURATION.....	37
4.1 Main Web Page	40
4.2 System.....	42
4.2.1 System Information.....	43
4.2.2 IP Configuration	44
4.2.3 IP Status	46

4.2.4 Users Configuration	46
4.2.5 Privilege Levels	50
4.2.6 NTP Configuration	51
4.2.7 Time Configuration	52
4.2.8 UPnP	54
4.2.9 DHCP Relay	56
4.2.10 DHCP Relay Statistics	57
4.2.11 CPU Load	59
4.2.12 System Log	60
4.2.13 Detailed Log	61
4.2.14 Remote Syslog	62
4.2.15 SMTP Configuration	63
4.2.16 Web Firmware Upgrade	64
4.2.17 TFTP Firmware Upgrade	65
4.2.18 Save Startup Config.....	66
4.2.19 Configuration Download	66
4.2.20 Configuration Upload.....	67
4.2.21 Configuration Activate.....	67
4.2.22 Configuration Delete.....	68
4.2.23 Image Select	68
4.2.24 Factory Default	69
4.2.25 System Reboot.....	70
4.3 Simple Network Management Protocol	71
4.3.1 SNMP Overview	71
4.3.2 SNMP System Configuration	72
4.3.3 SNMP Trap Configuration.....	74
4.3.4 SNMP System Information	76
4.3.5 SNMPv3 Configuration	77
4.3.5.1 SNMPv3 Communities	77
4.3.5.2 SNMPv3 Users.....	78
4.3.5.3 SNMPv3 Groups	79
4.3.5.4 SNMPv3 Views.....	80
4.3.5.5 SNMPv3 Access.....	81
4.4 Port Management	83
4.4.1 Port Configuration.....	83
4.4.2 Port Statistics Overview	85
4.4.3 Port Statistics Detail.....	86
4.4.4 SFP Module Information.....	88
4.4.5 Port Mirror	89
4.5 Link Aggregation	92

4.5.1 Static Aggregation.....	94
4.5.2 LACP Configuration.....	95
4.5.3 LACP System Status	97
4.5.4 LACP Port Status.....	98
4.5.5 LACP Port Statistics	99
4.6 VLAN.....	100
4.6.1 VLAN Overview	100
4.6.2 IEEE 802.1Q VLAN	101
4.6.3 VLAN Port Configuration	104
4.6.4 VLAN Membership Status	110
4.6.5 VLAN Port Status.....	111
4.6.6 Port Isolation	113
4.6.7 VLAN setting example:.....	115
4.6.7.1 Two Separate 802.1Q VLANs	115
4.6.7.2 VLAN Trunking between two 802.1Q aware switches	117
4.6.7.3 Port Isolate	120
4.6.8 MAC-based VLAN.....	121
4.6.9 MAC-based VLAN Status	122
4.6.10 Protocol-based VLAN.....	122
4.6.11 Protocol-based VLAN Membership.....	124
4.7 Spanning Tree Protocol	126
4.7.1 Theory	126
4.7.2 STP System Configuration	132
4.7.3 Bridge Status	134
4.7.4 CIST Port Configuration	135
4.7.5 MSTI Priorities.....	138
4.7.6 MSTI Configuration.....	139
4.7.7 MSTI Ports Configuration	140
4.7.8 Port Status.....	142
4.7.9 Port Statistics.....	143
4.8 Multicast.....	144
4.8.1 IGMP Snooping	144
4.8.2 Profile Table.....	148
4.8.3 Address Entry	149
4.8.4 IGMP Snooping Configuration.....	150
4.8.5 IGMP Snooping VLAN Configuration.....	152
4.8.6 IGMP Snooping Port Group Filtering	154
4.8.7 IGMP Snooping Status	155
4.8.8 IGMP Group Information	156
4.8.9 IGMPv3 Information.....	157

4.8.10 MLD Snooping Configuration	158
4.8.11 MLD Snooping VLAN Configuration	159
4.8.12 MLD Snooping Port Group Filtering.....	161
4.8.13 MLD Snooping Status.....	162
4.8.14 MLD Group Information	163
4.8.15 MLDv2 Information	164
4.8.16 MVR (Multicast VLAN Registration).....	165
4.8.17 MVR Status	168
4.8.18 MVR Groups Information.....	169
4.8.19 MVR SFM Information	169
4.9 Quality of Service	171
4.9.1 Understanding QoS	171
4.9.2 Port Policing	172
4.9.3 Port Classification.....	172
4.9.4 Port Scheduler.....	174
4.9.5 Port Shaping.....	175
4.9.5.1 QoS Egress Port Schedule and Shapers	176
4.9.6 Port Tag Remarking.....	177
4.9.6.1 QoS Egress Port Tag Remarking	178
4.9.7 Port DSCP.....	179
4.9.8 DSCP-based QoS	180
4.9.9 DSCP Translation	181
4.9.10 DSCP Classification	182
4.9.11 QoS Control List	183
4.9.11.1 QoS Control Entry Configuration	185
4.9.12 QCL Status	187
4.9.13 Storm Control Configuration	188
4.9.14 WRED	189
4.9.15 QoS Statistics	192
4.9.16 Voice VLAN Configuration	192
4.9.17 Voice VLAN OUI Table	195
4.10 Access Control Lists.....	196
4.10.1 Access Control List Status	196
4.10.2 Access Control List Configuration.....	198
4.10.3 ACE Configuration	200
4.10.4 ACL Ports Configuration	210
4.10.5 ACL Rate Limiter Configuration	212
4.11 Authentication	213
4.11.1 Understanding IEEE 802.1X Port-Based Authentication.....	214
4.11.2 Authentication Configuration	217

4.11.3 Network Access Server Configuration	218
4.11.4 Network Access Overview	229
4.11.5 Network Access Statistics	230
4.11.6 RADIUS	237
4.11.7 TACACS+	239
4.11.8 RADIUS Overview	240
4.11.9 RADIUS Details	242
4.11.10 Windows Platform RADIUS Server Configuration.....	248
4.11.11 802.1X Client Configuration	253
4.12 Security	256
4.12.1 Port Limit Control.....	256
4.12.2 Access Management	260
4.12.3 Access Management Statistics	261
4.12.4 HTTPs	262
4.12.5 SSH.....	263
4.12.6 Port Security Status.....	263
4.12.7 Port Security Detail.....	266
4.12.8 DHCP Snooping	267
4.12.9 Snooping Table.....	268
4.12.10 IP Source Guard Configuration.....	269
4.12.11 IP Source Guard Static Table.....	270
4.12.12 ARP Inspection.....	271
4.12.13 ARP Inspection Static Table.....	272
4.12.14 Dynamic ARP Inspection Table.....	273
4.13 Address Table	275
4.13.1 MAC Table Configuration.....	275
4.13.2 MAC Address Table Status	277
4.14 LLDP	279
4.14.1 Link Layer Discovery Protocol	279
4.14.2 LLDP Configuration	279
4.14.3 LLDP MED Configuration	282
4.14.4 LLDP-MED Neighbor.....	288
4.14.5 Neighbor.....	292
4.14.6 Port Statistics.....	293
4.15 Network Diagnostics.....	295
4.15.1 Ping	296
4.15.2 IPv6 Ping.....	297
4.15.3 Remote IP Ping Test.....	298
4.15.4 Cable Diagnostics.....	299

4.16 Power over Ethernet (NS3502-8P-2T-2S only)	301
4.16.1 Power over Ethernet Powered Device.....	301
4.16.2 System Configuration	303
4.16.3 Power Over Ethernet Configuration.....	304
4.16.4 Port Sequential.....	306
4.16.5 Port Configuration.....	307
4.16.6 PoE Status.....	309
4.16.7 PoE Schedule.....	310
4.16.8 LLDP PoE Neighbours	314
4.17 Loop Protection	315
4.17.1 Configuration	315
4.17.2 Loop Protection Status	316
4.18 RMON	318
4.18.1 RMON Alarm Configuration	318
4.18.2 RMON Alarm Status	320
4.18.3 RMON Event Configuration	321
4.18.4 RMON Event Status	322
4.18.5 RMON History Configuration	323
4.18.6 RMON History Status	324
4.18.7 RMON Statistics Configuration	325
4.18.8 RMON Statistics Status	326
5. SWITCH OPERATION	328
5.1 Address Table	328
5.2 Learning	328
5.3 Forwarding & Filtering	328
5.4 Store-and-Forward	328
5.5 Auto-Negotiation	329
6. TROUBLESHOOTING	330
APPENDIX A: Networking Connection	331
A.1 Switch's Data RJ45 Pin Assignments - 1000Mbps, 1000BASE-T	331
A.2 10/100Mbps, 10/100BASE-TX	331
APPENDIX B : GLOSSARY	333

1. INTRODUCTION

Thanks you for purchasing IFS NS3502-8P-2T-2S Managed Switch, which comes with multiple Gigabit Ethernet copper and SFP/SFP+ fiber optic connectivity and robust layer 2 and layer 3 features. The description of this model is shown below:

Model Name	Gigabit RJ45 Ports	Gigabit SFP Slots	PoE Ports	10G SFP+ Slots
NS3502-8P-2T-2S	2	2	8	-

“**Managed Switch**” is used as an alternative name in this user’s manual.

1.1 Packet Contents

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

- ◆ **The Managed Switch**
- ◆ **Quick Installation Guide**
- ◆ **RJ45 to RS232 Cable**
- ◆ **Rubber Feet**
- ◆ **Two Rack-mounting Brackets with Attachment Screws**
- ◆ **Power Cord**
- ◆ **SFP Dust-proof Caps**

Model Name	SFP Dust-proof Caps
NS3502-8P-2T-2S	2

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 Description

Ideal Combination of 1G Uplink, high-density, Gigabit and Layer 2 Static Routing

IFS NS3502-8P-2T-2S is a Layer 2+ managed Gigabit/10 Gigabit Ethernet switch and supports **static Layer 3 routing** in a 1U case. The NS3502-8P-2T-2S can handle extremely large amounts of data in a secure topology linking to an enterprise backbone or high capacity servers.

Layer 3 IPv4 and IPv6 VLAN Routing for Secure and Flexible Management

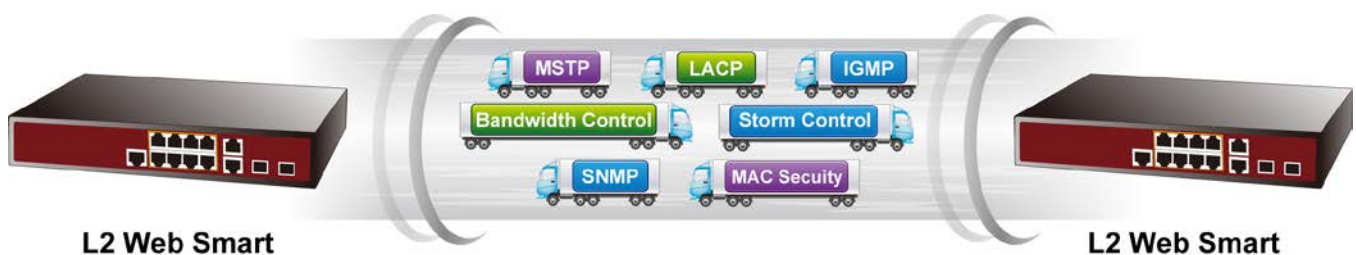
The NS3502-8P-2T-2S switch not only provides ultra high transmission performance, and excellent layer 2 and layer 4 technologies, but also layer 3 IPv4/IPv6 VLAN routing feature which allows to cross over different VLANs and different IP addresses for the purpose of having a highly-secured, flexible management and simpler networking application.

IPv6/IPv4 Dual Stack

Supporting both IPv6 and IPv4 protocols, the NS3502-8P-2T-2S helps the SMBs to step in the IPv6 era with the lowest investment as its network facilities need not to be replaced or overhauled if the IPv6 FTTx edge network is set up.

Robust Layer 2 Features

The NS3502-8P-2T-2S can be programmed for advanced switch management functions such as dynamic port link aggregation, **Q-in-Q VLAN**, private VLAN, **Multiple Spanning Tree protocol (MSTP)**, Layer 2 to Layer 3 QoS, bandwidth control and **IGMP/MLD Snooping**. Via the link aggregation of supporting ports, the NS3502-8P-2T-2S allows the operation of a high-speed trunk to combine with multiple fiber ports and supports fail-over as well.



Powerful Security

The NS3502-8P-2T-2S offers a comprehensive **layer 2 to layer 3 Access Control List (ACL)** for enforcing security to the edge. It can be used to restrict network access by denying packets based on source and destination IP address, TCP/UDP ports or defined typical network applications. Its protection mechanism also comprises **802.1X Port-based** and **MAC-based** user and device authentication. With the **private VLAN** function, communication between edge ports can be prevented to ensure user privacy. The NS3502-8P-2T-2S also provides **DHCP Snooping**, **IP Source Guard** and **Dynamic ARP Inspection** functions to prevent IP snooping from attack and discard ARP packets with invalid MAC address. The network administrators can now construct highly secured corporate networks with considerably less time and effort than before.

Excellent Traffic Control

The NS3502-8P-2T-2S is loaded with powerful traffic management and QoS features to enhance connection services by SMBs. The QoS features include wire-speed Layer 3 traffic classifiers and bandwidth limit that are particular useful for multi-tenant unit,

multi business unit, Telco, or Network Service Provider's applications. It also empowers the enterprises to take full advantages of the limited network resources and guarantees the best performance in VoIP and video conferencing transmission.

Efficient and Secure Management

The NS3502-8P-2T-2S Managed Switch is equipped with console, Web and SNMP management interfaces. With the built-in Web-based management interface, the NS3502-8P-2T-2S offers an easy-to-use, platform-independent management and configuration facility. The NS3502-8P-2T-2S supports standard Simple Network Management Protocol (SNMP) and can be managed via any management software based on standard of SNMP protocol. For reducing product learning time, the NS3502-8P-2T-2S offers Cisco-like command via Telnet or console port and customer doesn't need to learn new command from these switches. Moreover, the NS3502-8P-2T-2S offers secure remote management by supporting **SSH**, **SSL** and **SNMPv3** connection which encrypt the packet content at each session.

Flexibility and Extension Solution

The multi-mini-GBIC slots built in the NS3502-8P-2T-2S support dual speed as it features 100BASE-FX and 1000BASE-SX/LX SFP (Small Form-factor Pluggable) fiber-optic modules. Now the administrator can flexibly choose the suitable SFP transceiver according to not only the transmission distance, but also the transmission speed required. The distance can be extended from 550 meters to 2km (multi-mode fiber) up to above 10/20/30/40/50/70 kilometers (single-mode fiber or WDM fiber). They are well suited for applications within the enterprise data centers and distributions.

Intelligent SFP Diagnosis Mechanism

The NS3502-8P-2T-2S supports SFP-DDM (**Digital Diagnostic Monitor**) function that greatly helps network administrator to easily monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.

1.3 How to Use This Manual

This User's 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, SWITCH OPERATION

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

Section 6, POWER over ETHERNET OVERVIEW

The chapter introduces the IEEE 802.3af / 802.3at PoE standard and PoE provision of the Managed Switch.

Section 7, TROUBLESHOOTING

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

Appendix A

The section contains cable information of the Managed Switch.

1.4 Product Features

➤ **Physical Port**

- **10/100/1000BASE-T** Gigabit RJ45 copper
- **100/1000BASE-X** mini-GBIC/SFP slots
- RJ45 console interface for switch basic management and setup

➤ **Power over Ethernet**

- Complies with IEEE 802.3at High Power over Ethernet end-span PSE
- Complies with IEEE 802.3af Power over Ethernet end-span PSE
- Up to 8 ports of IEEE 802.3af/802.3at devices powered
- Supports PoE Power up to 30.8 watts for each PoE port
- Auto detects powered device (PD)
- Circuit protection prevents power interference between ports
- Remote power feeding up to 100 meters
- PoE Management
 - Total PoE power budget control
 - Per port PoE function enable/disable
 - PoE Port Power feeding priority
 - Per PoE port power limitation
 - PD classification detection
 - PD alive check
 - PoE schedule
 - PD power recycling schedule

➤ **Layer 2 Features**

- Prevents packet loss with back pressure (half-duplex) and IEEE 802.3x pause frame flow control (full-duplex)
- High performance of Store-and-Forward architecture, and runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
- Storm Control support
 - Broadcast/Unicast/Unknown-unicast
- Supports **VLAN**
 - IEEE 802.1Q tagged VLAN
 - Up to 255 VLANs groups, out of 4094 VLAN IDs
 - Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
 - Private VLAN Edge (PVE)
 - Protocol-based VLAN
 - MAC-based VLAN
 - IP Subnet-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)
- Up to 8 ports per trunk group
- Up to 16Gbps bandwidth (full duplex mode)

- Provides port mirror (many-to-1)

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

- Loop protection to avoid broadcast loops

- **Layer 3 IP Routing Features**

- Supports maximum 32 static routes and route summarization

- **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
 - TOS/DSCP/IP Precedence of IPv4/IPv6 packets
 - IP TCP/UDP port number
 - Typical network application
- Strict priority and Weighted Round Robin (WRR) CoS policies
- 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**

- Authentication
 - IEEE 802.1x Port-based/MAC-based network access authentication
 - IEEE 802.1x Authentication with Guest VLAN
 - Built-in RADIUS client to cooperate with the RADIUS servers
 - RADIUS/TACACS+ users access authentication

- Access Control List
 - IP-based Access Control List (ACL)
 - MAC-based Access Control List (ACL)
- Source MAC/IP address binding
- **DHCP Snooping** to filter distrusted 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**

- IPv4 and IPv6 dual stack management
- Switch Management Interfaces
 - Console/Telnet Command Line Interface
 - Web switch management
 - SNMP v1, v2c, and v3 switch management
 - SSH/SSL secure access
- **IPv6** Address/NTP management
- Built-in Trivial File Transfer Protocol (TFTP) client
- BOOTP and DHCP for IP address assignment
- System Maintenance
 - Firmware upload/download via HTTP/TFTP
 - Reset button for system reboot or reset to factory default
 - Dual Images
- DHCP Relay and Option 82
- User Privilege levels control
- NTP (Network Time Protocol)
- Link Layer Discovery Protocol (LLDP) and LLDP-MED
- Network Diagnostic
 - SFP-DDM (Digital Diagnostic Monitor)
 - Cable Diagnostic technology provides the mechanism to detect and report potential cabling issues
 - ICMPv6/ICMPv4 Remote Ping
- SMTP/Syslog remote alarm
- Four RMON groups (history, statistics, alarms and events)
- SNMP trap for interface Link Up and Link Down notification
- System Log
- IFS Smart Discovery Utility for deploy management

1.5 Product Specifications

NS3502-8P-2T-2S

Product	NS3502-8P-2T-2S
Hardware Specifications	
Copper Ports	10 10/100/1000BASE-T RJ45 Auto-MDI/MDI-X ports
SFP/mini-GBIC Slots	2 x 100/1000BASE-X SFP interfaces with Port-11 to Port-12 Supports 100/1000Mbps dual mode and DDM
PoE Injector Port	8 ports with 802.3at/af PoE injector function with Port-1 to Port-8
Console	1 x RJ45 serial port (115200, 8, N, 1)
Switch Architecture	Store-and-Forward
Switch Fabric	24Gbps/non-blocking
Throughput	17.76Mpps@64 bytes
Address Table	8K entries, automatic source address learning and aging
Shared Data Buffer	1392KB
Flow Control	IEEE 802.3x pause frame for full-duplex Back pressure for half-duplex
Jumbo Frame	9KB
Reset Button	< 5 sec: System reboot > 5 sec: Factory default
LED	System: Fan Alert (Green), SYS (Green), PWR (Green) 10/100/1000T RJ45 Interfaces (Port 1 to Port 8): 10/100/1000Mbps LNK/ACT (Green) PoE-in-Use (Orange) 10/100/1000T RJ45 Interfaces (Port 9 to Port 10): LNK/ACT (Green) 1000Mbps (Orange) 100/1000Mbps SFP Combo Interfaces (Port 11 to Port 12): LNK/ACT (Green) 1000Mbps (Orange)
Power Requirements	100~240V AC, 50/60Hz
Power Consumption (Full Loading)	320 watts/1091.9 BTU (max.)
ESD Protection	6KV DC
Dimensions (W x D x H)	330 x 200 x 43.5 mm, 1U height
Weight	2kg
Power over Ethernet	
PoE Standard	IEEE 802.3af/802.3at PoE/PSE
PoE Power Supply Type	End-span
PoE Power Output	Per port 54V DC, max. 30.8 watts
Power Pin Assignment	1/2(+), 3/6(-)

PoE Power Budget		260 watts (max.) @ 50 degrees C														
PoE Ability	PD @ 7 watts	8 units														
	PD @ 15.4 watts	8 units														
	PD @ 30.8 watts	8 units														
Layer2 Management Functions																
Basic Management Interfaces		Console, Telnet, Web browser, SNMP v1, v2c														
Secure Management Interfaces		SSH, SSL, SNMP v3														
Port Configuration		Port disable/enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Flow Control disable/enable														
Port Status		Display each port's speed duplex mode, link status, flow control status, auto negotiation status, trunk status														
Port Mirroring		TX/RX/Both Many-to-1 monitor														
VLAN		802.1Q tagged based VLAN, up to 255 VLAN groups Q-in-Q tunneling Private VLAN Edge (PVE) MAC-based VLAN Protocol-based VLAN Voice VLAN MVR (Multicast VLAN Registration) Up to 255 VLAN groups, out of 4094 VLAN IDs														
Link Aggregation		IEEE 802.3ad LACP/Static Trunk Supports 6 trunk groups with 8 ports per trunk														
QoS		Traffic classification based, strict priority and WRR 8-level priority for switching - Port number - 802.1p priority - 802.1Q VLAN tag - DSCP/TOS field in IP packet														
IGMP Snooping		IGMP (v1/v2/v3) Snooping, up to 255 multicast groups IGMP Querier mode support														
MLD Snooping		MLD (v1/v2) Snooping, up to 255 multicast groups MLD Querier mode support														
Access Control List		IP-based ACL/MAC-based ACL Up to 256 entries														
Bandwidth Control		Per port bandwidth control Ingress: 100Kbps~1000Mbps Egress: 100Kbps~1000Mbps														
SNMP MIBs		<table border="0"> <tr> <td>RFC 1213 MIB-II</td> <td>RFC 2819 RMON MIB (Groups 1, 2, 3 and 9)</td> </tr> <tr> <td>RFC 2863 IF-MIB</td> <td>RFC 2618 RADIUS Client MIB</td> </tr> <tr> <td>RFC 1493 Bridge MIB</td> <td>RFC 3411 SNMP-Frameworks-MIB</td> </tr> <tr> <td>RFC 1643 Ethernet MIB</td> <td>IEEE 802.1X PAE</td> </tr> <tr> <td>RFC 2863 Interface MIB</td> <td>LLDP</td> </tr> <tr> <td>RFC 2665 Ether-Like MIB</td> <td>MAU-MIB</td> </tr> <tr> <td>RFC 2737 Entity MIB</td> <td>Power over Ethernet MIB</td> </tr> </table>	RFC 1213 MIB-II	RFC 2819 RMON MIB (Groups 1, 2, 3 and 9)	RFC 2863 IF-MIB	RFC 2618 RADIUS Client MIB	RFC 1493 Bridge MIB	RFC 3411 SNMP-Frameworks-MIB	RFC 1643 Ethernet MIB	IEEE 802.1X PAE	RFC 2863 Interface MIB	LLDP	RFC 2665 Ether-Like MIB	MAU-MIB	RFC 2737 Entity MIB	Power over Ethernet MIB
RFC 1213 MIB-II	RFC 2819 RMON MIB (Groups 1, 2, 3 and 9)															
RFC 2863 IF-MIB	RFC 2618 RADIUS Client MIB															
RFC 1493 Bridge MIB	RFC 3411 SNMP-Frameworks-MIB															
RFC 1643 Ethernet MIB	IEEE 802.1X PAE															
RFC 2863 Interface MIB	LLDP															
RFC 2665 Ether-Like MIB	MAU-MIB															
RFC 2737 Entity MIB	Power over Ethernet MIB															
Layer 3 Functions																

IP Interfaces	Max. 8 VLAN interfaces	
Routing Table	Max. 32 routing entries	
Routing Protocols	IPv4 software static routing IPv6 software static routing	
Standards Conformance		
Regulatory Compliance	FCC Part 15 Class A, CE	
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/100BASE-FX IEEE 802.3z 1000BASE-SX/LX IEEE 802.3ab 1000BASE-T IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of Service	IEEE 802.1Q VLAN tagging IEEE 802.1x Port Authentication Network Control IEEE 802.1ab LLDP IEEE 802.3af Power over Ethernet IEEE 802.3at Power over Ethernet Plus RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP v1 RFC 2236 IGMP v2 RFC 3376 IGMP v3 RFC 2710 MLD v1 RFC 3810 MLD v2
Environments		
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	
Storage	Temperature: -10 ~ 70 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	

2. INSTALLATION

This section describes the hardware features and installation of the Managed Switch on the desktop or rack mount. 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, please read this chapter completely.

2.1 Hardware Description

2.1.1 Switch Front Panel

The front panel provides a simple interface monitoring the Managed Switch. [Figures 2-1-1](#) show the front panel of the Managed Switch.

NS3502-8P-2T-2S Front Panel

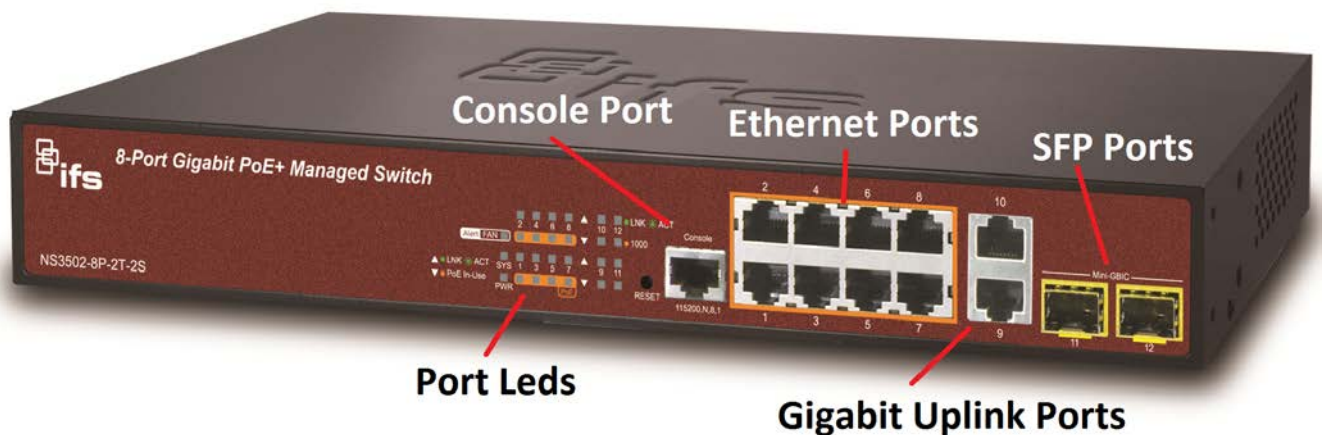


Figure 2-1-1: Front Panel of NS3502-8P-2T-2S

■ Gigabit TP interface

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

■ SFP slot

100/1000BASE-X mini-GBIC slot, SFP (Small Factor Pluggable) transceiver module: From 550 meters to 2km (multi-mode fiber), up to above 10/20/30/40/50/70 kilometers (single-mode fiber).

■ 1 Gigabit SFP+ slot

1GBASE-SR/LR mini-GBIC slot, SFP+ (Small Factor Pluggable Plus) Transceiver module supports from 300 meters (multi-mode fiber) up to 10 kilometers (single mode fiber)

■ Console port

The console port is a RJ45 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 RJ45 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

The front panel of the NS3502-8P-2T-2S comes with a reset button 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 Pressed and Released	Function
< 5 sec: System Reboot	Reboot the Managed Switch.
> 5 sec: Factory Default	Reset the Managed Switch to Factory Default configuration. The Managed Switch will then reboot and load the default settings as shown below: <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

The reset button of NS3502-8P-2T-2S-48T4X is located at the side of the switch.

2.1.2 LED Indications

The front panel LEDs indicate instant status of power and system status, fan status, port links / PoE-in-use and data activity; they help monitor and troubleshoot when needed. [Figures 2-1-2](#) show the LED indications of the Managed Switch.

NS3502-8P-2T-2S LED Indication



Figure 2-1-2: NS3502-8P-2T-2S LED on Front Panel

■ System

LED	Color	Function
-----	-------	----------

Fan Alert	Green	Lights to indicate that the fan is not working.
SYS	Green	Lights to indicate the system is working. Off to indicate the system is booting.
PWR	Green	Lights to indicate the Switch has power.

■ **Per 10/100/1000BASE-T PoE+ Port**

LED	Color	Function
LNK/ACT	Green	Lights To indicate the link through that port is successfully established. Blinks To indicate that the switch is actively sending or receiving data over that port.
PoE-in-Use	Orange	Lights to indicate the port is providing 54VDC in-line power. Off to indicate the connected device is not a PoE Powered Device (PD).

■ **10/100/1000BASE-T Interfaces (Port-9 to Port-10)**

LED	Color	Function
LNK/ACT	Green	Lights To indicate the link through that port is successfully established. Blinks To indicate that the switch is actively sending or receiving data over that port.
1000	Orange	Lights To indicate that the port is operating at 1000Mbps . Off If LNK/ACT LED is lit, it indicates that the port is operating at 10/100Mbps . If LNK/ACT LED is off, it indicates that the port is link-down.

■ **10/100/1000BASE-X SFP Interfaces (Port-11 to Port-12)**

LED	Color	Function
LNK/ACT	Green	Lights To indicate the link through that port is successfully established. Blinks To indicate that the switch is actively sending or receiving data over that port.
1000	Orange	Lights To indicate that the port is operating at 1000Mbps . Off If LNK/ACT LED is lit, it indicates that the port is operating at 100Mbps . If LNK/ACT LED is off, it indicates that the port is link-down.

2.1.3 Switch Rear Panel

The rear panel of the Managed Switch consists of the AC/DC inlet power socket. [Figures 2-1-3](#) show the rear panel of the Managed Switch.

NS3502-8P-2T-2S Rear Panel



Figure 2-1-3: Rear Panel of NS3502-8P-2T-2S

■ **AC Power Receptacle**

For compatibility with electrical voltages in most areas of the world, the Managed Switch's power supply can automatically adjust line power in the range of 100-240V AC and 50/60 Hz.

Plug the female end of the power cord firmly into the receptacle on the rear panel of the Managed Switch and the other end of the power cord into an electrical outlet and 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.

Power Notice: 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.

2.2 Installing the 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.

2.2.1 Desktop Installation

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

Step 1: Attach the rubber feet to the recessed areas on the bottom of the Managed Switch.

Step 2: Place the Managed Switch on the desktop or the shelf near an AC power source, as shown in Figure 2-2-1.

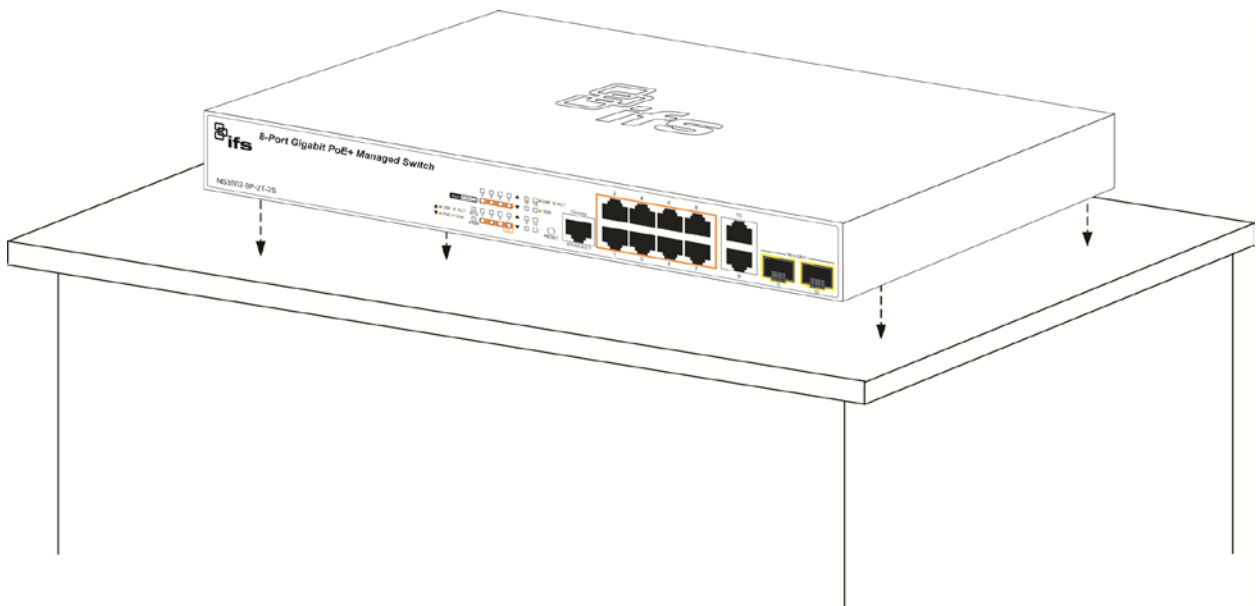


Figure 2-2-1: Place the Managed Switch on the Desktop

Step 3: Keep enough ventilation space between the Managed Switch and the surrounding objects.



Note

When choosing a location, please keep in mind the environmental restrictions discussed in Chapter 1, Section 4, and specifications.

Step 4: Connect the Managed Switch to network devices.

Connect one end of a standard network cable to the 10/100/1000 RJ45 ports on the front of the Managed Switch. Connect the other end of the cable to the network devices such as printer server, workstation or router.



Note

Connection to the Managed Switch requires UTP Category 5e network cabling with RJ45 tips. For more information, please see the Cabling Specification in Appendix A.

Step 5: 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.

Step 1: Place the Managed Switch on a hard flat surface, with the front panel positioned towards the front side.

Step 2: Attach the rack-mount bracket to each side of the Managed Switch with supplied screws attached to the package.

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

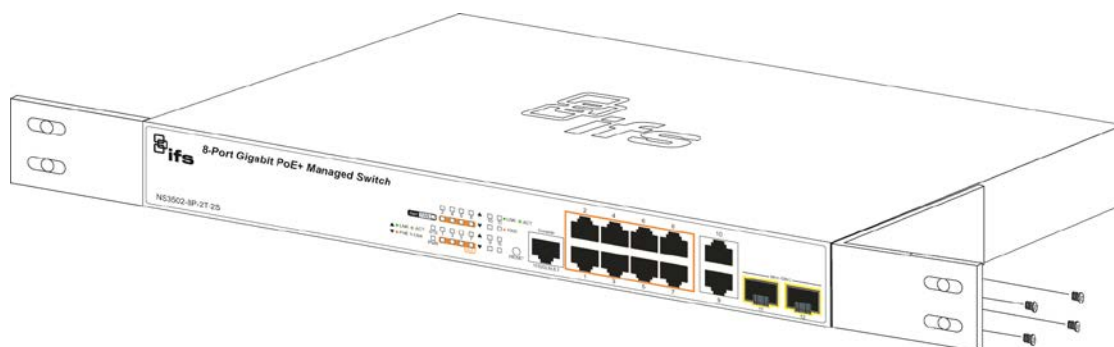


Figure 2-2-2: Attach Brackets to the Managed Switch.



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

Step 3: Secure the brackets tightly.

Step 4: Follow the same steps to attach the second bracket to the opposite side.

Step 5: After the brackets are attached to the Managed Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-2-3.

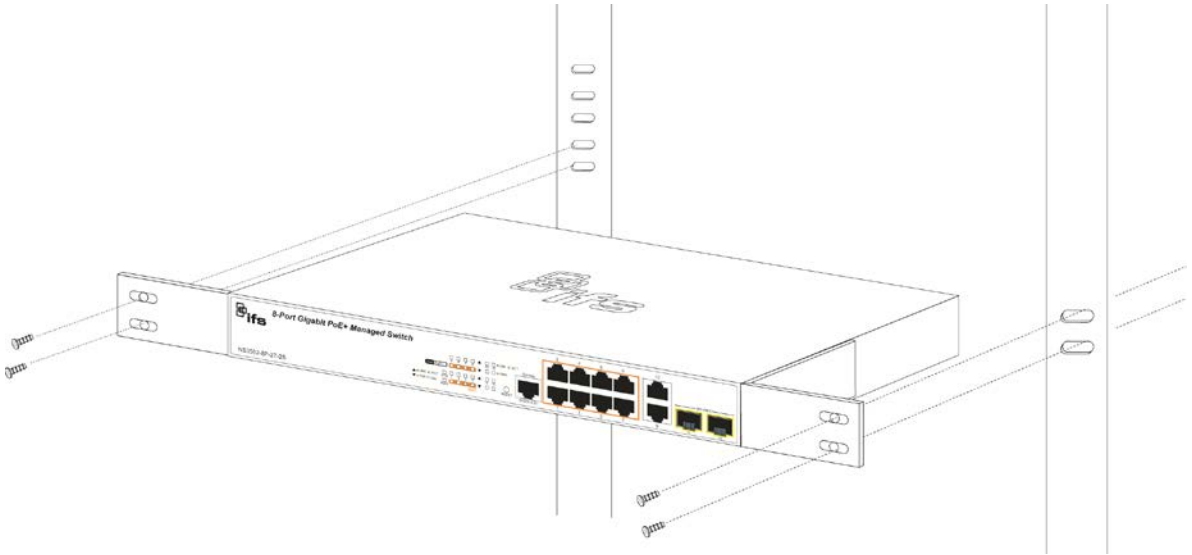


Figure 2-2-3: Mounting Managed Switch in a Rack

Step 6: Proceed with Steps 4 and 5 of session 2.2.1 Desktop Installation to connect the network cabling and supply power to the Managed Switch.

2.2.3 Installing the SFP/SFP+ Transceiver

The sections describe how to insert an SFP/SFP+ transceiver into an SFP/SFP+ slot. The SFP/SFP+ transceivers are hot-pluggable and hot-swappable. You can plug in and out the transceiver to/from any SFP/SFP+ port without having to power down the Managed Switch, as the Figure 2-2-4 shows..

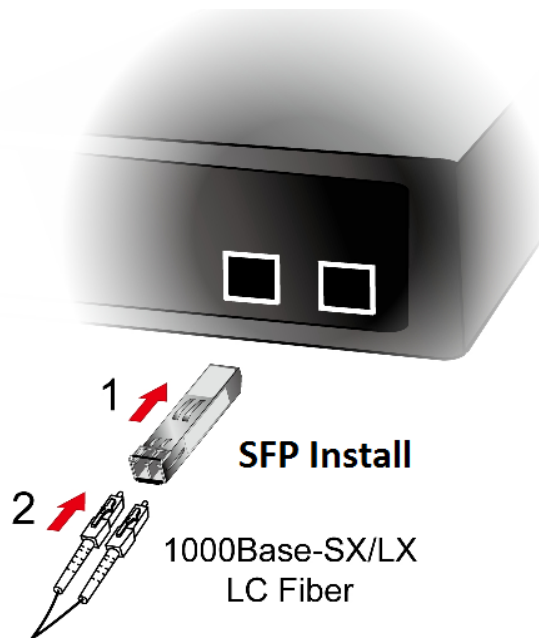


Figure 2-2-4: Plug-in the SFP/SFP+ Transceiver

■ Approved IFS SFP/SFP+ Transceivers

IFS Managed Switch supports both single mode and multi-mode SFP/SFP+ transceivers. The following list of approved IFS SFP/SFP+ transceivers is correct at the time of publication:

Fast Ethernet Transceiver (100BASE-X SFP)

S20-1SLC/A-20	SFP, LC Connector, Single Mode, 10/100 Fast Ethernet, 1 fiber, 1310nm/1550nm, 20km , A End
S20-1SLC/B-20	SFP, LC Connector, Single Mode, 10/100 Fast Ethernet, 1 fiber, 1310nm/1550nm, 20km , B End
S20-2MLC-2	SFP, LC Connector, Multi-Mode, 10/100 Fast Ethernet, 2 fiber,1310nm/1310nm, 2km
S20-2SLC-20	SFP, LC Connector, Single Mode, 10/100 Fast Ethernet, 2 fiber,1310nm/1310nm, 20km

Gigabit Ethernet Transceiver (1000BASE-X SFP)

IFS Model	SFP Description
S30-1SLC/A-10	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1310nm/1550nm, 10km , A End
S30-1SLC/A-20	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1310nm/1550nm, 20km, A End
S30-1SLC/A-60	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1310nm/1550nm, 60km, A End
S30-1SLC/B-10	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1550nm/1310nm, 10km , B End
S30-1SLC/B-20	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1550nm/1310nm, 20km, B End
S30-1SLC/B-60	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1550nm/1310nm, 60km, B End
S30-2MLC	SFP, LC Connector, Multi-Mode, Gigabit, 2 fiber,850nm/850nm, 550m
S30-2MLC-2	SFP, LC Connector, Multi-Mode, Gigabit, 2 fiber,1310nm/1310nm, 2km
S30-2SLC-10	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1310nm/1310nm, 10km
S30-2SLC-30	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1310nm/1310nm, 30km
S30-2SLC-70	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1550nm/1550nm, 70km
S30-RJ	SFP, RJ-45, Gigabit, 100m



It is recommended to use IFS SFP/SFP+ on the Managed Switch. If you insert an SFP/SFP+ transceiver that is not supported, the Managed Switch will not recognize it.

1. Before we connect the NS3502-8P-2T-2S to the other network device, we have to make sure both sides of the SFP transceivers are with the same media type, for example: 100BASE-SX to 1000BASE-SX, 1000Bas-LX to 1000BASE-LX.
2. Check whether the fiber-optic cable type matches with the SFP transceiver requirement.
 - To connect to 1000BASE-SX SFP transceiver, please use the multi-mode fiber cable with one side being the male duplex LC connector type.
 - To connect to 1000BASE-LX SFP transceiver, please use the single-mode fiber cable with one side being the male duplex LC connector type.

■ **Connect the Fiber Cable**

1. Insert the duplex LC connector into the SFP/SFP+ transceiver.
2. Connect the other end of the cable to a device with SFP/SFP+ transceiver installed.
3. Check the LNK/ACT LED of the SFP/SFP+ slot on the front of the Managed Switch. Ensure that the SFP/SFP+ transceiver is operating correctly.
4. Check the Link mode of the SFP/SFP+ port if the link fails. To function with some fiber-NICs or Media Converters, user has to set the port Link mode to “**1000M Force**” or “**100M Force**”.

■ **Remove the Transceiver Module**

1. Make sure there is no network activity anymore.
2. Remove the Fiber-Optic Cable gently.
3. Lift up the lever of the SFP module and turn it to a horizontal position.
4. Pull out the module gently through the lever.

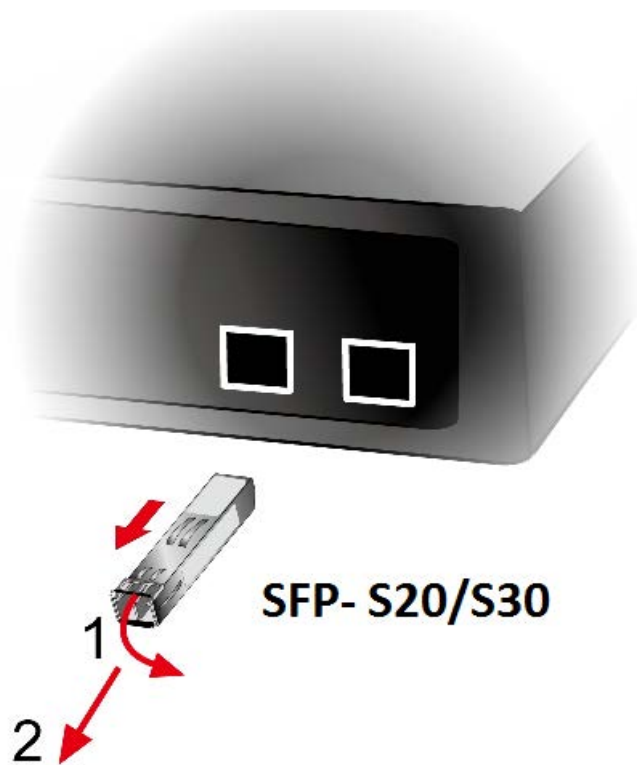


Figure 2-2-5: How to Pull Out the SFP/SFP+ Transceiver



Note

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/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
- Administration Console Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Requirements

- **Workstations** running Windows 2000/XP, 2003, Vista/7/8, 2008, MAC OS9 or later, or Linux, UNIX , or other platforms compatible with **TCP/IP** protocols.
- **Workstation** is installed with **Ethernet NIC** (Network Interface Card)
- **Serial Port** connect (Terminal)
 - The above PC with COM Port (DB9/RS-232) or USB-to-RS232 converter
- 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 8.0 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:

- An administration **console**
- **Web browser** interface
- An external **SNMP-based network management application**

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

Method	Advantages	Disadvantages
Console	<ul style="list-style-type: none"> • No IP address or subnet needed • Text-based • Telnet functionality and HyperTerminal built into Windows 95/98/NT/2000/ME/XP operating systems • Secure 	<ul style="list-style-type: none"> • Must be near the switch or use dial-up connection • Not convenient for remote users • Modem connection may prove to be unreliable or slow
Web Browser	<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 Administration Console

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

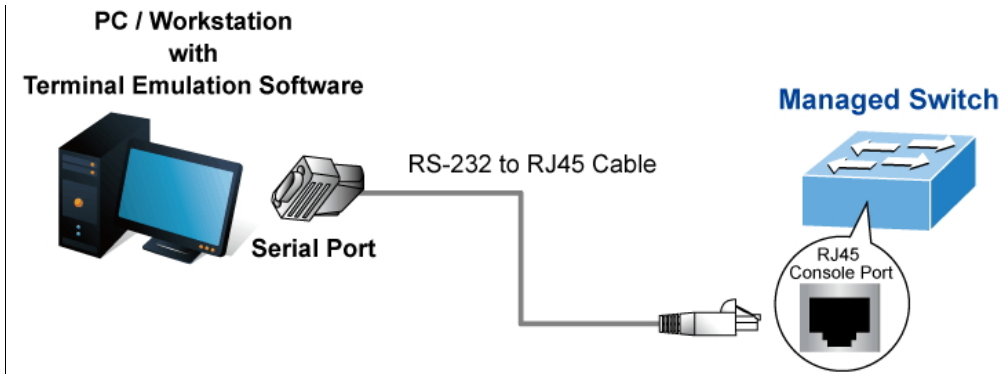


Figure 3-1-1: Console Management

Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as **HyperTerminal**) to the Managed Switch console (serial) port. When using this management method, a **straight DB9 RS232 cable** is required to connect the switch to the PC. After making this connection, configure the terminal-emulation program to use the following parameters:

The default parameters are:

- 115200 bps
- 8 data bits
- No parity
- 1 stop bit

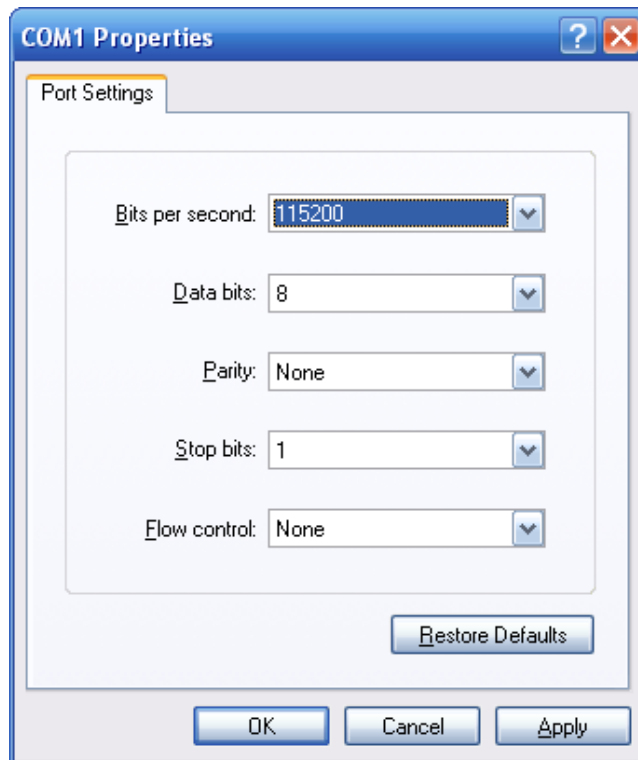


Figure 3-1-2: Terminal Parameter Settings

You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

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 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.

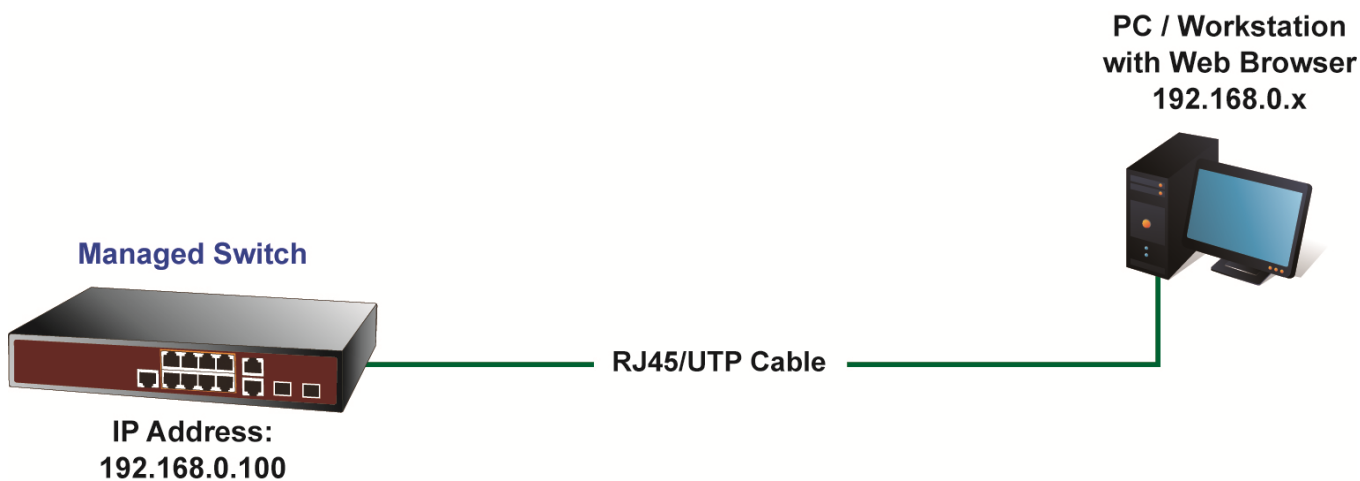


Figure 3-1-3: Web Management

You can then use your Web browser to list and manage the Managed Switch configuration parameters from one central location, just as if you were directly connected to the Managed Switch's console port. Web Management requires either **Microsoft Internet Explorer 8.0** or later, **Safari** or **Mozilla Firefox 1.5** or later.

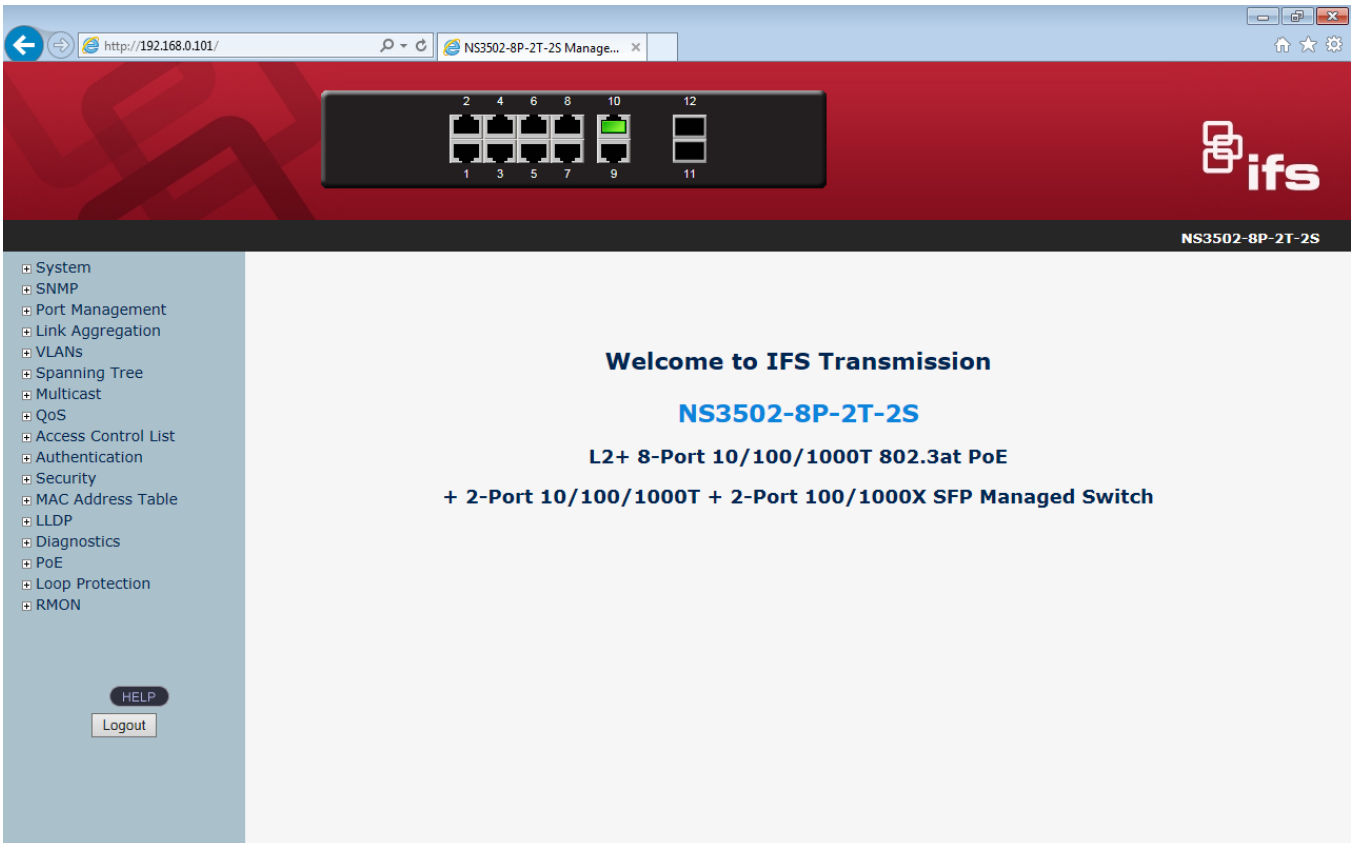


Figure 3-1-4: Web Main Screen of Managed Switch

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 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.

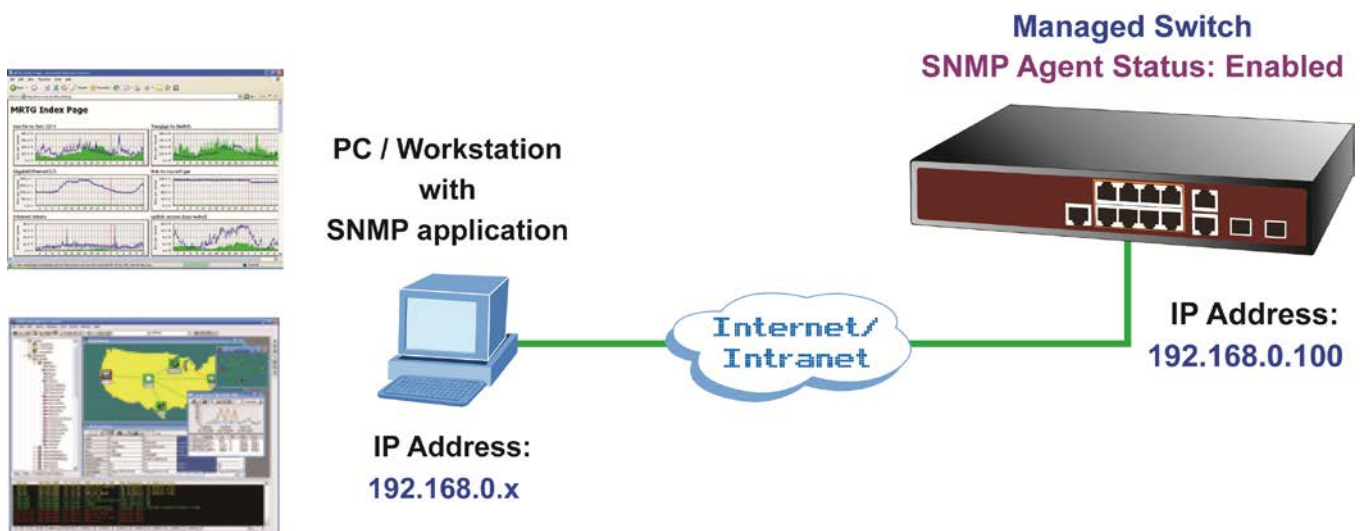


Figure 3-1-5: SNMP Management

3.6 IFS Smart Discovery Utility

For easily listing the Managed Switch in your Ethernet environment, the IFS Smart Discovery Utility from user's manual CD-ROM is an ideal solution. The following installation instructions are to guide you to running the IFS Smart Discovery Utility.

1. Deposit the IFS Smart Discovery Utility in administrator PC.
2. Run this utility as the following screen appears.

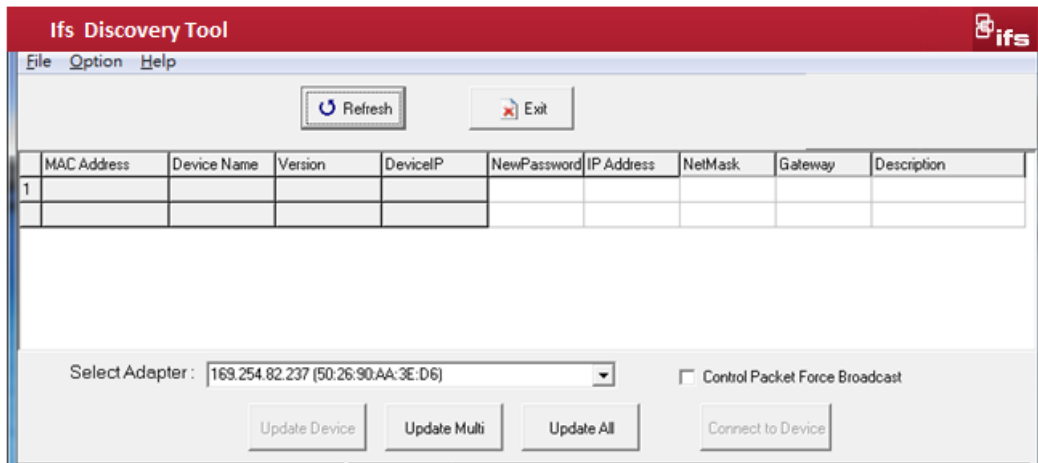


Figure 3-1-6: IFS Smart Discovery Utility Screen



If there are two LAN cards or above in the same administrator PC, choose a different LAN card by using the “**Select Adapter**” tool.

3. Press “**Refresh**” button for the currently connected devices in the discovery list as the screen shows below:

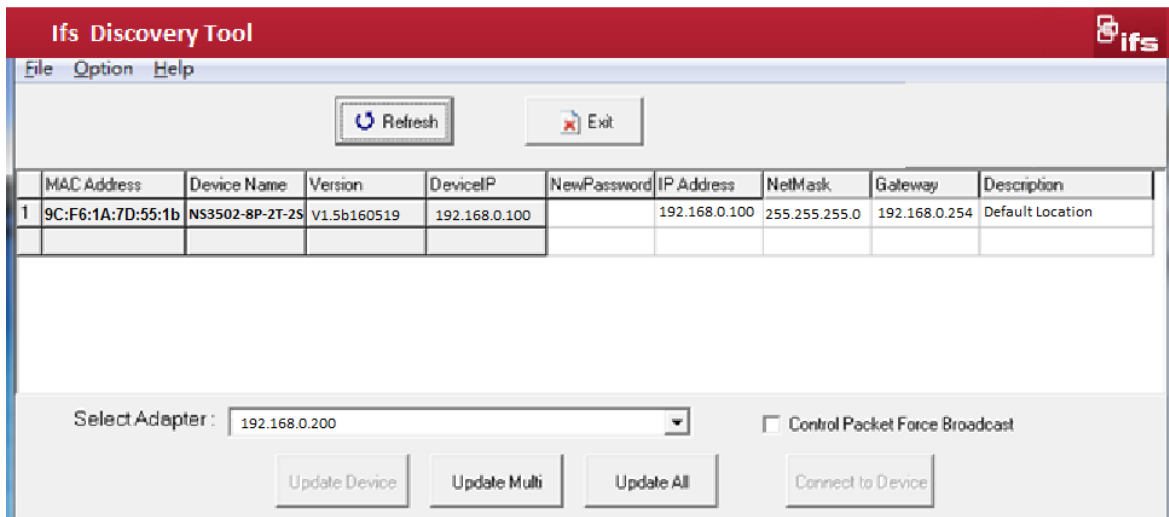


Figure 3-1-7: IFS Smart Discovery Utility Screen

1. This utility shows all necessary information from the devices, such as MAC Address, Device Name, firmware version, and Device IP Subnet address. It can also assign new password, IP Subnet address and description for the devices.

2. After setup is completed, press “**Update Device**”, “**Update Multi**” or “**Update All**” button to take effect. The meaning of the 3 buttons above are shown as below:

- **Update Device:** use current setting on one single device.
- **Update Multi:** use current setting on choose multi-devices.
- **Update All:** use current setting on whole devices in the list.

The same functions mentioned above also can be found in “**Option**” tools bar.

3. To click the “**Control Packet Force Broadcast**” function, it can allow assign new setting value to the Web Smart Switch under a different IP subnet address.

4. Press “**Connect to Device**” button and the Web login screen appears in [Figure 3-1-4](#).

5. Press “**Exit**” button to shut down the IFS Smart Discovery Utility.

4. WEB CONFIGURATION

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

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 8.0. 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.

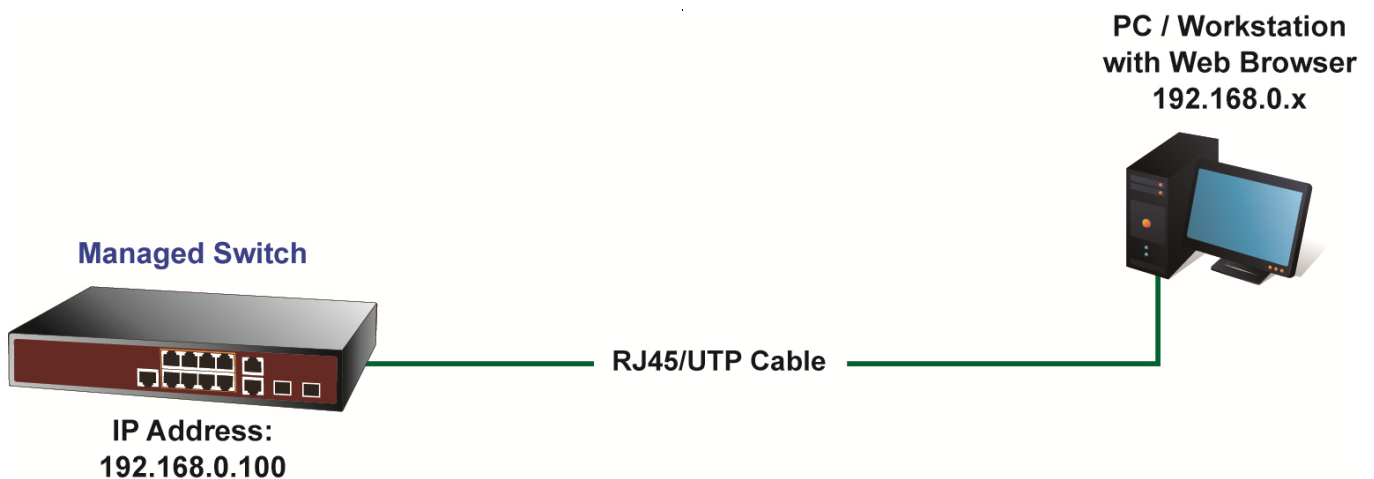


Figure 4-1-1: Web Management

■ Logging on the Managed Switch

1. Use Internet Explorer 8.0 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.

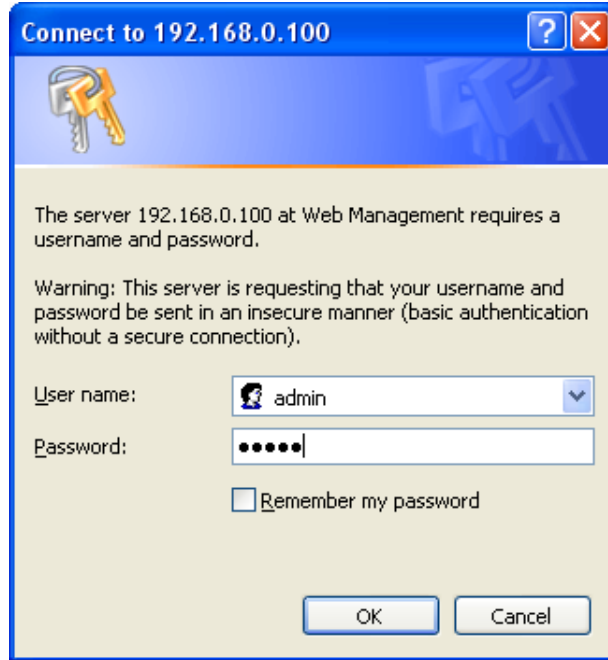


Figure 4-1-2: Login Screen

Default User name: **admin**

Default Password: **admin**

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

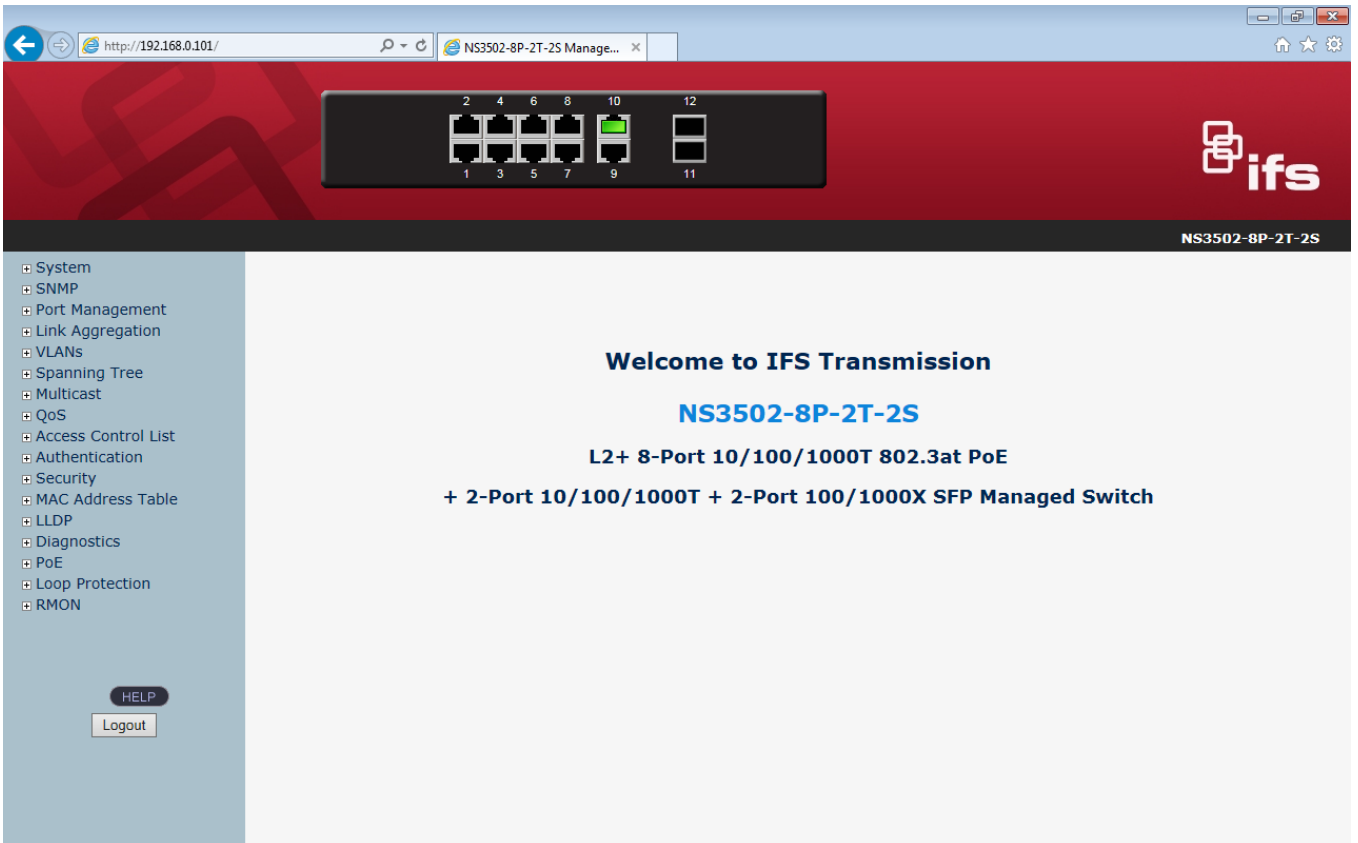


Figure 4-1-3: Web Main Page

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 lets you access all the commands and statistics the Managed Switch provides.



1. It is recommended to use Internet Explorer 8.0 or above to access Managed Switch.
2. The changed IP address takes 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.

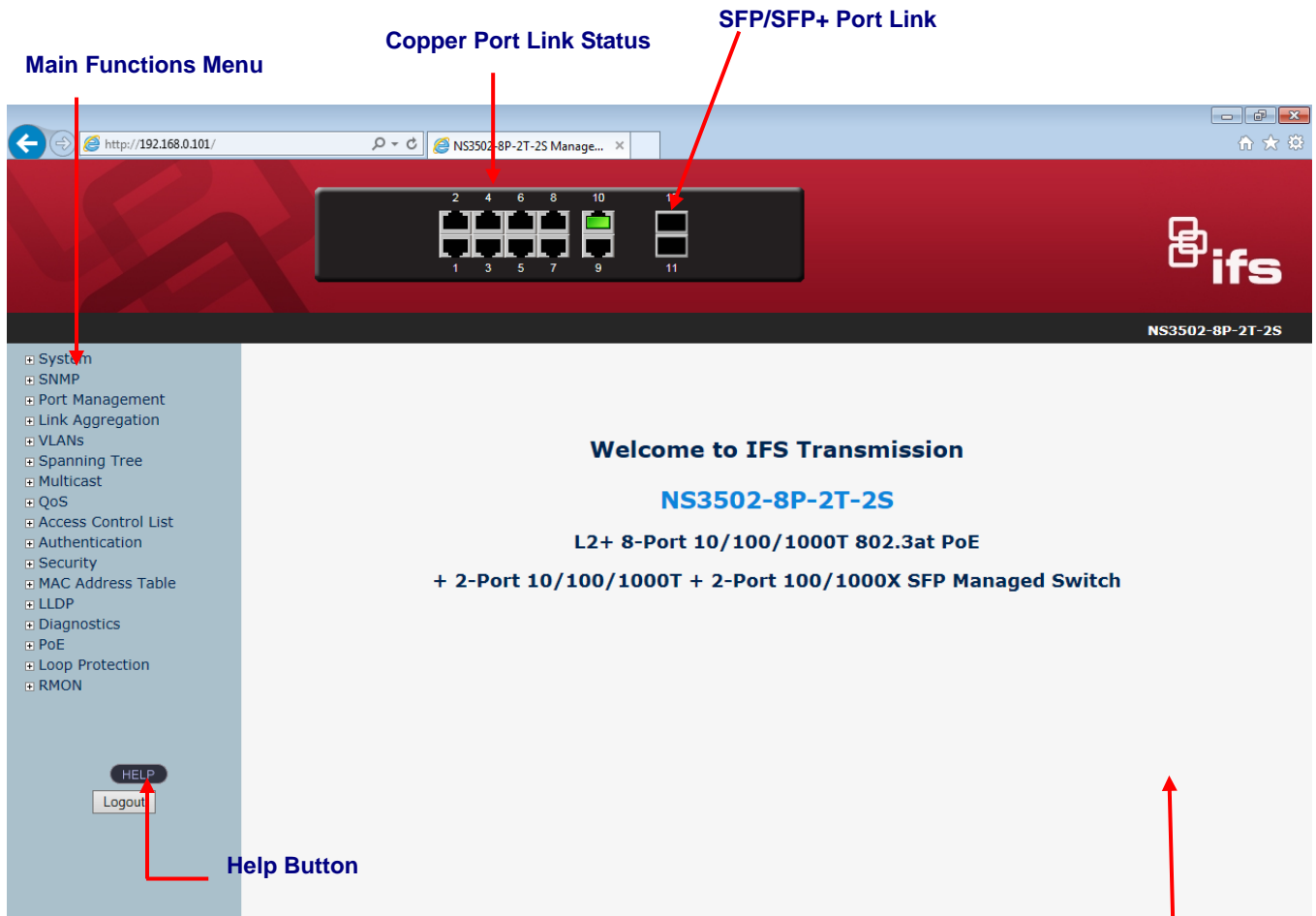


Figure 4-1-4: Web Main Page

Main Screen

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 status are illustrated as follows:

State	Disabled	Down	Link
RJ45 Ports			
SFP Ports			
PoE 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 set up the Managed Switch by selecting the functions those listed in the Main Function. The screen in [Figure 4-1-5](#) appears.

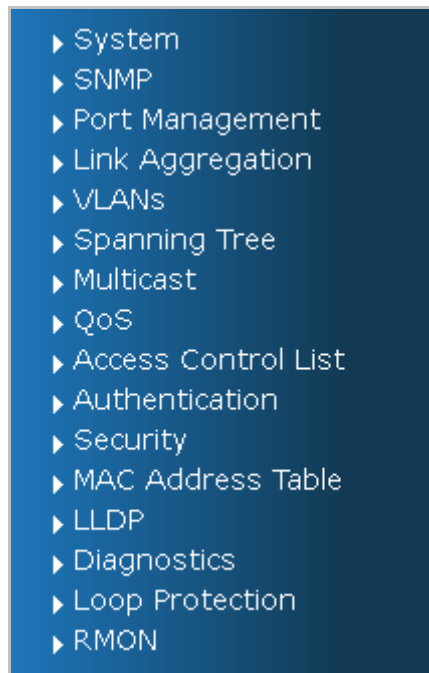


Figure 4-1-5: Managed Switch Main Functions Menu

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. This section has the following items:

- **System Information** The Managed Switch system information is provided here.
- **IP Configuration** Configures the Managed Switch-managed IPv4/IPv6 interface and IP routes on this page.
- **IP Status** This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.
- **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.
- **Privilege Levels** This page provides an overview of the privilege levels.
- **NTP Configuration** Configure NTP server on this page.
- **Time Configuration** Configure time parameter on this page.
- **UPnP** Configure UPnP on this page.
- **DHCP Relay** Configure DHCP Relay on this page.
- **DHCP Relay Statistics** This page provides statistics for DHCP relay.
- **CPU Load** This page displays the CPU load, using an SVG graph.
- **System Log** The Managed Switch system log information is provided here.
- **Detailed Log** The Managed Switch system detailed log information is provided here.
- **Remote Syslog** Configure remote syslog on this page.
- **SMTP Configuration** Configuration SMTP parameters on this page.
- **Web Firmware Upgrade** This page facilitates an update of the firmware controlling the Managed Switch.
- **TFTP Firmware Upgrade** Upgrade the firmware via TFTP server
- **Save Startup Config** This copies *running-config* to *startup-config*, thereby ensuring that the currently active configuration will be used at the next reboot.
- **Configuration Download** You can download the files on the switch.
- **Configuration Upload** You can upload the files to the switch.
- **Configuration Activate** You can activate the configuration file present on the switch.
- **Configuration Delete** You can delete the writable files which stored in flash.
- **Image Select** Configuration active or alternate firmware on this page.
- **Factory Default** You can reset the configuration of the Managed Switch on this page. Only the IP configuration is retained.
- **System Reboot** You can restart the Managed Switch on this page. After restarting, the Managed Switch will boot normally.

4.2.1 System Information

The System Information page provides information for the current device information. System Information 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	
Contact Name	NS3502-8P-2T-2S
Location	
Hardware	
MAC Address	9C:F6:1A:7D:55:22
Temperature	55.0 C - 131.0 F
Time	
System Date	1970-01-01 Thu 00:38:01+00:00
System Uptime	0d 00:38:01
Software	
Software Version	v1.5b160616
Software Date	2016-06-16T10:07:35+0800

Auto-refresh

Figure 4-2-1: System Information Page Screenshot

The page includes the following fields:

Object	Description
• Contact	The system contact configured in SNMP System Information System Contact.
• Name	The system name configured in SNMP System Information System Name.
• Location	The system location configured in SNMP System Information System Location.
• MAC Address	The MAC Address of this Managed Switch.
• Temperature	Indicates chipset temperature.
• System Date	The current (GMT) system time and date. The system time is obtained through the configured NTP Server, if 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 Managed 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; any changes made locally will be undone.

4.2.2 IP Configuration

The IP Configuration includes the IP Configuration, IP Interface and IP Routes. The configured column is used to view or change the IP configuration. The maximum number of interfaces supported is 128 and the maximum number of routes is 32. The 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				
<ul style="list-style-type: none"> • IP Configurations 	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #d3d3d3; width: 20%;">Mode</td> <td>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.</td> </tr> <tr> <td style="background-color: #d3d3d3;">DNS Server</td> <td> This setting controls the DNS name resolution done by the switch. The following modes are supported: <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 </td> </tr> </table>	Mode	Configure whether the IP stack should act as a Host or a Router . In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.	DNS Server	This setting controls the DNS name resolution done by the switch. The following modes are supported: <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
Mode	Configure whether the IP stack should act as a Host or a Router . In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.				
DNS Server	This setting controls the DNS name resolution done by the switch. The following modes are supported: <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 <code>0.0.0.0</code> or IPv6 <code>:::</code> 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.

Auto-refresh

IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	9C:F6:1A:7D:55:22	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.101/24	
VLAN1	IPv6	fe80:9ef6:1aff:fe04:c5c3	

IP Routes

Network	Gateway	Status
0.0.0.0/0	192.168.0.254	<UP GATEWAY HW_RT>
127.0.0.1/32	127.0.0.1	<UP HOST>
192.168.0.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.0.200	Vlan1:fe80:9ef6:1aff:fe04:c5c3

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

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

: Click to refresh the page.

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, press “**Apply**” button to take effect. Please login web interface with new user name and password, the screen in [Figure 4-2-4](#) appears.

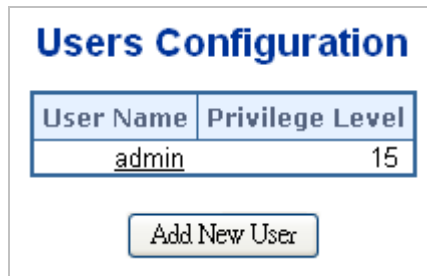


Figure 4-2-4: Users Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • User Name 	The name identifying the user. This is also a link to Add/Edit User.
<ul style="list-style-type: none"> • Privilege Level 	<p>The privilege level of the user.</p> <p>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.</p> <p>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.</p> <p>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.</p>

Buttons

: Click to add a new user.

Add / Edit User

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

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

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Username 	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31 . The valid user name is a combination of letters, numbers and underscores.
<ul style="list-style-type: none"> • Password 	The password of the user. The allowed string length is 1 to 31 .
<ul style="list-style-type: none"> • Password (again) 	Please enter the user's new password here again to confirm.
<ul style="list-style-type: none"> • Privilege Level 	<p>The privilege level of the user.</p> <p>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.</p> <p>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.</p> <p>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.</p>

Buttons

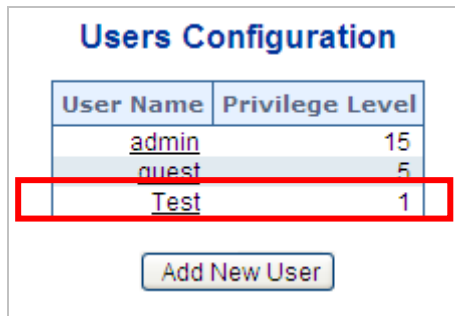
Apply : Click to apply changes.

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)

Once the new user is added, the new user entry shown on the Users Configuration page.



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 the “**Apply**” 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 ▼
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 ▼
Mirroring	5 ▼	10 ▼	5 ▼	10 ▼
MVR	5 ▼	10 ▼	5 ▼	10 ▼
NTP	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 ▼
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 contain 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.

	<ul style="list-style-type: none"> ■ 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 privilege level group has an authorization 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).

Buttons

: Click to apply 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. The NTP Configuration screen in [Figure 4-2-8](#) appears.

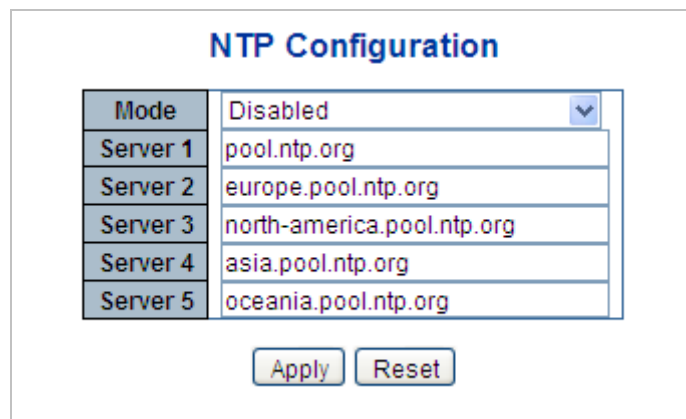




Figure 4-2-8: NTP Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Mode 	<p>Indicates the NTP mode operation. Possible modes are:</p> <ul style="list-style-type: none"> ■ Enabled: Enable NTP mode operation. When enable NTP mode operation, the agent forward and to transfer 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"> • Server # 	<p>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 separates each field (:).</p> <p>For example, 'fe80:9ef6:1aff:fe04:c5c3'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example, ':::192.1.2.34'.</p>

Buttons

: Click to apply changes.

: 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	<input type="text"/> (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 <input type="text"/> (1 - 1440) Minutes


Figure 4-2-9: Time Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Time Zone 	Lists various Time Zones world wide. Select appropriate Time Zone from the drop down and click Save to set.
<ul style="list-style-type: none"> 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)
<ul style="list-style-type: none"> 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).
<ul style="list-style-type: none"> Start Time Settings 	<ul style="list-style-type: none"> Week - Select the starting week number. Day - Select the starting day.

	<ul style="list-style-type: none"> • 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.

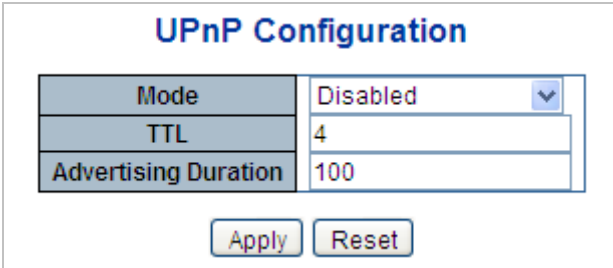


Figure 4-2-10: UPnP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Mode	Indicates the UPnP operation mode. Possible modes are: <ul style="list-style-type: none"> ■ Enabled: Enable UPnP mode operation. ■ Disabled: Disable UPnP mode operation.

	When the mode is enabled, two ACEs are added automatically to trap UPnP related packets to CPU. The ACEs are automatically removed when the mode is disabled.
• TTL	The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range of 1 to 255.
• Advertising Duration	The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive 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.

Buttons

Apply: Click to apply changes

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

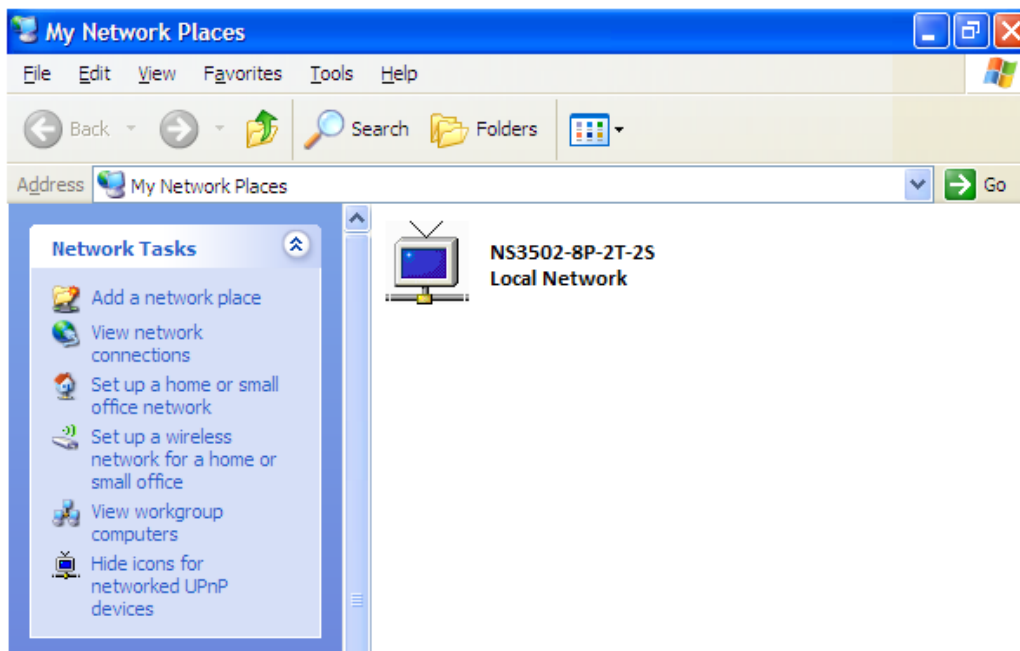


Figure 4-2-11: UPnP devices show on Windows My Network Place

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. 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 equals the DHCP relay agent's MAC address. The DHCP Relay Configuration screen in [Figure 4-2-12](#) appears.

DHCP Relay Configuration	
Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Keep


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 enabling DHCP relay mode operation, the agent forwards and transfers DHCP messages between the clients and the server when they are not on the same subnet domain. And the DHCP broadcast message won't flood 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 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 enabling DHCP relay information mode operation, the agent inserts specific information (option82) into a DHCP message when forwarding to DHCP server and removing 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 enabling DHCP relay information mode operation, if agent receives 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 that already contains it. ■ Drop: Drop the package when receiving a DHCP message that already contains relay information.

Buttons

: Click to apply changes

: 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.

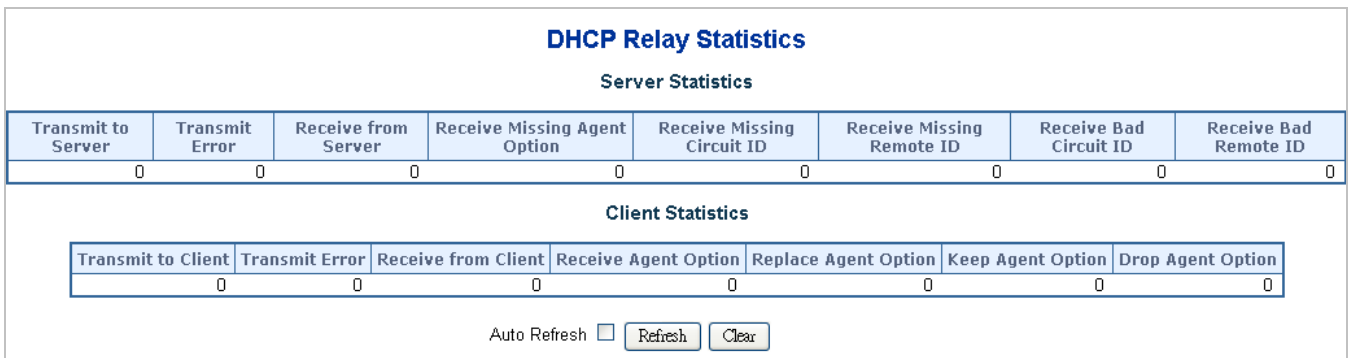


Figure 4-2-13: DHCP Relay Statistics Page Screenshot

The page includes the following fields:

Server Statistics

Object	Description
• Transmit to Server	The packets number that relayed from client to server.
• Transmit Error	The packets number that errors sending packets to clients.
• Receive from Server	The packets number that received packets from server.
• Receive Missing Agent Option	The packets number that received packets without agent information options.
• Receive Missing Circuit ID	The packets number that received packets which the Circuit ID option was missing.
• Receive Missing Remote ID	The packets number that received packets which Remote ID option was missing.
• Receive Bad Circuit ID	The packets number that the Circuit ID option did not match known circuit ID.
• Receive Bad Remote ID	The packets number that the Remote ID option did not match known Remote ID.

Client Statistics

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

Buttons

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

: Click to refresh the page immediately.

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

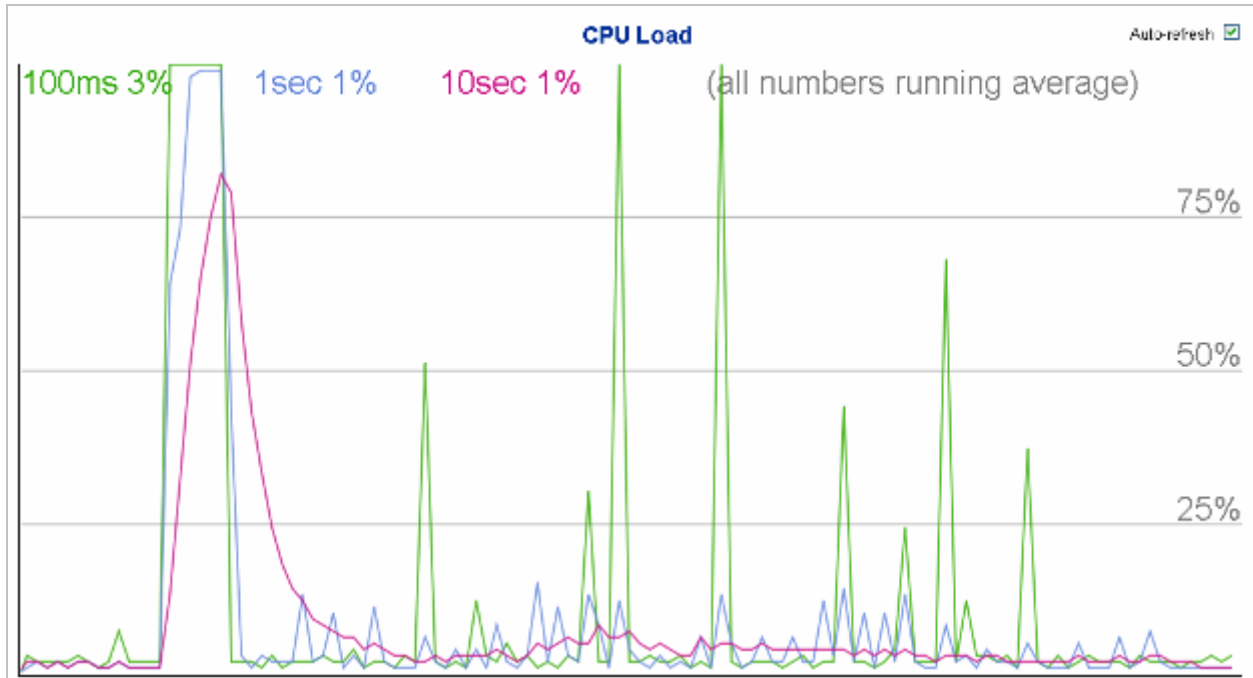


Figure 4-2-14: CPU Load Page Screenshot

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

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"> • Clear Level 	To clear the system log entry level. 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.

: Updates the system log entries, starting from the current entry ID.

: Flushes the selected log entries.

: Hides the selected log entries.

: Downloads the selected log entries.

- : Updates the system log entries, starting from the first available entry ID.
- : Updates the system log entries, ending at the last entry currently displayed.
- : Updates the system log entries, starting from the last entry currently displayed.
- : Updates the system log entries, ending at the last available entry ID.

4.2.13 Detailed Log

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

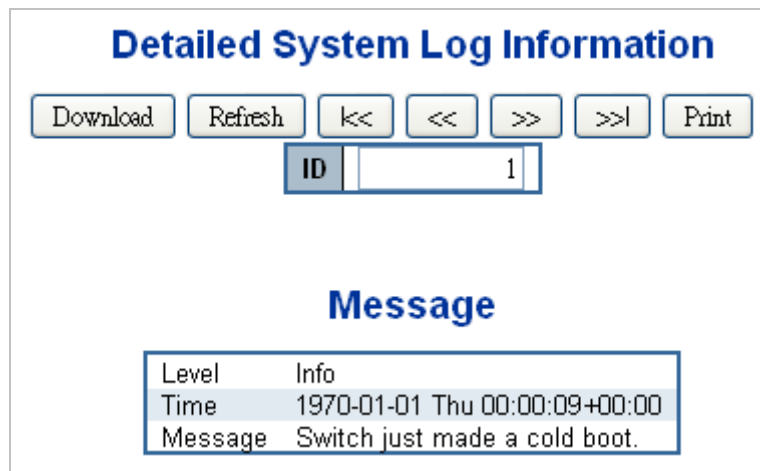

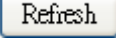







Figure 4-2-15: Detailed Log Page Screenshot

The page includes the following fields:

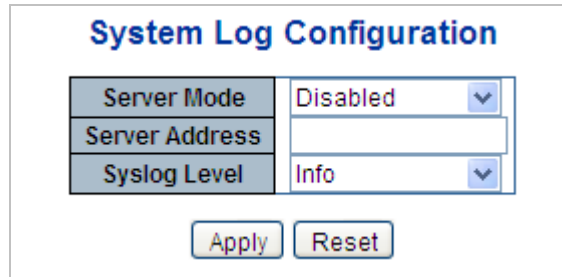
Object	Description
• ID	The ID (≥ 1) of the system log entry.
• Message	The message of the system log entry.

Buttons

- : Download the system log entry to the current entry ID.
- : 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 the system log entry to the current entry ID.

4.2.14 Remote Syslog

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



System Log Configuration	
Server Mode	Disabled
Server Address	
Syslog Level	Info
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Figure 4-2-17: Remote Syslog Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• 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 remote syslog mode operation.■ Disabled: Disable remote syslog mode operation.
<ul style="list-style-type: none">• Syslog Server IP	<p>Indicates the IPv4 host address of syslog server. If the switch provides 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.■ Warning: Send warnings and errors.■ Error: Send errors.

Buttons

: Click to apply changes

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

4.2.15 SMTP Configuration

This page facilitates an SMTP Configuration on the switch. The SMTP Configure screen in [Figure 4-2-18](#) appears.

Field	Value	Constraint
SMTP Mode	<input type="checkbox"/> Enable	
SMTP Server	interlogix.com	(<128 Digits)
SMTP Port	25	(1 ~ 65535)
SMTP Authentication	<input type="checkbox"/> Enable	
Authentication User Name	1234	(< 64 Digits)
Authentication Password	••••	(< 21 Digits)
E-mail From	abcd@interlogix.com	(< 128 Digits)
E-mail Subject	UTC IFS	(< 64 Digits)
E-mail 1 To	abcd@interlogix.com	(< 128 Digits)
E-mail 2 To	abcd@interlogix.com	(< 128 Digits)

Buttons: Apply, Reset

Figure 4-2-18: SMTP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• SMTP Mode	Controls whether SMTP is enabled on this switch.
• SMTP Server	Type the SMTP server name or the IP address of the SMTP server.
• SMTP Port	Set port number of SMTP service.
• SMTP Authentication	Controls whether SMTP authentication is enabled. If authentication is required when an e-mail is sent.
• Authentication User Name	Type the user name for the SMTP server if Authentication is Enable.
• Authentication Password	Type the password for the SMTP server if Authentication is Enable.
• E-mail From	Type the sender's E-mail address. This address is used for reply e-mails.
• E-mail Subject	Type the subject/title of the e-mail.
• E-mail 1 To	Type the receiver's e-mail address.
• E-mail 2 To	

Buttons

test: Send a test mail to mail server to check this account is available or not.

Save: Click to save changes.

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

4.2.16 Web Firmware Upgrade

This page facilitates an update of the firmware controlling the switch. The Web Firmware Upgrade screen in [Figure 4-2-19](#) appears.

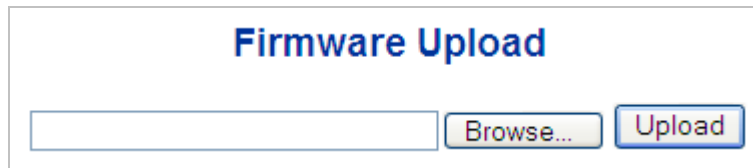


Figure 4-2-19: Web Firmware Upgrade Page Screenshot

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

1. Click **System** -> **Web Firmware Upgrade**.
2. The Firmware Upgrade screen is displayed as in [Figure 4-2-19](#).
3. Click the "Browse" button of the Main page, the system would pop up the file selection menu to choose firmware.
4. Select on the firmware then click "Upload", the **Software Upload Progress** would show the file with upload status.
5. Once the software is loaded to the system successfully, the following screen appears. The system will load the new software after reboot.

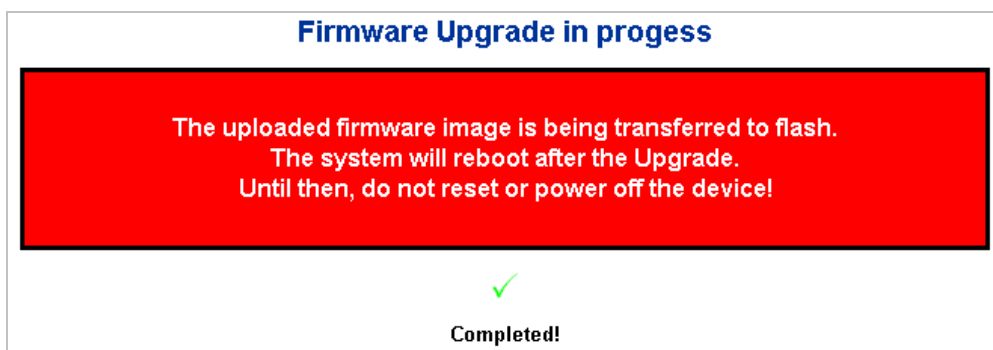


Figure 4-2-20: Software Successfully Loaded Notice Screen



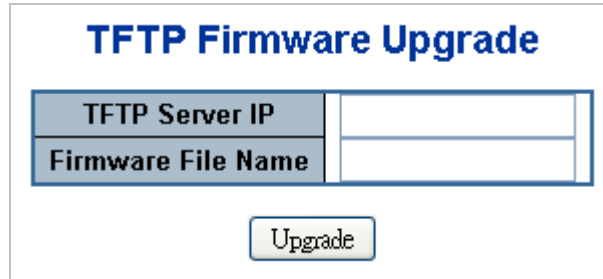
DO NOT Power OFF the Managed Switch until the update progress is complete.



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.

4.2.17 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 4-2-21](#) appears.



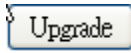
The screenshot shows a web page titled "TFTP Firmware Upgrade". It contains a form with two input fields: "TFTP Server IP" and "Firmware File Name". Below the form is a button labeled "Upgrade".

Figure 4-2-20: 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.

4.2.18 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 4-2-22](#) appears. After saving the configuration, the screen [Figure 4-2-23](#) will appear.

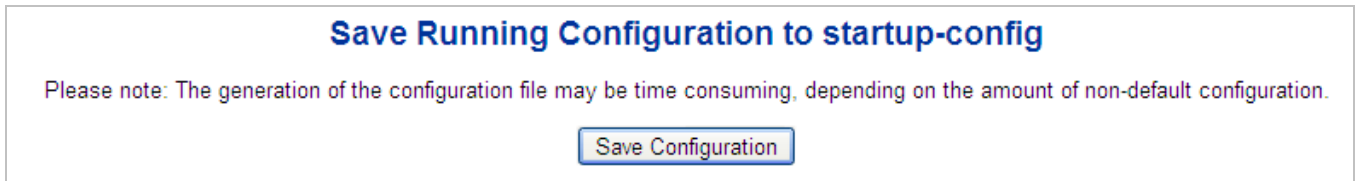


Figure 4-2-22: Configuration Save Page Screenshot



Figure 4-2-23: Finish Saving Page Screenshot

4.2.19 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 4-2-24](#) shown below.

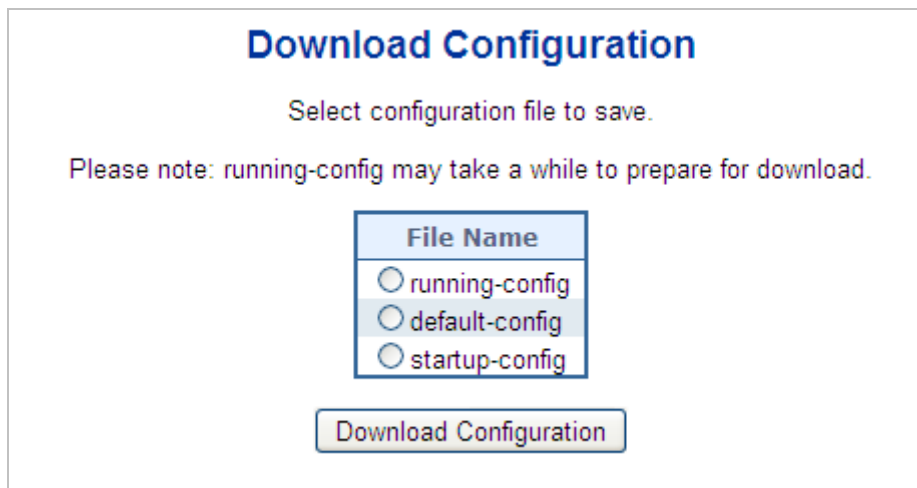


Figure 4-2-24: Configuration Download Page Screenshot

4.2.20 Configuration Upload

Configuration Upload page allows the upload the running-config and startup-config on the switch. Please refer to the Figure 4-2-25 shown below.

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	<input type="text"/>

Figure 4-2-25: 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.

4.2.21 Configuration Activate

Configuration Activate page allows to activate the startup-config and default-config files present on the switch. Please refer to the Figure 4-2-26 shown below.


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

Figure 4-2-26: 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.

4.2.22 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 4-2-27 shown below.

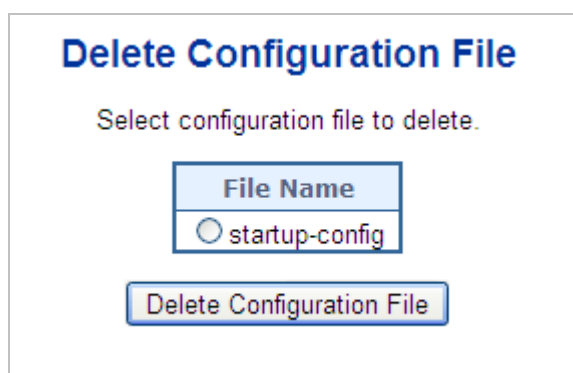


Figure 4-2-27: Configuration Delete Page Screenshot

4.2.23 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 4-2-28 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.
-




Figure 4-2-28: 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.

Buttons

 Click to use the alternate image. This button may be disabled depending on system state.

4.2.24 Factory Default

You can reset the configuration of the Managed 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 4-2-29](#) appears.

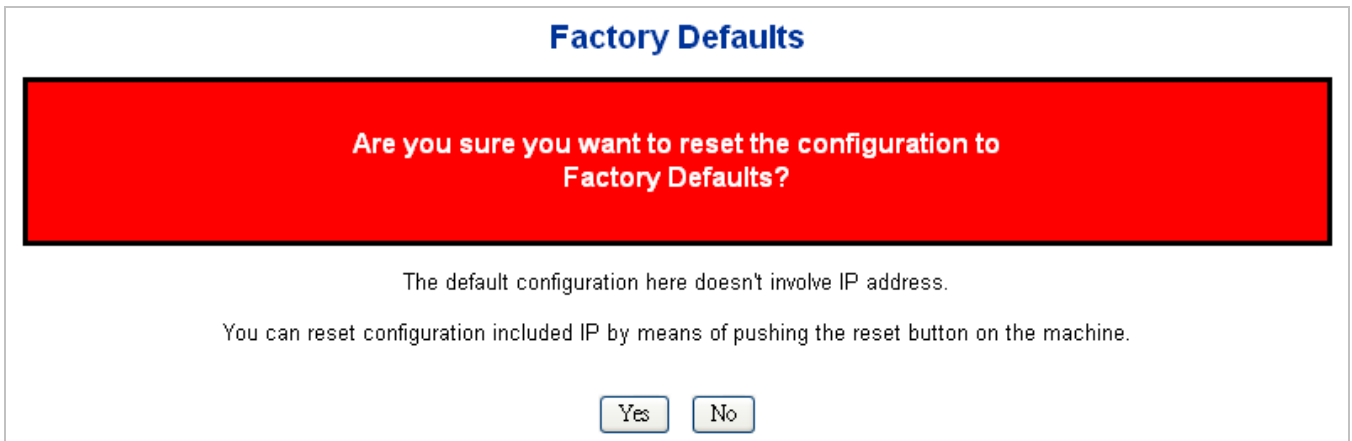


Figure 4-2-29: Factory Default Page Screenshot

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.

4.2.25 System Reboot

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user have to re-login the WEB interface about 60 seconds later, the System Reboot screen in [Figure 4-2-30](#) appears.

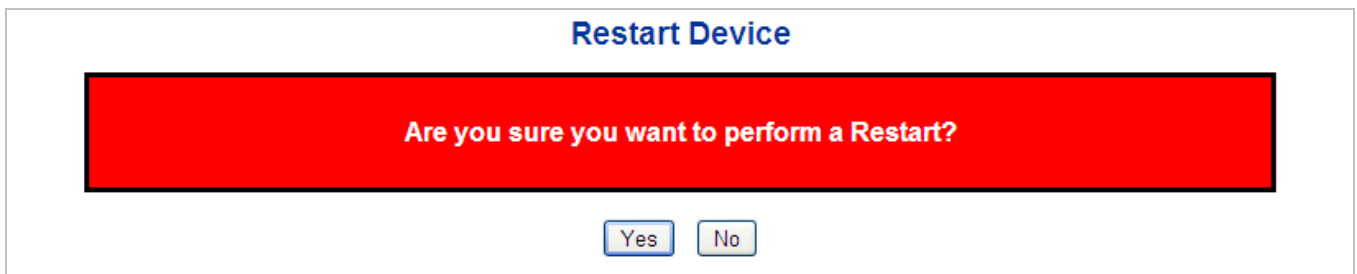
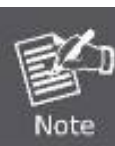


Figure 4-2-30: System Reboot Page Screenshot

Buttons

: Click to reboot the system.

: Click to return to the Port State page without rebooting the system.



You can also check the **SYS LED** on the front panel to identify whether the System is loaded completely or not. If the SYS LED is blinking, then it is in the firmware load stage; if the SYS LED light is on, you can use the Web browser to login the Managed Switch.

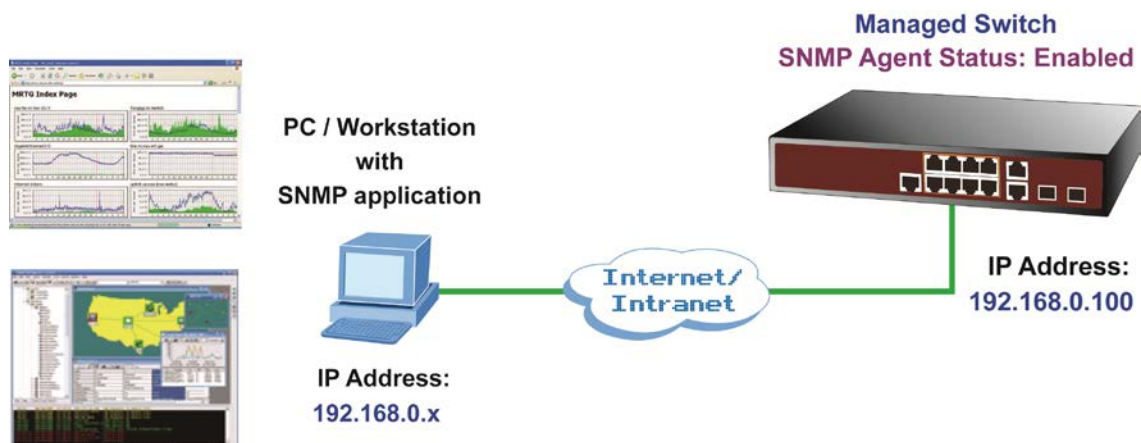
4.3 Simple Network Management Protocol

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.
- **Trap Configuration** Configure SNMP trap on this page.
- **System Information** The system information is provided here.
- **SNMPv3 Communities** Configure SNMPv3 communities table on this page.
- **SNMPv3 Users** Configure SNMPv3 users table on this page.
- **SNMPv3 Groups** Configure SNMPv3 groups table on this page.
- **SNMPv3 Views** Configure SNMPv3 views table on this page.
- **SNMPv3 Access** Configure SNMPv3 accesses table on this page.

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

Apply Reset


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


The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Mode	Indicates the SNMP mode operation. Possible modes are: <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. 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"> • 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 	<p>Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.</p>

Buttons

: Click to apply changes

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

4.3.3 SNMP 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 type="text"/>
Trap Mode	Disabled ▼
Trap Version	SNMP v2c ▼
Trap Community	Public
Trap Destination Address	<input 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 type="text"/>
Trap Security Name	None ▼

SNMP Trap Event

System	<input type="checkbox"/> Warm Start <input type="checkbox"/> Cold Start	
Interface	<input type="checkbox"/> Enable	
	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"/> Authentication Fail	
Switch	<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
<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • 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.
• Trap Destination Address	Indicates the SNMP trap destination address.
• Trap Destination Port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.
• Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: <ul style="list-style-type: none"> ■ Enabled: Enable SNMP trap authentication failure. ■ Disabled: Disable SNMP trap authentication failure.
• Trap Inform Timeout (seconds)	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147 .
• Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255 .
• Trap Probe Security Engine ID	Indicates the SNMPv3 trap probe security engine ID mode of operation. Possible values are: <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.
• Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.
• Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.
• System	Enable/disable that the Interface group's traps. Possible traps are: <ul style="list-style-type: none"> ■ Warm Start: Enable/disable Warm Start trap. ■ Cold Start: Enable/disable Cold Start trap.
• Interface	Indicates that the Interface group's traps. Possible traps are: <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.
• AAA	Indicates that the AAA group's traps. Possible traps are: <ul style="list-style-type: none"> ■ Authentication Fail: Enable/disable SNMP trap authentication failure trap.

<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.

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.

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.

Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0

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 apply 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.

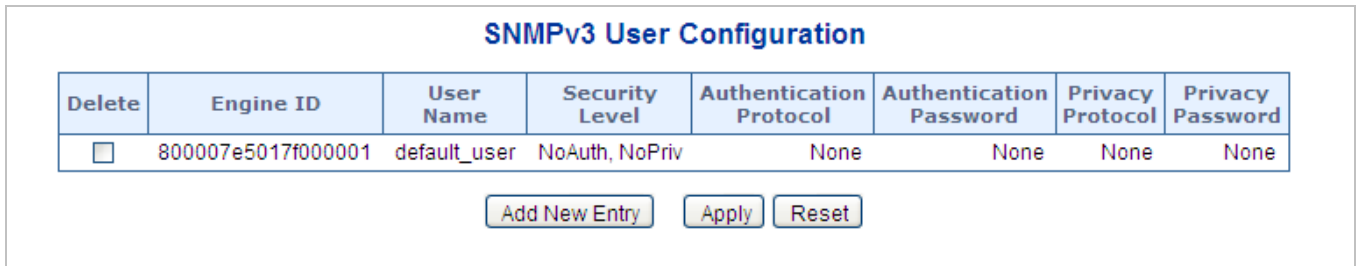


Figure 4-3-5: SNMPv3 Users Configuration Page Screenshot

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"> Engine ID 	<p>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.</p> <p>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.</p>
<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, and the allowed content is ASCII characters from 33 to 126.
<ul style="list-style-type: none"> Security Level 	<p>Indicates the security model that this entry should belong to. Possible security models are:</p> <ul style="list-style-type: none"> ■ NoAuth, NoPriv: None authentication and none privacy. ■ Auth, NoPriv: Authentication and none privacy. ■ Auth, Priv: Authentication and privacy. <p>The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.</p>
<ul style="list-style-type: none"> Authentication Protocol 	<p>Indicates the authentication protocol that this entry should belong to. Possible authentication protocol are:</p> <ul style="list-style-type: none"> ■ None: None authentication protocol.

	<ul style="list-style-type: none"> ■ 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. <p>The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.</p>
<ul style="list-style-type: none"> • Authentication Password 	<p>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.</p>
<ul style="list-style-type: none"> • 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. ■ AES: An optional flag to indicate that this user uses AES authentication protocol.
<ul style="list-style-type: none"> • Privacy Password 	<p>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.</p>

Buttons

Add New Entry: Click to add a new user entry.

Apply: Click to apply 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.

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 apply 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 4-3-7](#) appears.



Figure 4-3-7: SNMPv3 Views 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.

<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>In 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 Entry**: Click to add a new view entry.
- Apply**: Click to apply 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 	<p>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.</p>
<ul style="list-style-type: none"> • Security Model 	<p>Indicates the security model that this entry should belong to. Possible security models are:</p> <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 	<p>Indicates the security model that this entry should belong to. Possible security models are:</p> <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 	<p>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.</p>
<ul style="list-style-type: none"> • Write View Name 	<p>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.</p>

Buttons

Add New Entry: Click to add a new access entry.

Apply: Click to apply changes

Reset: 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 Module Information** Display 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	
			Current	Configured	Current Rx	Current Tx	Configured			
*				<All>				10056	<All>	
1		●	1Gfdx	Auto	×	×		10056	Discard	
2		●	Down	Auto	×	×		10056	Discard	
3		●	Down	Auto	×	×		10056	Discard	
4		●	Down	Auto	×	×		10056	Discard	
5		●	Down	Auto	×	×		10056	Discard	
6		●	Down	Auto	×	×		10056	Discard	
7		●	Down	Auto	×	×		10056	Discard	
8		●	Down	Auto	×	×		10056	Discard	

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.
• Port Description	Indicates the per port description.
• 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.

<ul style="list-style-type: none"> • 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"> ■ Auto - Setup Auto negotiation for copper interface. ■ 10Mbps HDX - Force sets 10Mbps/Half-Duplex mode. ■ 10Mbps FDX - Force sets 10Mbps/Full-Duplex mode. ■ 100Mbps HDX - Force sets 100Mbps/Half-Duplex mode. ■ 100Mbps FDX - Force sets 100Mbps/Full-Duplex mode. ■ 1Gbps FDX - Force sets 1000Mbps/Full-Duplex mode. ■ Auto Fiber (10G) – Setup 10G fiber port for negotiation automatically. ■ Disable - Shutdown the port manually.
<ul style="list-style-type: none"> • 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>
<ul style="list-style-type: none"> • Maximum Frame Size 	<p>Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 10056 bytes.</p>
<ul style="list-style-type: none"> • 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.



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

Buttons

Apply: Click to apply 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.

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	1076	1047	158972	862468	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0

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

Download : Download the Port Statistics Overview result as EXECL file.

Refresh : Click to refresh the page immediately.

Clear : Clears the counters for all ports.

Print : Print the Port Statistics Overview result.

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

4.4.3 Port Statistics Detail

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

Detailed Port Statistics Port 1			
Port 1		Auto-refresh <input type="checkbox"/>	Refresh <input type="button" value="Refresh"/> Clear <input type="button" value="Clear"/>
Receive Total		Transmit Total	
Rx Packets	2335	Tx Packets	2066
Rx Octets	431172	Tx Octets	1531131
Rx Unicast	2039	Tx Unicast	2050
Rx Multicast	48	Tx Multicast	11
Rx Broadcast	248	Tx Broadcast	5
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	1465	Tx 64 Bytes	242
Rx 65-127 Bytes	175	Tx 65-127 Bytes	53
Rx 128-255 Bytes	66	Tx 128-255 Bytes	523
Rx 256-511 Bytes	553	Tx 256-511 Bytes	203
Rx 512-1023 Bytes	76	Tx 512-1023 Bytes	284
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	761
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	2283	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	2066
Receive Error Counters		Transmit Error Counters	
Rx Drops	52	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	52		

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 has an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

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

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

Object	Description
• Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
• Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
• Rx Undersize	The number of short frames received with valid CRC.
• Rx Oversize	The number of long frames received with valid CRC.
• Rx Fragments	The number of short frames received with invalid CRC.
• Rx Jabber	The number of long frames 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 frames are frames that are smaller than 64 bytes.
- 2 Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

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

Buttons

: Click 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 Module Information

The NS3502-8P-2T-2S has supported the SFP module with **digital diagnostics monitoring (DDM)** function, this feature is also known as digital optical monitoring (DOM). You can check the physical or operational status of an SFP module via the SFP Module Information page. This page shows the operational status, such as the transceiver type, speed, wavelength, optical output power, optical input power, temperature, laser bias current and transceiver supply voltage in real time. You can also use the 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)
11	--	--	--	--	--	--	--	--	--
12	--	--	--	--	--	--	--	--	--

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"> ■ 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 get from the SFP module. Different vendors SFP modules might shows different speed information.
<ul style="list-style-type: none"> • Wave Length (nm) 	Display the wavelength of current SFP module, the wavelength value is get from the SFP module. Use this column to check if the wavelength values of two nodes are the matched while the fiber connection is failed.
<ul style="list-style-type: none"> • Distance (m) 	Display the supports distance of current SFP module, the distance value is get from the SFP module.
<ul style="list-style-type: none"> • Temperature (C) – SFP DDM Module Only 	Display the temperature of current SFP DDM module, the temperature value is get from the SFP DDM module.
<ul style="list-style-type: none"> • Voltage(V) – SFP DDM Module Only 	Display the voltage of current SFP DDM module, the voltage value is get from the SFP DDM module.

<ul style="list-style-type: none"> • Current(mA) – SFP DDM Module Only 	Display the Ampere of current SFP DDM module, the Ampere value is get from the SFP DDM module.
<ul style="list-style-type: none"> • TX power (dBm) – SFP DDM Module Only 	Display the TX power of current SFP DDM module, the TX power value is get from the SFP DDM module.
<ul style="list-style-type: none"> • RX power (dBm) – SFP DDM Module Only 	Display the RX power of current SFP DDM module, the RX power value is get from the SFP DDM module.

Buttons

SFP Monitor Event Alert: send trap

Warning Temperature: degrees C

Check SFP Monitor Event Alert box; it will be in accordance with your warning temperature setting and allows users to record message out via SNMP Trap.

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

: Click to apply changes

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

: Click to refresh the page immediately.

4.4.5 Port Mirror

Configure port Mirroring on this page. This function provide to monitoring 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

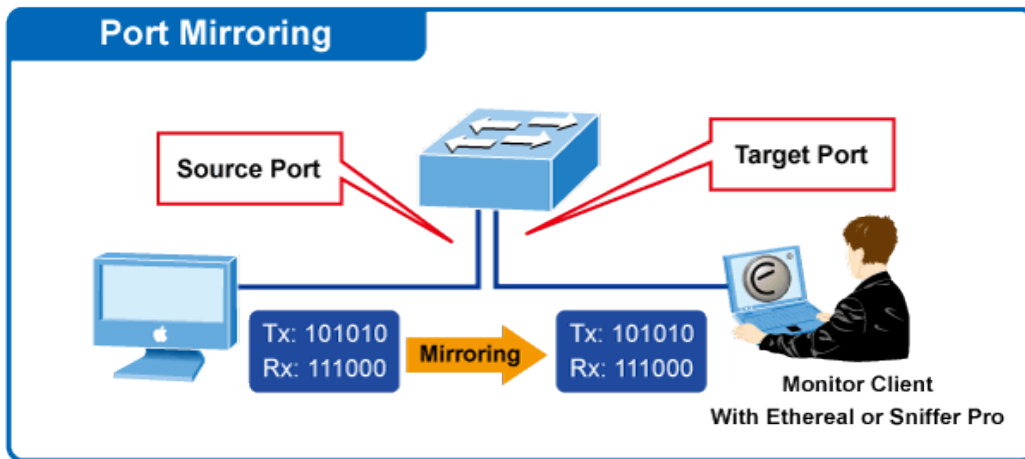


Figure 4-4-7: Port Mirror Application

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 4-4-8](#) appears.

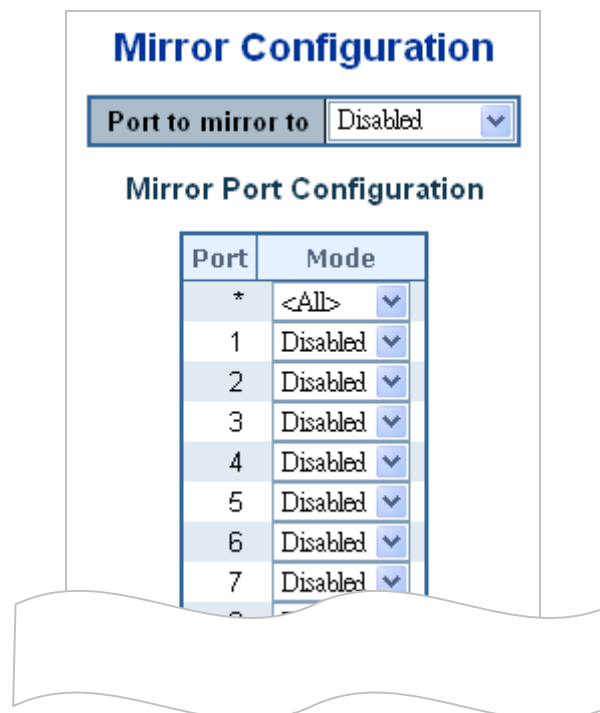


Figure 4-4-8: Mirror Configuration Page Screenshot

The page includes the following fields:


Object	Description
<ul style="list-style-type: none"> • Port to mirror on 	Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port. Disabled disables mirroring.


<ul style="list-style-type: none"> • Port 	The logical port for the settings contained in the same row.
<ul style="list-style-type: none"> • Mode 	<p>Select mirror mode.</p> <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 or 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

 **Apply**: Click to apply changes

 **Reset**: 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.

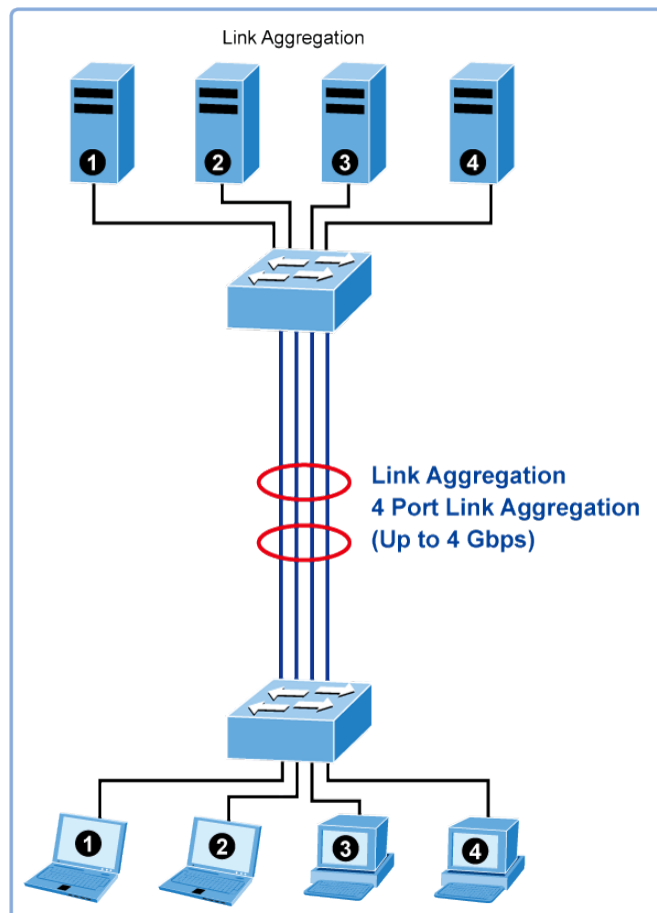


Figure 4-5-1: Link Aggregation

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

It allows a maximum of 10 ports to be aggregated at the same time. The Managed Switch support 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 aggregation s 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.

Hash Code Contributors

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

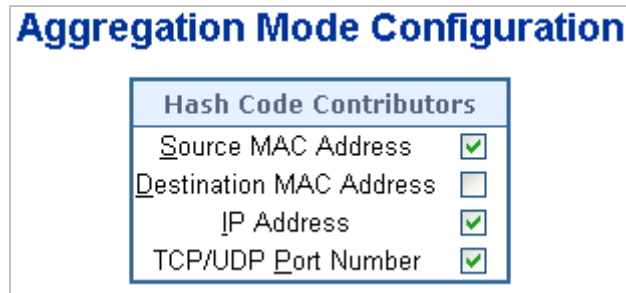


Figure 4-5-2 : Aggregation Mode Configuration Page Screenshot

The page includes the following fields:

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

Static Aggregation Group Configuration

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

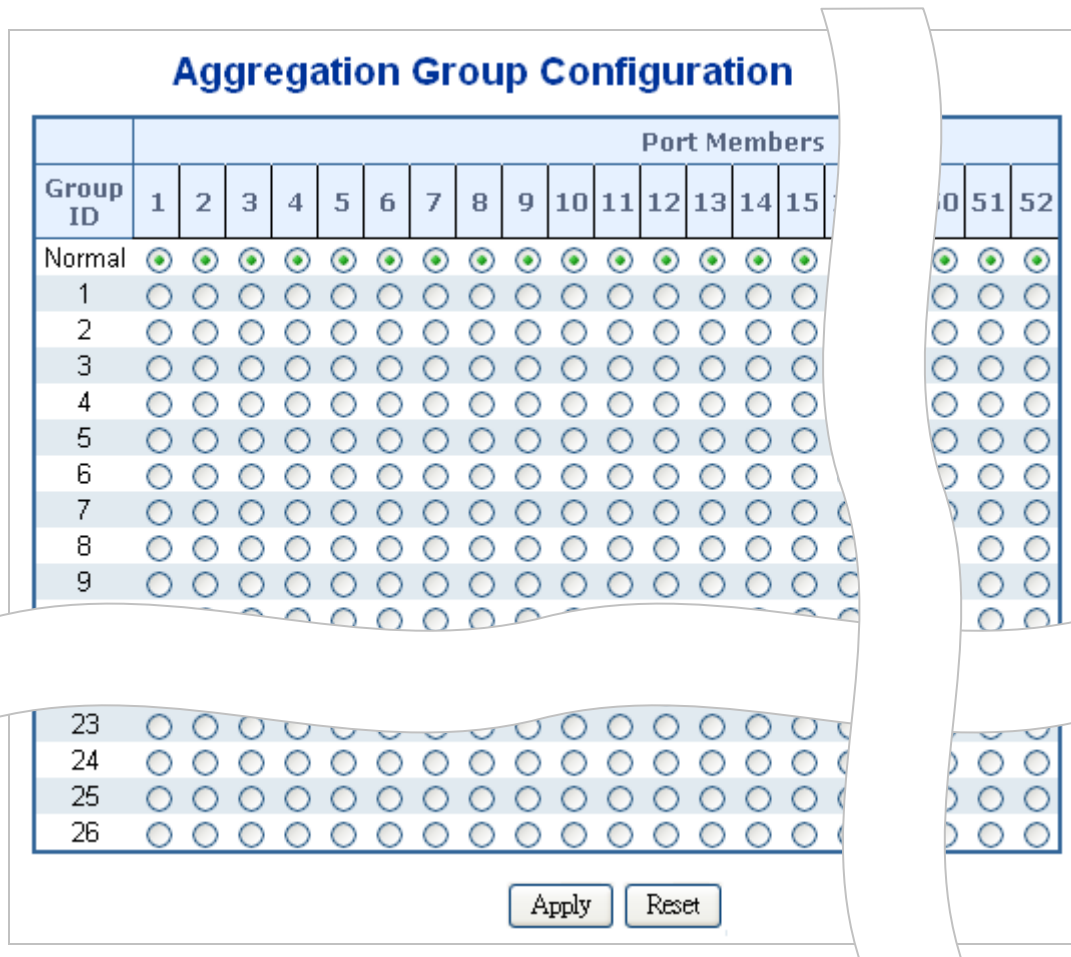
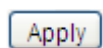


Figure 4-5-3: Aggregation Group Configuration Page Screenshot

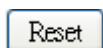
The page includes the following fields:

.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.

Buttons



: Click to apply changes



: 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 Configuration screen in [Figure 4-5-4](#) appears.

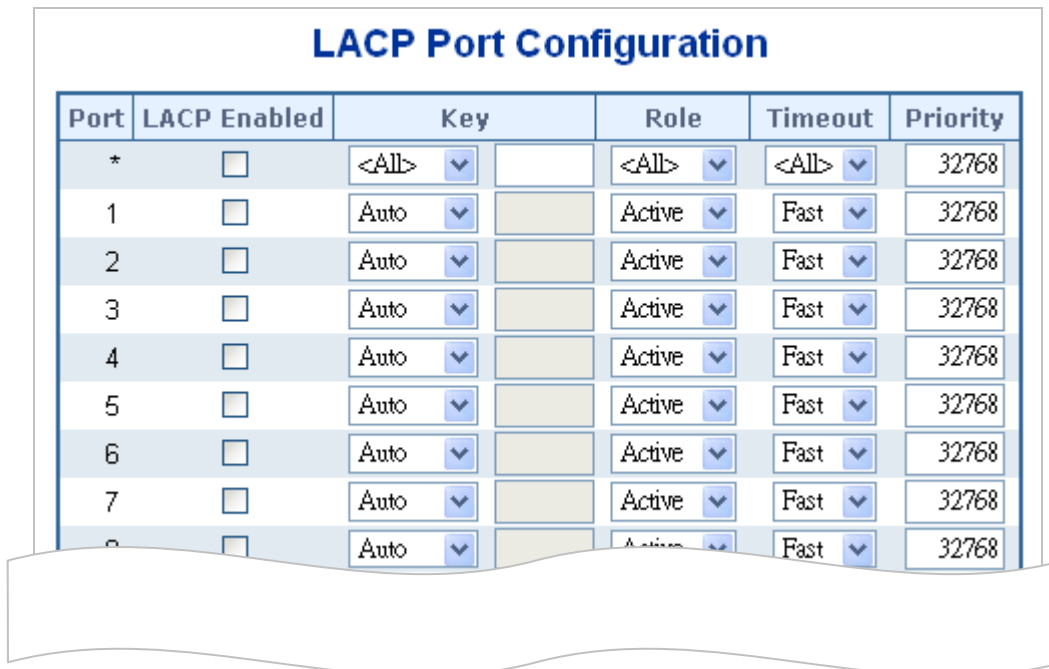



Figure 4-5-4 : LACP Port Configuration Page Screenshot


The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	The switch port number.
<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • 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.</p> <p>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>
<ul style="list-style-type: none"> • 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).
<ul style="list-style-type: none"> • 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.

<ul style="list-style-type: none"> • Priority 	<p>The Priority controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.</p>
---	---

Buttons

: Click to apply 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 displays the current LACP aggregation Groups and LACP Port status. The LACP System Status screen in [Figure 4-5-5](#) appears.

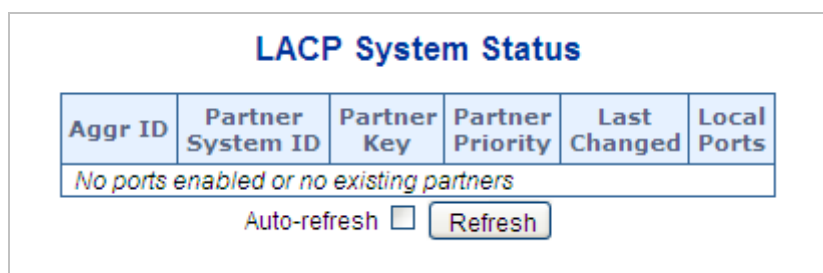


Figure 4-5-5: LACP System Status Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Aggr ID 	<p>The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'</p>
<ul style="list-style-type: none"> • Partner System ID 	<p>The system ID (MAC address) of the aggregation partner.</p>
<ul style="list-style-type: none"> • Partner Key 	<p>The Key that the partner has assigned to this aggregation ID.</p>
<ul style="list-style-type: none"> • Partner Priority 	<p>The priority of the aggregation partner.</p>
<ul style="list-style-type: none"> • Last changed 	<p>The time since this aggregation changed.</p>
<ul style="list-style-type: none"> • Local Ports 	<p>Shows which ports are a part of this aggregation for this switch.</p>

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.

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	-	-	-	-	-

Figure 4-5-6: LACP Status Page Screenshot

The page includes the following fields:

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

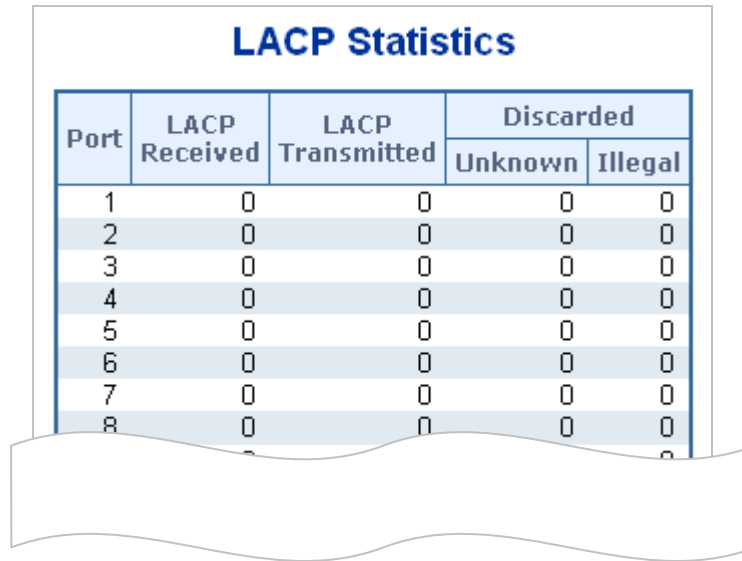
Buttons

Click 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.



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

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 segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

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



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

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

VLAN allow 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:

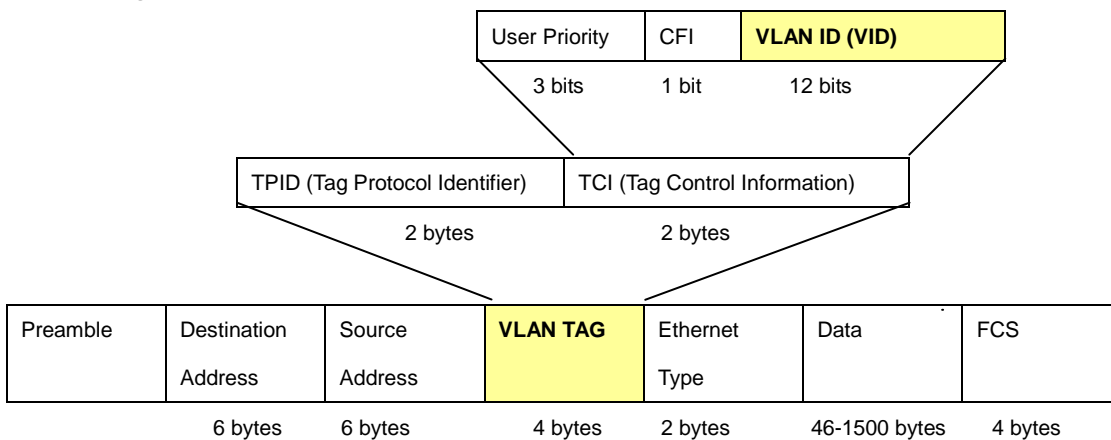
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

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.

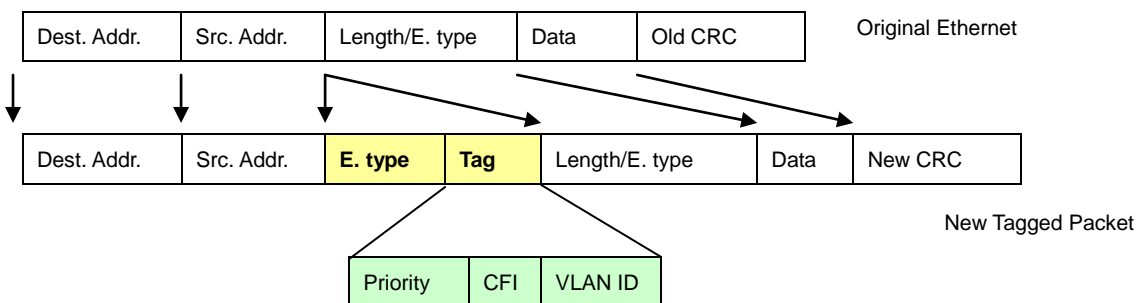
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

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.

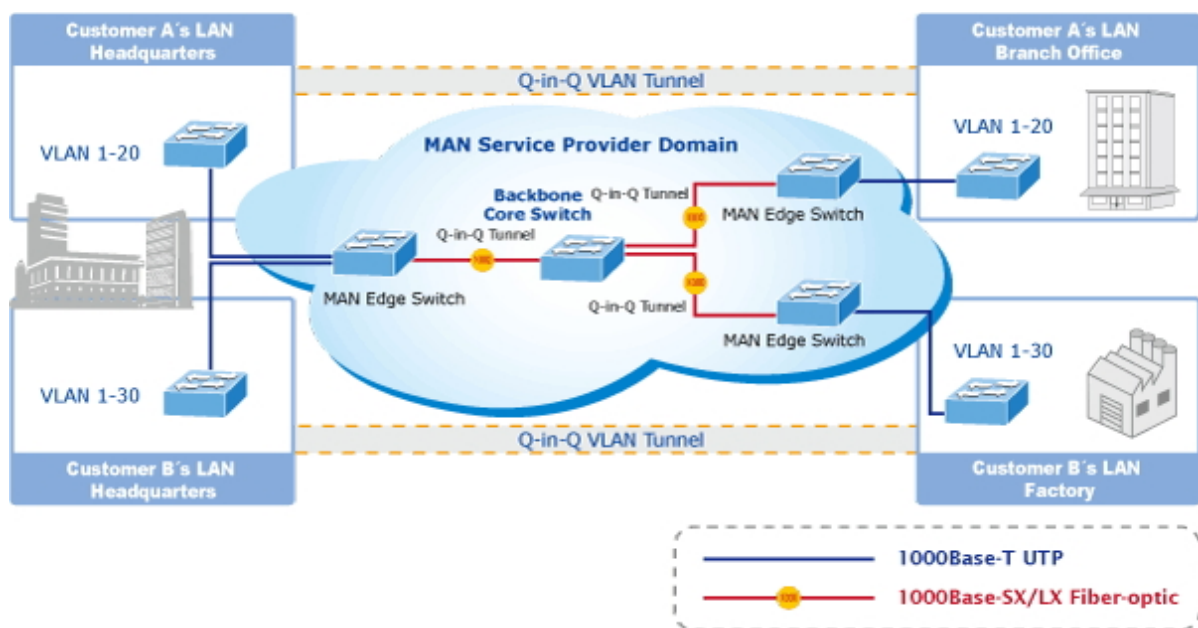
Frame Income / Frame Leave	Income Frame is tagged	Income Frame is untagged
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remain untagged

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

■ IEEE 802.1Q Tunneling (Q-in-Q)

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

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



The Managed Switch supports multiple VLAN tags and can therefore be used in MAN 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: <code>1,10-13,200,300</code>. Spaces are allowed in between the delimiters.</p>
<ul style="list-style-type: none"> Ethertype for Custom 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	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<All>	1	<All>	<input type="checkbox"/>	<All>	<All>	1	
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	

Figure 4-6-2 : Port VLAN Configuration Screenshot

The page includes the following fields:

Object	Description						
<ul style="list-style-type: none"> • Port 	<p>This is the logical port number for this row.</p>						
<ul style="list-style-type: none"> • Mode 	<table border="1"> <tr> <td data-bbox="338 392 523 817">Access</td> <td data-bbox="523 392 1404 817"> <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 • 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 </td> </tr> <tr> <td data-bbox="338 817 523 1400">Trunk</td> <td data-bbox="523 817 1404 1400"> <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 </td> </tr> <tr> <td data-bbox="338 1400 523 1780">Hybrid</td> <td data-bbox="523 1400 1404 1780"> <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 or, 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 </td> </tr> </table>	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 • 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 or, 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
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 • 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 or, 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 						

	<p>Tagging configuration is set to untag Port VLAN.</p> <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: On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress. ■ C-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. ■ S-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag. ■ S-Custom-Port: On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.
<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"> ■ If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. ■ If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. <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"> ■ Tagged and Untagged Both tagged and untagged frames are accepted. ■ Tagged Only Only tagged frames are accepted on ingress. Untagged frames are discarded.

	<ul style="list-style-type: none"> ■ Untagged Only Only untagged frames are accepted on ingress. Tagged frames are discarded.
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"> ■ Untag Port VLAN Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. ■ Tag All All frames, whether classified to the Port VLAN or not, are transmitted with a tag. ■ Untag All All frames, whether classified to the Port VLAN or not, are transmitted without a tag.
<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

Apply: Click to apply changes

Reset: 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.

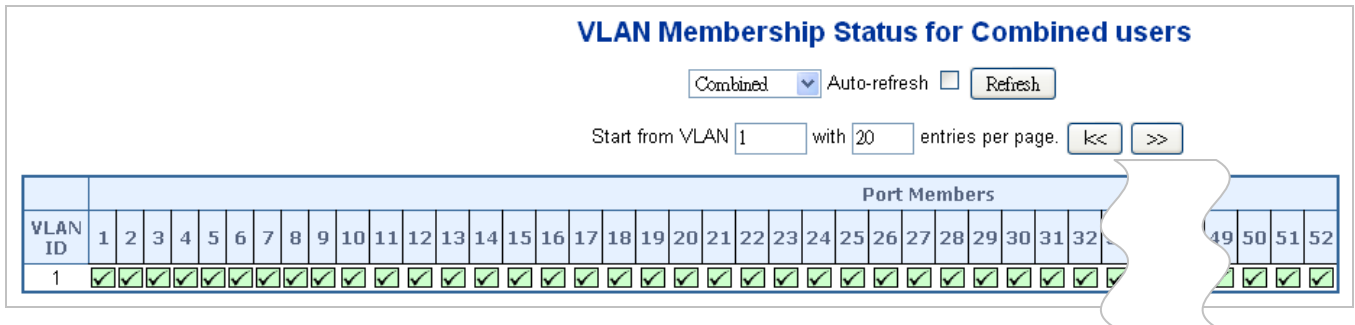


Figure 4-6-4: VLAN Membership Status for Static User Page Screenshot

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</p>

	allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.
--	--

Buttons

Combined ▾ : Select VLAN Users from this drop down list.

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

Refresh : Click to refresh the page immediately.

<< : 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.

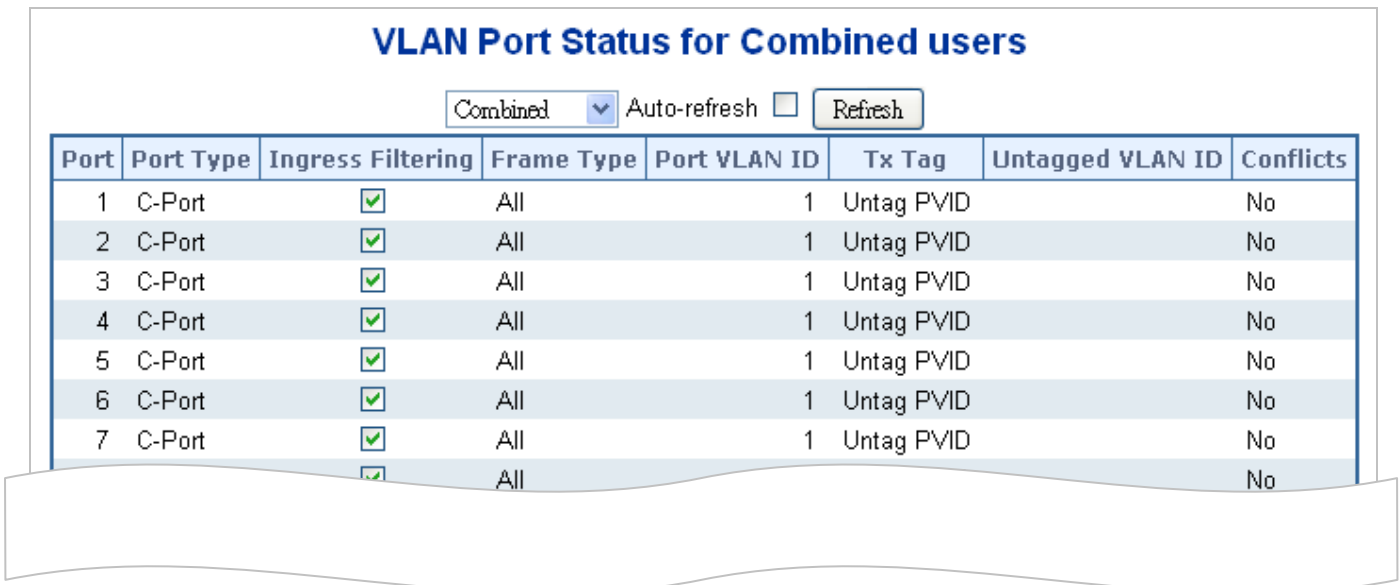


Figure 4-6-5: VLAN Port Status for Combined users Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	The logical port for the settings contained in the same row.
<ul style="list-style-type: none"> • Port Type 	Show the VLAN Awareness for the port. If VLAN awareness is enabled, the tag is removed from tagged frames received on the port. VLAN tagged frames are classified to the VLAN ID in the tag. If VLAN awareness is disabled, all frames are classified to the Port VLAN ID and

	tags are not removed.
• Ingress Filtering	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	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: <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.

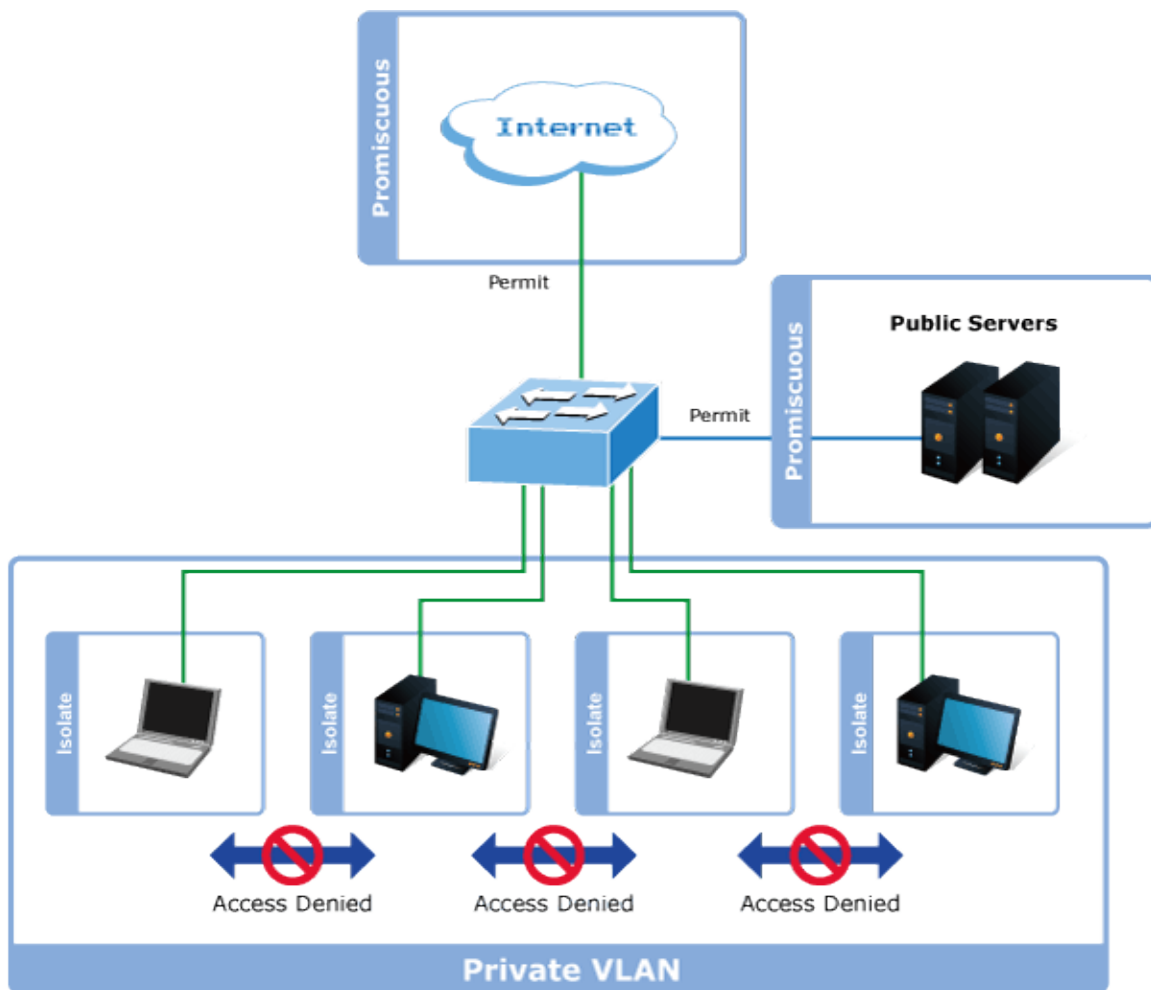
: Click to refresh the page immediately.

4.6.6 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 4-6-6](#) appears.

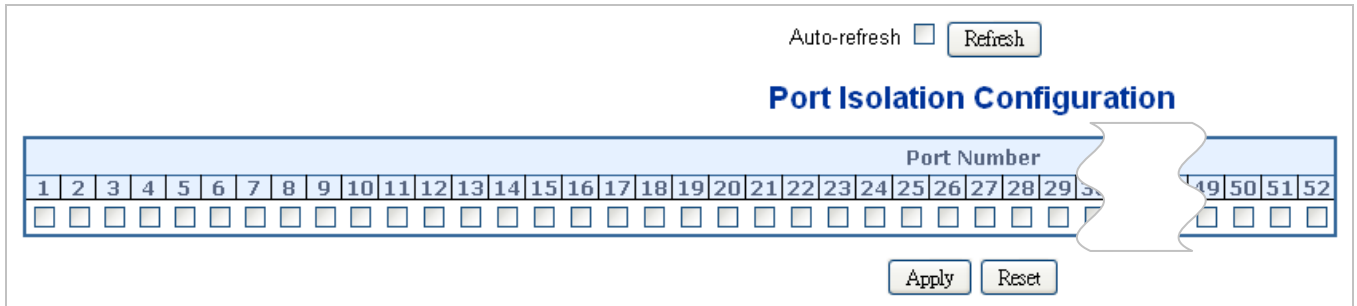


Figure 4-6-6: Port Isolation Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port Members 	<p>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.</p> <p>By default, port isolation is disabled on all ports.</p>

Buttons

Apply: Click to apply 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 VLAN setting example:

- Separate VLAN
- 802.1Q VLAN Trunk
- Port Isolate

4.6.7.1 Two Separate 802.1Q VLANs

The diagram shows how the Managed Switch handle 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 4-6-7](#) appears and [Table 4-6-8](#) describes the port configuration of the Managed Switches.

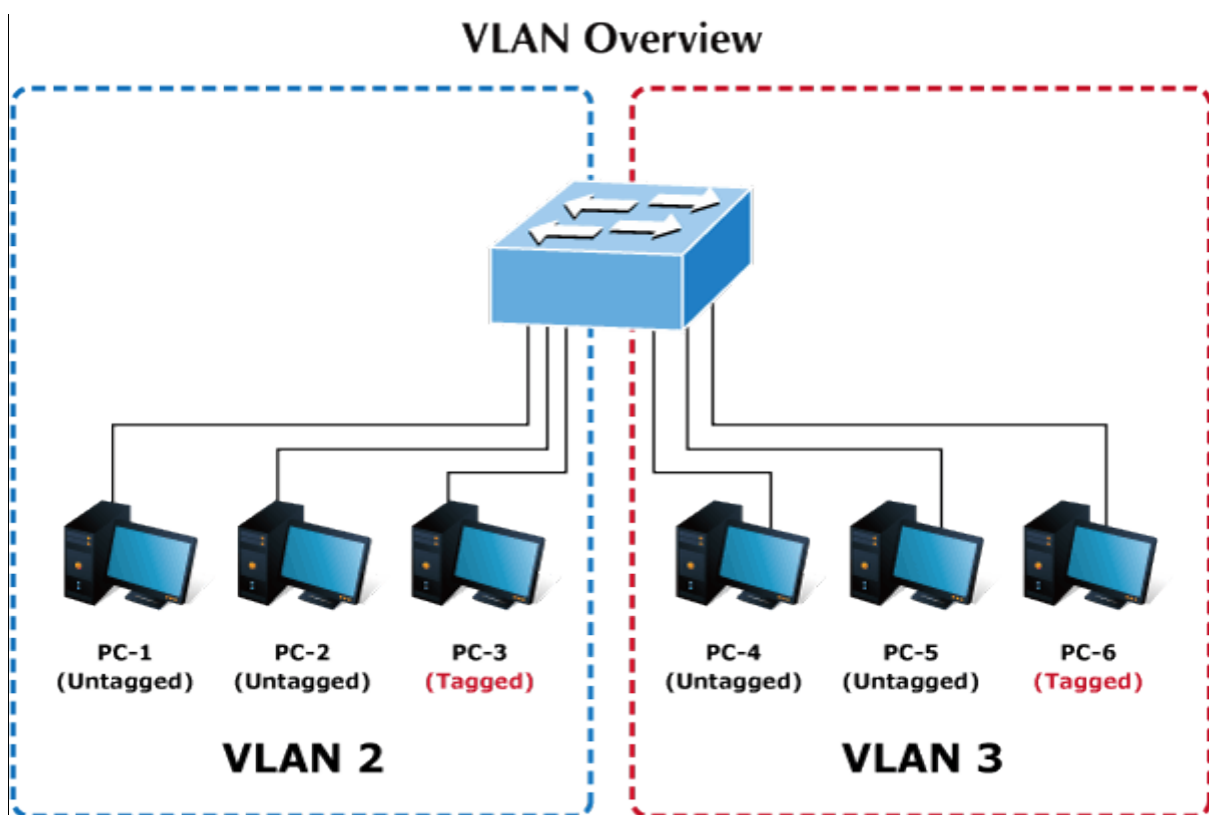


Figure 4-6-7: Two Separate VLANs Diagram

VLAN Group	VID	Untagged Members	Tagged Members
VLAN Group 1	1	Port-7 ~ Port-52	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 is 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 received 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 it 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] transmit a **tagged** packet with **VLAN Tag=2** enters **Port-3**, [PC-1] and [PC-2] will received the packet through **Port-1** and **Port-2**.
6. While the packet leaves **Port-1** and **Port-2**, it will be stripped away it tag becoming an **untagged** packet.

■ **Untagged packet entering VLAN 3**

1. While [PC-4] transmit an **untagged** packet enters **Port-4**, the switch will tag it with a **VLAN Tag=3**. [PC-5] and [PC-6] will received the packet through **Port-5** and **Port-6**.
2. While the packet leaves **Port-5**, it will be stripped away it 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 just set as default VLAN, but only focus on VLAN 2 and VLAN 3 traffic flow

Setup steps

1. Add VLAN Group

Add two VLANs – VLAN 2 and VLAN 3

Type 1-3 in 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 4-6-8: 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-52

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 4-6-9: Change Port VLAN of Port 1~3 to be VLAN2 and Port VLAN of Port 4~6 to be VLAN3

3. Enable VLAN Tag for specific ports

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 4-6-10 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 4-6-10: Check VLAN 2 and 3 Members on VLAN Membership Page

4.6.7.2 VLAN Trucking 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 4-6-11 appears.

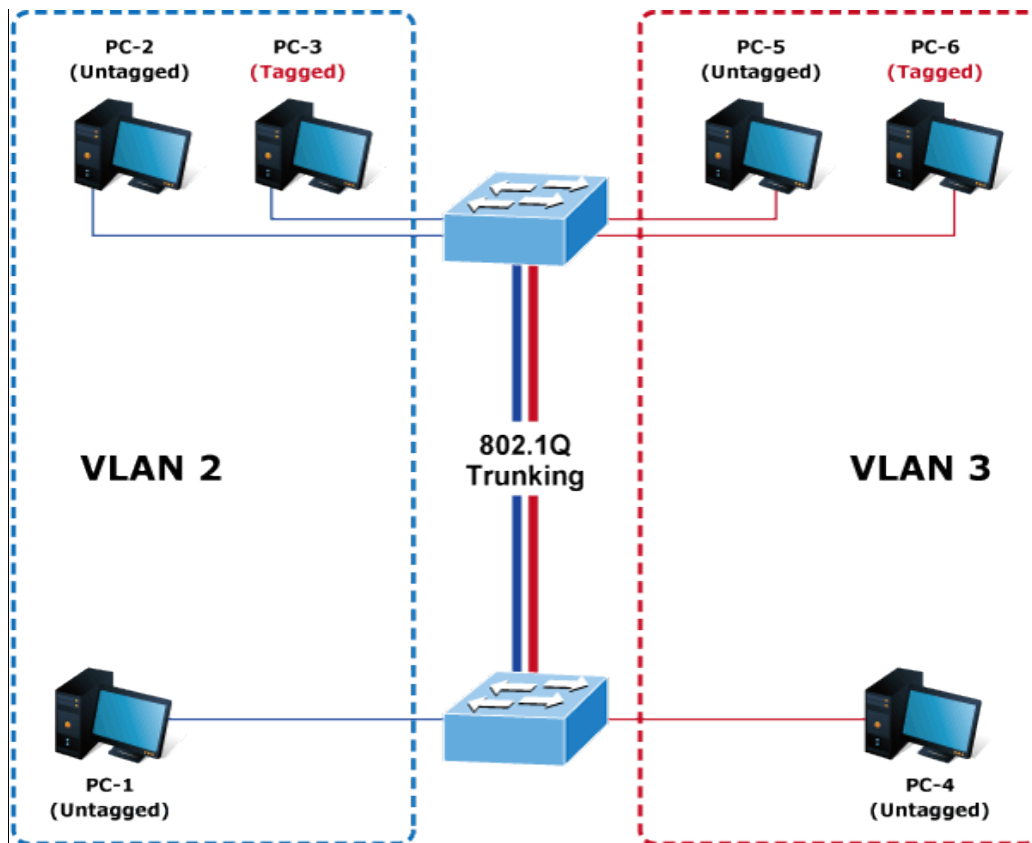


Figure 4-6-11: VLAN Trunking Diagram

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 4-6-12: 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-52

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 4-6-13: 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 4-6-14](#).

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	

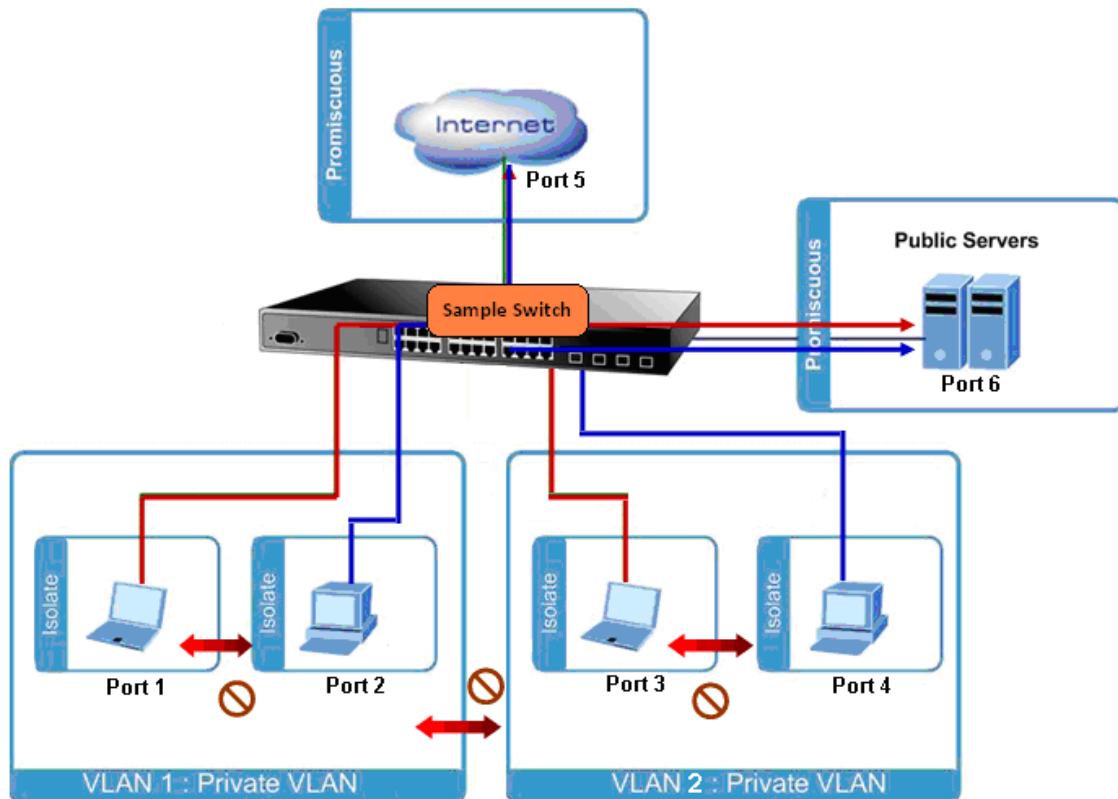
Figure 4-6-14: VLAN Overlap Port Setting & VLAN 1 – The Public Area Member Assign

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.

- 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.

4.6.7.3 Port Isolate

The diagram shows how the Managed Switch handles isolated and promiscuous ports, and the each PC is not able to access the isolated port of each other's PCs. But they all need to access with the same server/AP/Printer. This section will show you how to configure the port for the server – that could be accessed by each isolated port.



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.

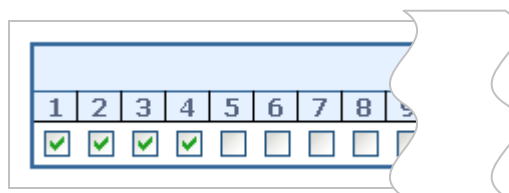


Figure 4-6-17: The Configuration of Isolated and Promiscuous Port

4.6.8 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 4-6-18](#) appears.

Figure 4-6-18: 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.
<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.
<ul style="list-style-type: none"> • Adding a New MAC-based VLAN 	Click "Add New Entry" to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095. The MAC-based VLAN entry is enabled when you click on "Save". A MAC-based VLAN without any port members will be deleted when you click "Save". The "Delete" button can be used to undo the addition of new MAC-based VLANs.

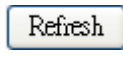
Buttons


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


: Click to apply 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.

: 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.

4.6.9 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 4-6-19](#) appears.

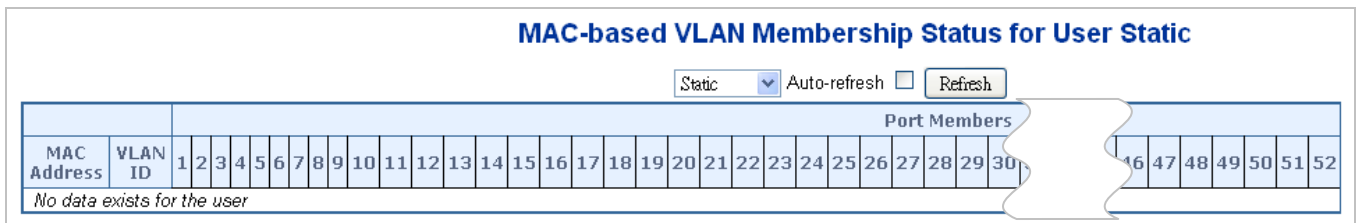


Figure 4-6-19: MAC-based VLAN Membership Configuration for User Static Page Screenshot

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.

4.6.10 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 4-6-20](#) appears.



Figure 4-6-20: 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"> 1. Ethernet 2. LLC 3. 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 selected.</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 preceding Frame Type selection menu.</p> <p>Below is the criteria for three different Frame Types:</p> <ol style="list-style-type: none"> 1. For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff 2. For LLC: Valid value in this case is comprised of two different sub-values. <ol style="list-style-type: none"> a. DSAP: 1-byte long string (0x00-0xff) b. SSAP: 1-byte long string (0x00-0xff) 3. For SNAP: Valid value in this case also is comprised of two different sub-values. <ol style="list-style-type: none"> a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff. b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top

	<p>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.</p> <p>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).</p> <p>Note: special character and underscore(_) are not allowed.</p>
<ul style="list-style-type: none"> • Adding a New Group to VLAN mapping entry 	<p>Click “Add New Entry” to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed.</p> <p>The “Delete” button can be used to undo the addition of new entry.</p>

Buttons

Add New Entry: Click to add a new entry in mapping table.

Apply: Click to apply 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.

4.6.11 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 4-6-21](#) appears.

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

The page includes the following fields:

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

<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • Group Name 	A valid Group Name is a string of almost 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.
<ul style="list-style-type: none"> • VLAN ID 	Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.
<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • Adding a New Group to VLAN mapping entry 	Click "Add New Entry" to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The "Delete" button can be used to undo the addition of new entry.

Buttons

: Click to apply 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

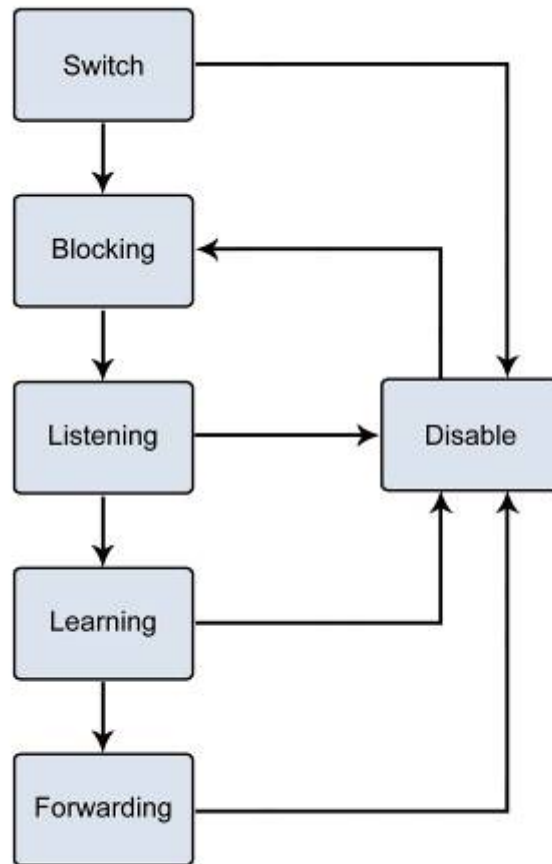



Figure 4-7-1: STP Port State Transitions

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.

 <p>Note</p>	<p>On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges.</p> <p>On the port level, STP sets the Root Port and the Designated Ports.</p>
---	---

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 _ 2 x (Forward Delay - 1 second)

Max. Age _ 2 x (Hello Time + 1 second)

Port Priority – A Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port.

Port Cost – A Port Cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

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.

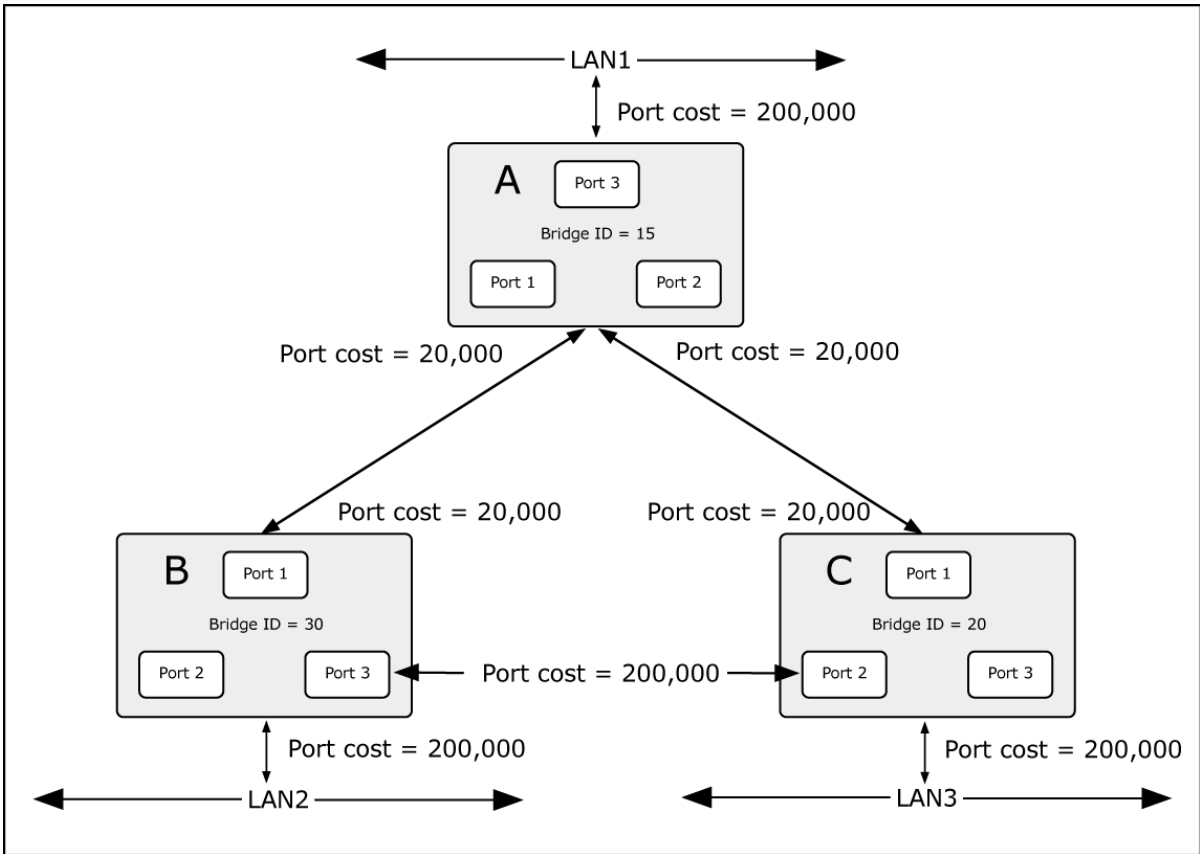


Figure 4-7-2: Before Applying the STA Rules

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

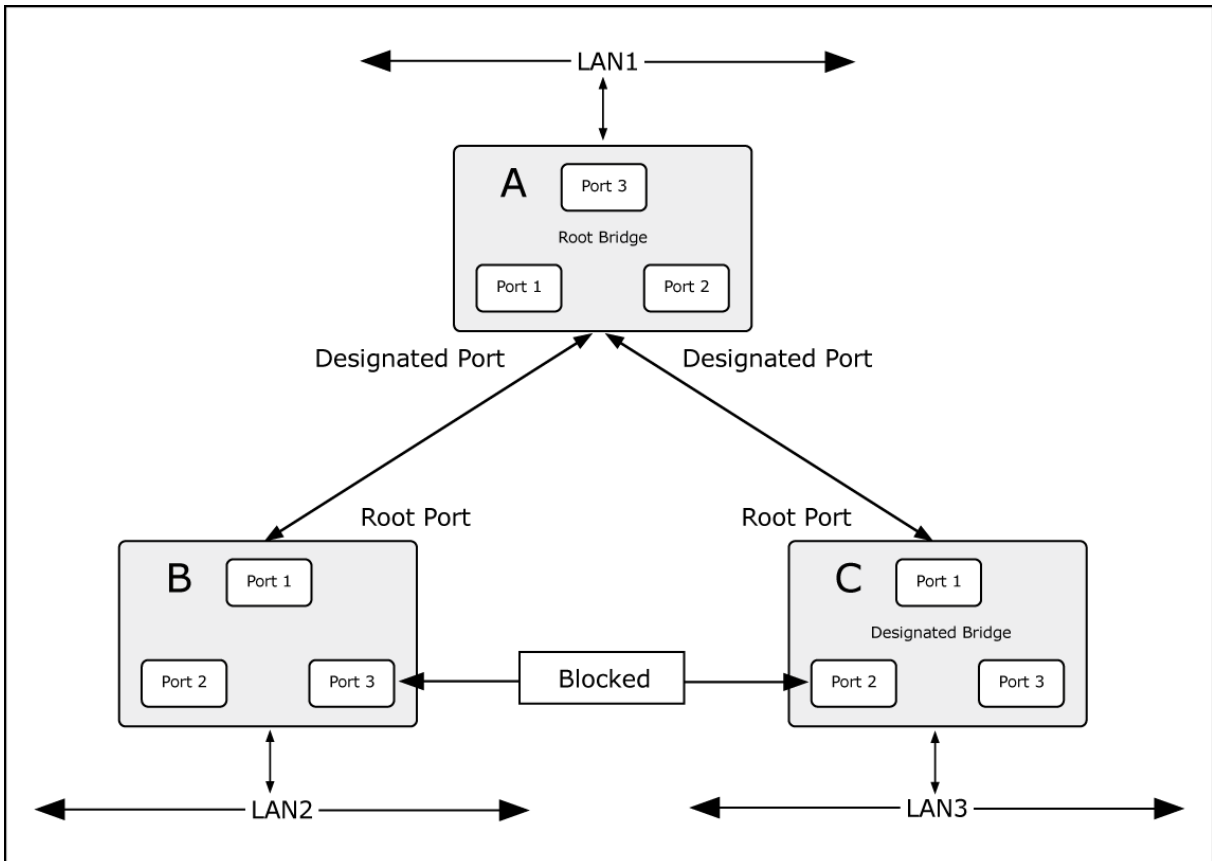


Figure 4-7-3: After Applying the STA Rules

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. 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.

The screenshot displays the 'STP Bridge Configuration' page, which is divided into two main sections: 'Basic Settings' and 'Advanced Settings'. At the bottom, there are 'Apply' and 'Reset' buttons.

STP Bridge Configuration	
Basic Settings	
Protocol Version	MSTP
Bridge Priority	32768
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	

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

The page includes the following fields:

Basic Settings

Object	Description
<ul style="list-style-type: none"> • Protocol Version 	<p>The STP protocol version setting. Valid values are:</p> <ul style="list-style-type: none"> ■ STP (IEEE 802.1D Spanning Tree Protocol) ■ RSTP (IEEE 802.2w Rapid Spanning Tree Protocol) ■ MSTP (IEEE 802.1s Multiple Spanning Tree Protocol)
<ul style="list-style-type: none"> • Bridge Priority 	<p>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.</p> <p>For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.</p>
<ul style="list-style-type: none"> • Forward Delay 	<p>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</p> <ul style="list-style-type: none"> -Default: 15 -Minimum: The higher of 4 or [(Max. Message Age / 2) + 1] -Maximum: 30
<ul style="list-style-type: none"> • Max Age 	<p>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.</p> <ul style="list-style-type: none"> -Default: 20 -Minimum: The higher of 6 or [2 x (Hello Time + 1)]. -Maximum: The lower of 40 or [2 x (Forward Delay - 1)]
<ul style="list-style-type: none"> • Maximum Hop Count 	<p>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.</p>
<ul style="list-style-type: none"> • Transmit Hold Count 	<p>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.</p>

Advanced Settings

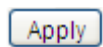
Object	Description
<ul style="list-style-type: none"> • Edge Port BPDU Filtering 	<p>Control whether a port explicitly configured as Edge will transmit and receive BPDUs.</p>
<ul style="list-style-type: none"> • Edge Port BPDU Guard 	<p>Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.</p>

<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • 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).

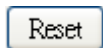


The Managed Switch implements the Rapid Spanning Protocol as the default spanning tree protocol. When selecting “**Compatibles**” mode, the system uses the RSTP (802.1w) to be compatible and to co-work with another STP (802.1D)’s BPDU control packet.

Buttons



: Click to apply 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	80:00-00:30:4F:11:22:55	80:00-00:30:4F:11:22:55	-	0	Steady	-

Auto-refresh [Refresh](#)

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

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • MSTI 	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
<ul style="list-style-type: none"> • Bridge ID 	The Bridge ID of this Bridge instance.
<ul style="list-style-type: none"> • Root ID 	The Bridge ID of the currently elected root bridge.
<ul style="list-style-type: none"> • Root Port 	The switch port currently assigned the <i>root</i> port role.
<ul style="list-style-type: none"> • 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.

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


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.

<ul style="list-style-type: none"> • Path Cost 	<p>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.</p>
<ul style="list-style-type: none"> • Priority 	<p>Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).</p> <p>Default: 128</p> <p>Range: 0-240, in steps of 16</p>
<ul style="list-style-type: none"> • AdminEdge 	<p>Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized).</p>
<ul style="list-style-type: none"> • AutoEdge 	<p>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.</p>
<ul style="list-style-type: none"> • Restricted Role 	<p>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.</p>
<ul style="list-style-type: none"> • Restricted TCN 	<p>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.</p>
<ul style="list-style-type: none"> • BPDUGuard 	<p>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.</p>
<ul style="list-style-type: none"> • Point-to-point 	<p>Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transitions to the forwarding state is faster for point-to-point LANs than for shared media.</p>

Buttons

 : Click to apply 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	Priority
*	<All> ▼
CIST	32768 ▼
MSTI1	32768 ▼
MSTI2	32768 ▼
MSTI3	32768 ▼
MSTI4	32768 ▼
MSTI5	32768 ▼
MSTI6	32768 ▼
MSTI7	32768 ▼


Apply Reset

Figure 4-7-7: MSTI Priority Page Screenshot

The page includes the following fields:

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

Buttons

: Click to apply changes

: 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	9C:F6:1A:7D:55:1b
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	⌵
MSTI2	⌵
MSTI3	⌵
MSTI4	⌵
MSTI5	⌵
MSTI6	⌵
MSTI7	⌵

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 apply 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 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.

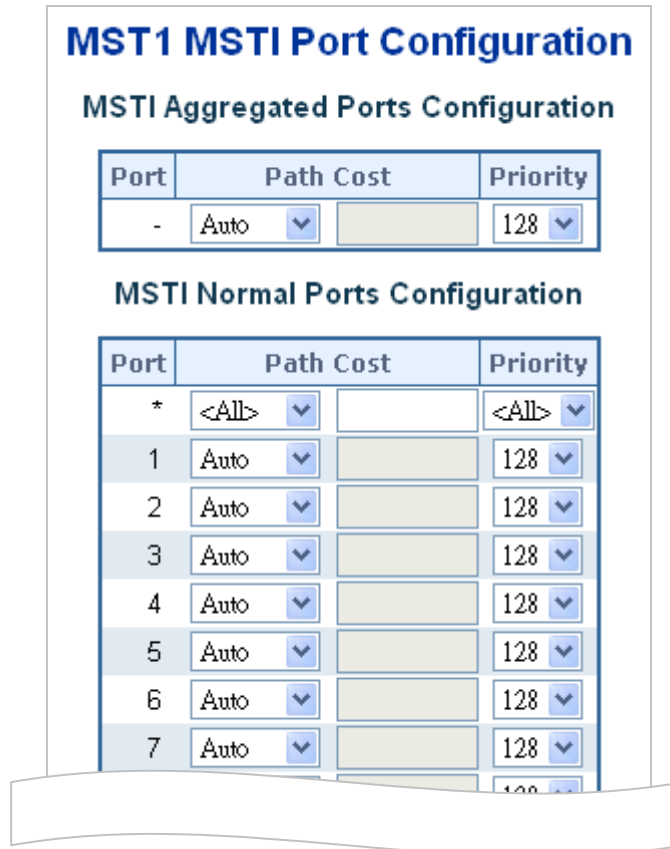


Figure 4-7-10 : MST1 MSTI Port Configuration Page Screenshot

The page includes the following fields:

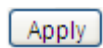
MSTx MSTI Port Configuration

Object	Description
<ul style="list-style-type: none"> • Port 	The switch port number of the corresponding STP CIST (and MSTI) port.
<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • Priority 	Controls the port priority. This can be used to control priority of ports having identical port cost.

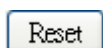
Buttons



: Click to set MSTx configuration



: Click to apply 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.

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	-

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

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	The switch port number of the logical STP port.
<ul style="list-style-type: none"> • CIST Role 	The current STP port role of the ICST port. The port role can be one of the following values: <ul style="list-style-type: none"> ■ AlternatePort ■ BackupPort ■ RootPort ■ DesignatedPort ■ Disable
<ul style="list-style-type: none"> • CIST State 	The current STP port state of the CIST port . The port state can be one of the following values: <ul style="list-style-type: none"> ■ Disabled ■ Learning ■ Forwarding
<ul style="list-style-type: none"> • Uptime 	The time since the bridge port was last initialized.

Buttons

Click to refresh the page immediately.

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

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
<i>No ports enabled</i>										
Auto-refresh <input type="checkbox"/> <input type="button" value="Refresh"/> <input type="button" value="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 Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

: Clears the counters for all ports.

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.

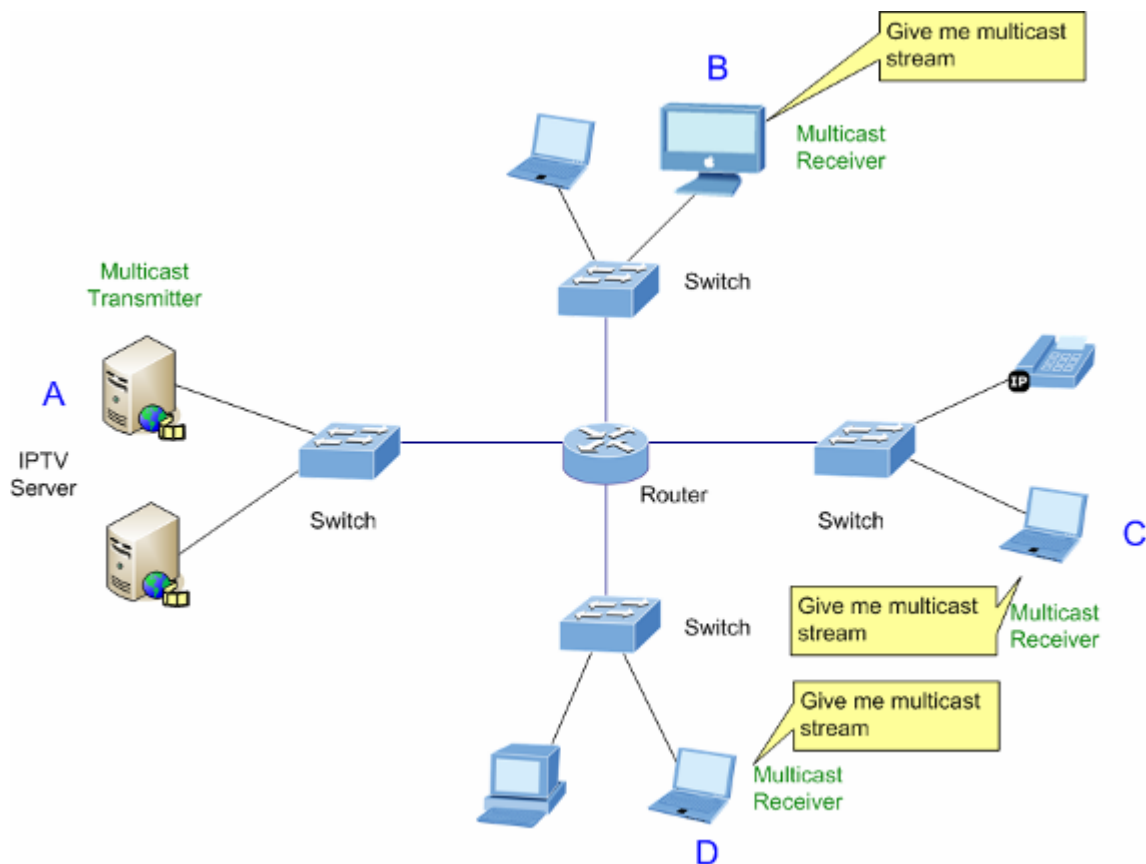


Figure 4-8-1: Multicast Service

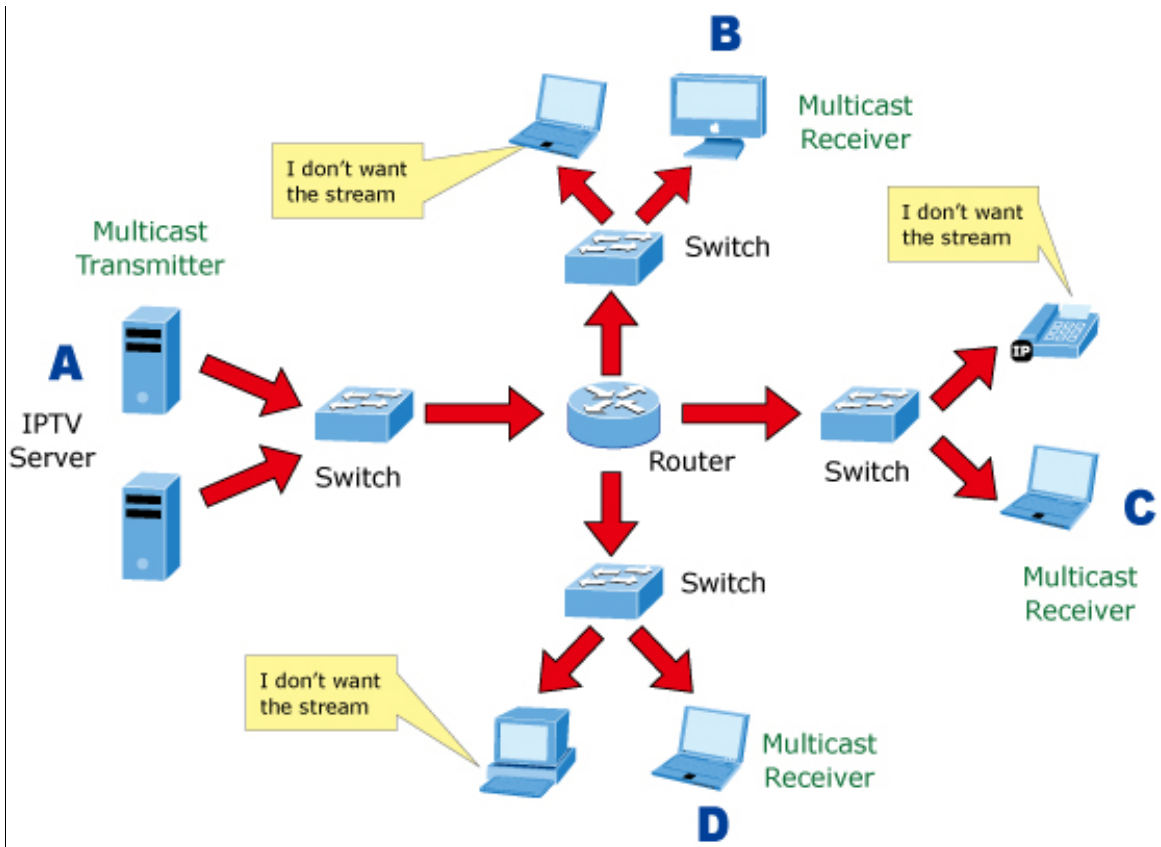


Figure 4-8-2: Multicast Flooding

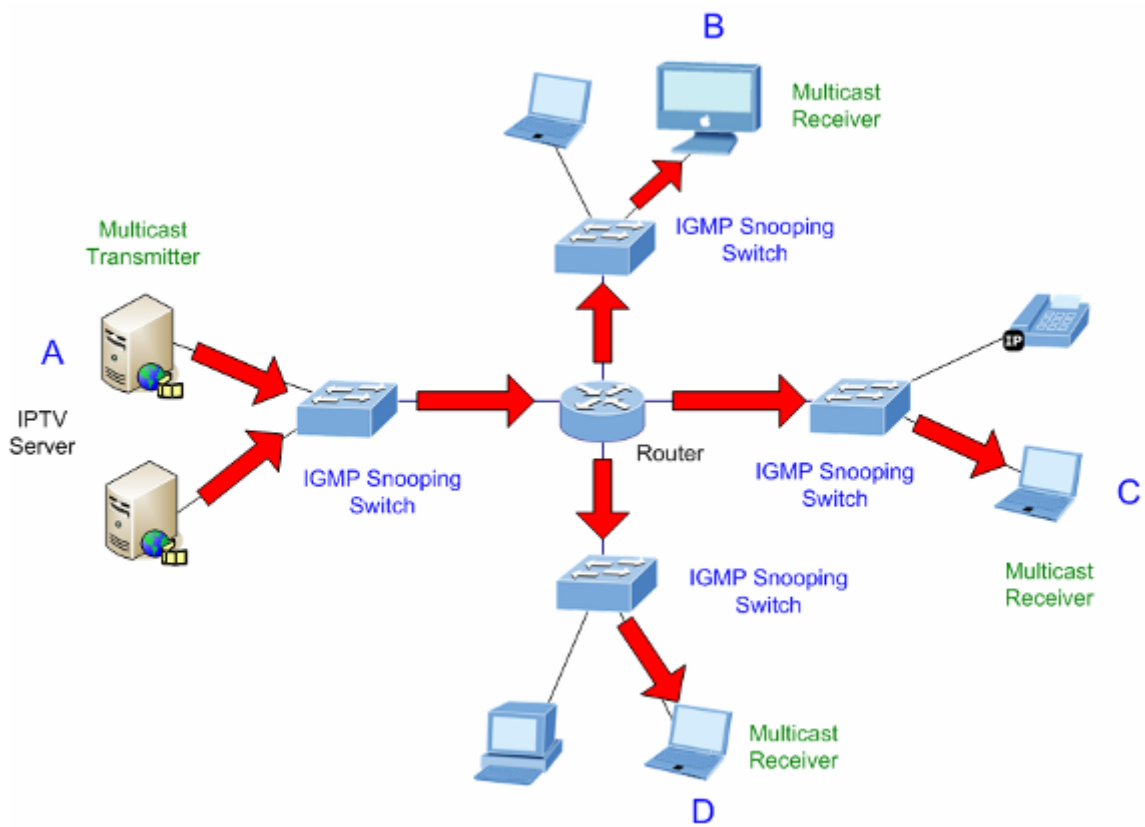


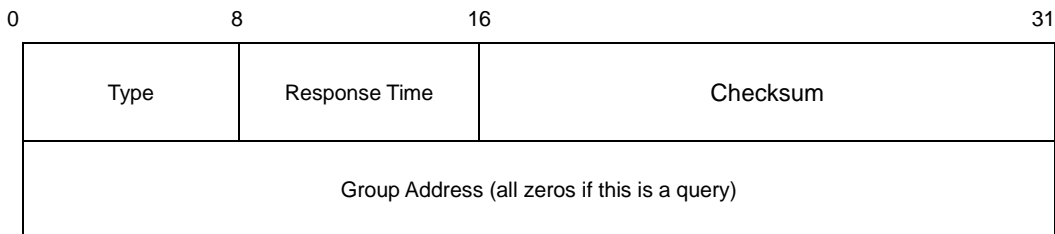
Figure 4-8-3: IGMP Snooping Multicast Stream Control

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



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:

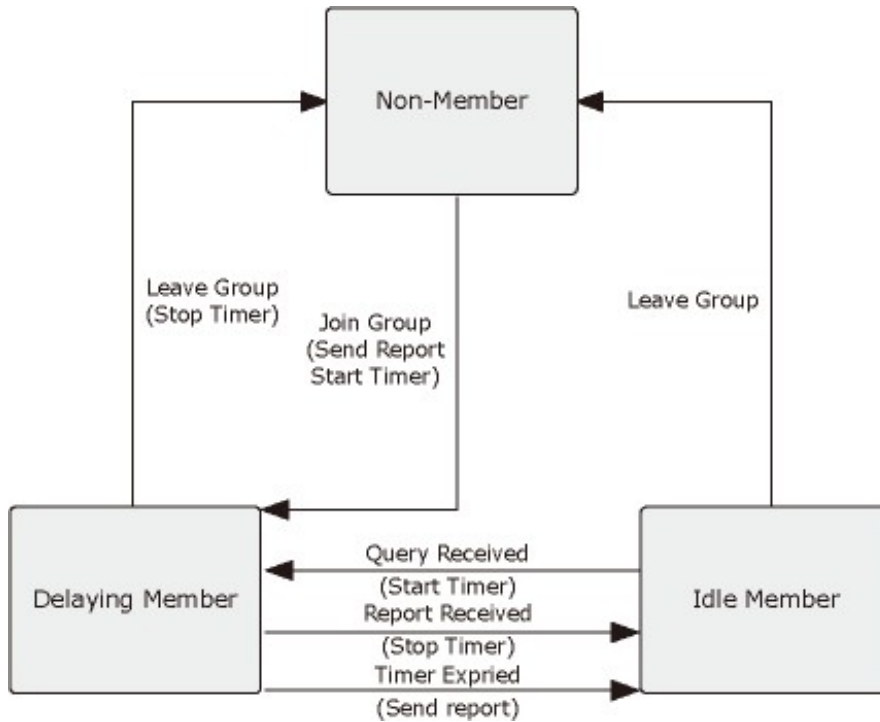



Figure 4-8-4: IGMP State Transitions

■ **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.

 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.

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 	<p>Enable/Disable the Global IPMC Profile.</p> <p>System starts to do filtering based on profile settings only when the global profile mode is enabled.</p>
<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"> • Profile Name 	<p>The name used for indexing the profile 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"> • Profile Description 	<p>Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile.</p> <p>No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.</p>
<ul style="list-style-type: none"> • Rule 	<p>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:</p> <p>: List the rules associated with the designated profile.</p> <p>: Adjust the rules associated with the designated profile.</p>

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.

IPMC Profile Address Configuration

Refresh | << | >>

Navigate Address Entry Setting in IPMC Profile by entries per page.

Delete	Entry Name	Start Address	End Address
Delete			

Add New Address (Range) Entry

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

Buttons

Add New Address (Range) Entry: Click to add new address range. Specify the name and configure the addresses. Click "Save".

Apply : Click to apply changes

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

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

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

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

4.8.4 IGMP Snooping Configuration

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

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


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	Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always

	active in spite of this setting.
• IGMP SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
• Leave Proxy 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 to be flooded by uplinking switch through the port that is 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

: Click to apply changes

: 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.

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


The page includes the following fields:


Object	Description
<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"> • VLAN ID 	The VLAN ID of the entry.
<ul style="list-style-type: none"> • IGMP Snooping Enable 	Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected.
<ul style="list-style-type: none"> • Querier Election 	Enable the IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
<ul style="list-style-type: none"> • Querier Address 	<p>Define the IPv4 address as source address used in IP header for IGMP Querier election.</p> <ul style="list-style-type: none"> ■ When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. ■ When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. <p>By default, this value will be 192.0.2.1</p>
<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 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 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.

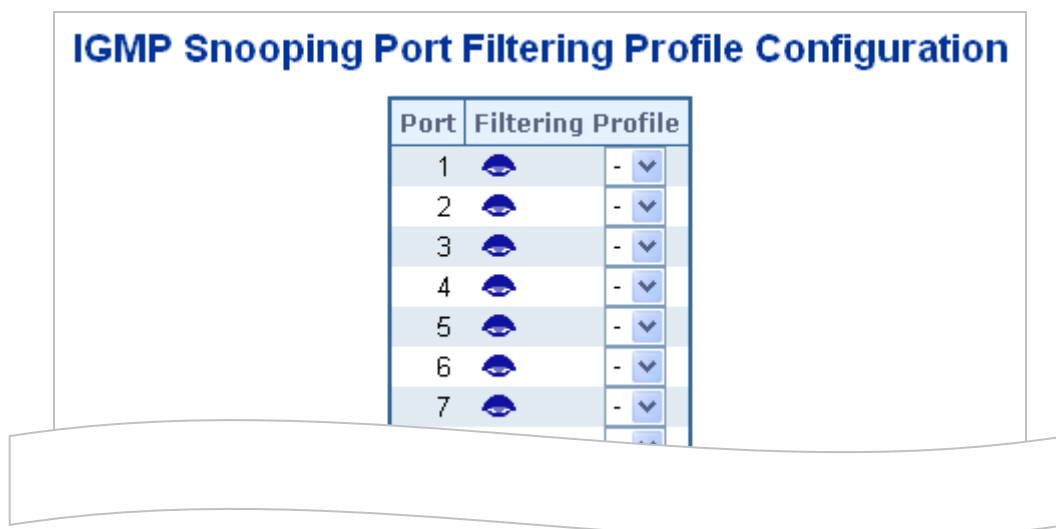


Figure 4-8-9: IGMP Snooping Port Filtering Profile Configuration Page Screenshot

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

Apply: Click to apply changes

Reset: 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.

Auto-refresh <input type="checkbox"/>		<input type="button" value="Refresh"/>	<input type="button" value="Clear"/>						
IGMP Snooping Status									
Statistics									
VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
Router Port									
Port	Status								
1	-								
2	-								
3	-								
4	-								
5	-								
6	-								
7	-								
8	-								
9	-								

Figure 4-8-10: IGMP 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	Show the Querier status is "ACTIVE" or "IDLE".
• 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.
• V3 Reports Received	The number of Received V3 Reports.
• V2 Leave Received	The number of Received V2 Leave.
• Router Port	Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.
• Port	Switch port number.
• Status	Indicate whether specific port is a router port or not.

Buttons

: 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.

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.

: 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.

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 ▼
9	Auto ▼	<input type="checkbox"/>	Unlimited ▼

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 , Force , default compatibility value is Auto.
• Fast Leave	Enable the fast leave on the port.
• Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

: 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.

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 .
• QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.
• QRI	Query Response Interval. The 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).
• LLQI (LMQI for IGMP)	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).
• URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons


: 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.

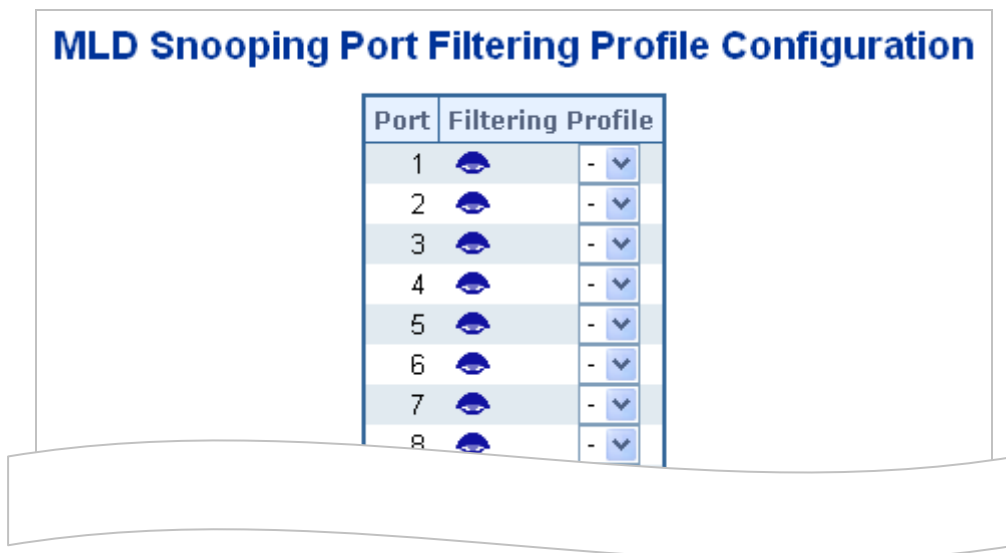


Figure 4-8-15: MLD Snooping Port Group Filtering Configuration Page Screenshot

The page includes the following fields:

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

Buttons

Apply: Click to apply changes

Reset: 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.

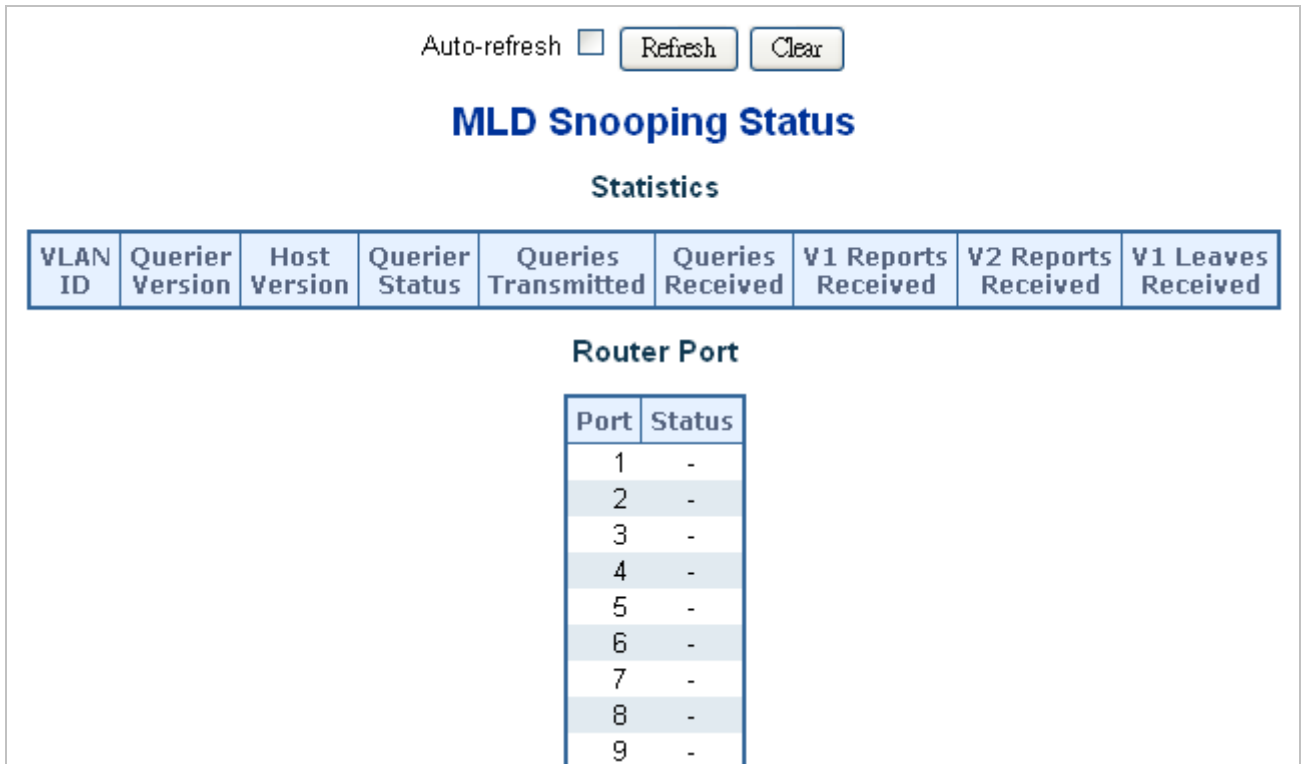


Figure 4-8-16: MLD Snooping Status Page Screenshot

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	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. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.

• Port	Switch port number.
• Status	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 Information screen in [Figure 4-8-17](#) appears.



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.

: 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.

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.

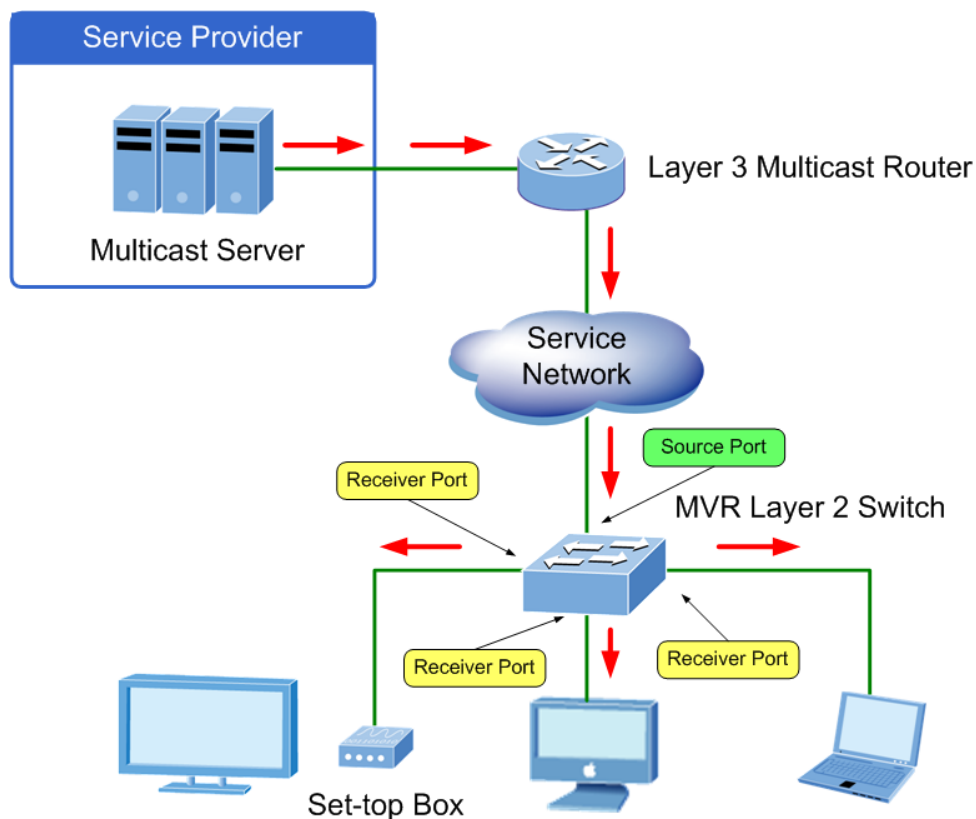
Updates the table, starting with the entry after the last entry currently displayed.

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 ▼

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>
<ul style="list-style-type: none"> • Delete 	<p>Check to delete the entry. The designated entry will be deleted during the next save.</p>
<ul style="list-style-type: none"> • MVR VID 	<p>Specify the Multicast VLAN ID.</p> <p>Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.</p>
<ul style="list-style-type: none"> • MVR Name 	<p>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</p>

	<p>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.</p>
<ul style="list-style-type: none"> • IGMP Address 	<p>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).</p> <p>When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.</p> <p>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.</p>
<ul style="list-style-type: none"> • Mode 	<p>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.</p>
<ul style="list-style-type: none"> • Tagging 	<p>Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.</p>
<ul style="list-style-type: none"> • Priority 	<p>Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.</p>
<ul style="list-style-type: none"> • LLQI 	<p>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.</p>
<ul style="list-style-type: none"> • Interface Channel Setting 	<p>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.</p>
<ul style="list-style-type: none"> • Port 	<p>The logical port for the settings.</p>
<ul style="list-style-type: none"> • Port Role 	<p>Configure an MVR port of the designated MVR VLAN as one of the following roles.</p> <ul style="list-style-type: none"> ■ Inactive: The designated port does not participate MVR operations. ■ Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. ■ Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages. <p>Be 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>

	The default Role is Inactive.
• Immediate Leave	Enable the fast leave on the port.

Buttons

- Add New MVR VLAN**: Click to add new MVR VLAN. Specify the VID 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.

4.8.17 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"/> Refresh 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

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

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.

: 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.



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 Understanding 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.

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	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

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.
• Enable	Controls whether the policer is enabled on this switch port.
• Rate	Controls the rate for the policer. 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 ". The default value is 500 .
• Unit	Controls the unit of measure for the policer rate as kbps , Mbps , fps or kfps . The default value is " kbps ".
• Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

: Click to apply changes

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

4.9.3 Port Classification

This page allows you to configure the basic QoS Ingress Classification settings for all switch ports. The Port Classification screen in [Figure 4-9-2](#) appears.

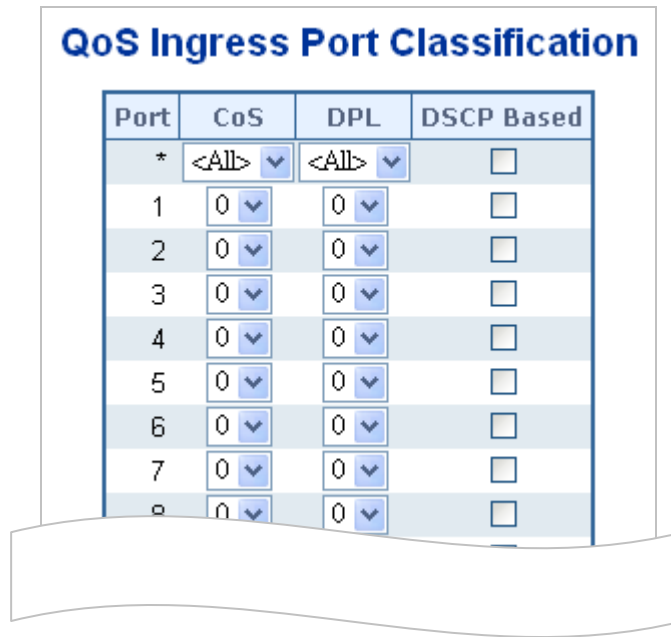


Figure 4-9-2 : QoS Ingress Port Classification Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	The port number for which the configuration below applies.
<ul style="list-style-type: none"> • CoS 	<p>Controls the default class of service.</p> <p>All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.</p> <p>If the port is VLAN aware and the frame is tagged, then the frame is classified to a CoS that is based on the PCP value in the tag as shown below. Otherwise the frame is classified to the default CoS.</p> <p style="text-align: center;">PCP value: 0 1 2 3 4 5 6 7</p> <p style="text-align: center;">CoS value: 1 0 2 3 4 5 6 7</p> <p>The classified CoS can be overruled by a QCL entry. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.</p> <p>Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.</p>
<ul style="list-style-type: none"> • DPL 	<p>Controls the default drop precedence level.</p> <p>All frames are classified to a drop precedence level.</p> <p>If the port is VLAN aware and the frame is tagged, then the frame is classified to a DPL that is equal to the DEI value in the tag. Otherwise the frame is classified</p>

	to the default DPL. The classified DPL can be overruled by a QCL entry
• DSCP Based	Click to Enable DSCP Based QoS Ingress Port Classification.

Buttons



: Click to apply changes



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

4.9.4 Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports. The Port Scheduler screen in [Figure 4-9-3](#) appears.

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

Figure 4-9-3: QoS Egress Port Schedule 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 schedulers. For more detail, please refer to chapter 4.9.5.1.
• Mode	Shows the scheduling mode for this port.
• Q0 ~ Q5	Shows the weight for this queue and port.

4.9.5 Port Shaping

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

QoS Egress Port Shapers										
Port	Shapers								Port	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7		
1	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

Figure 4-9-4: QoS Egress Port Shapers 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 the shapers.</p> <p>For more details, please refer to chapter 4.9.5.1.</p>
<ul style="list-style-type: none"> Q0 -Q7 	Shows "disabled" or actual queue shaper rate, e.g., "800 Mbps".
<ul style="list-style-type: none"> Port 	Shows "disabled" or actual port shaper rate, e.g., "800 Mbps".

4.9.5.1 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 4-9-5](#) appears.

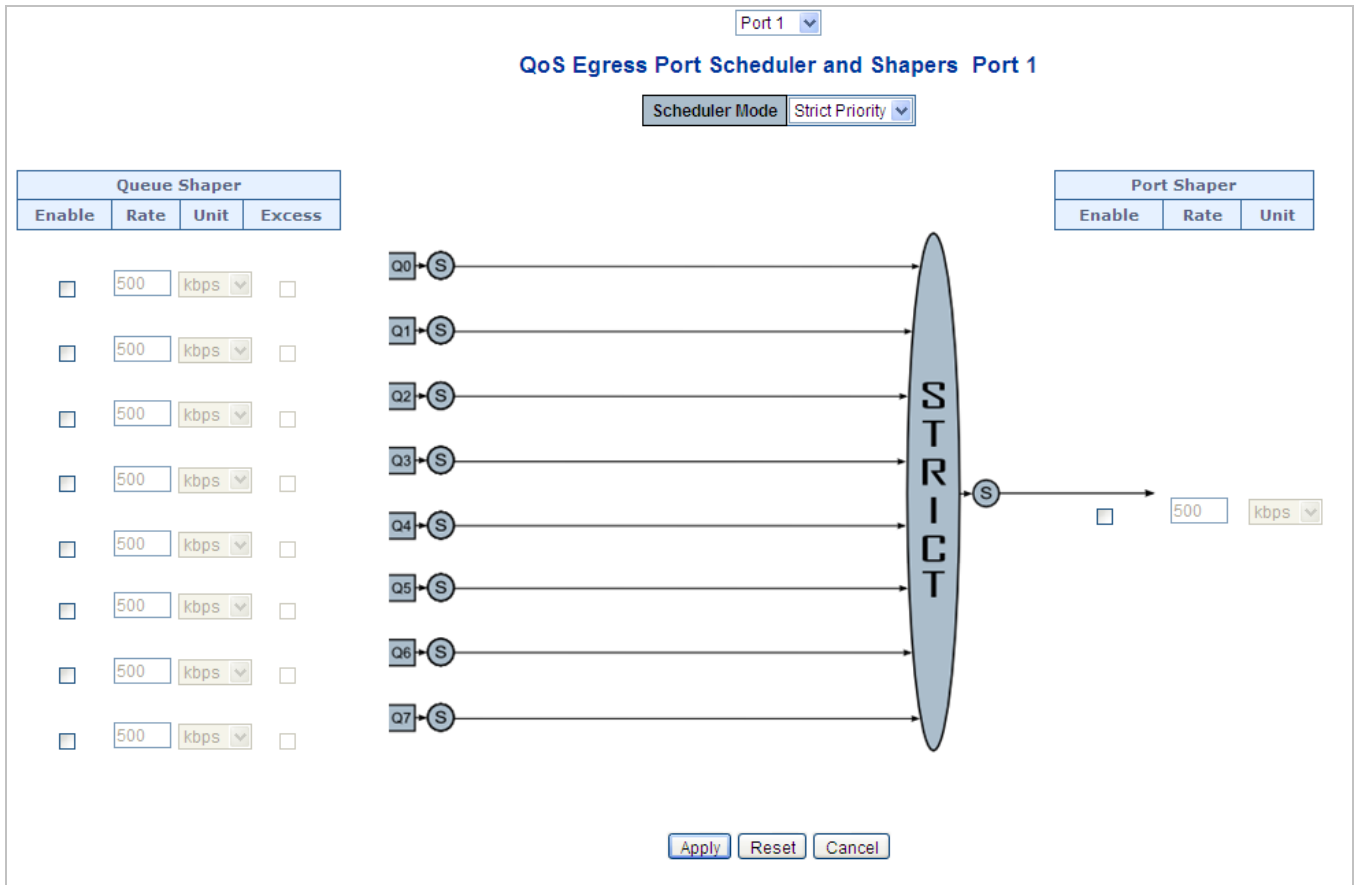


Figure 4-9-5: QoS Egress Port Schedule and Shapers Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Schedule Mode 	Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
<ul style="list-style-type: none"> • Queue Shaper Enable 	Controls whether the queue shaper is enabled for this queue on this switch port.
<ul style="list-style-type: none"> • Queue Shaper Rate 	Controls the rate for the queue shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps". The default value is 500 .
<ul style="list-style-type: none"> • Queue Shaper Unit 	Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps" . The default value is "kbps".
<ul style="list-style-type: none"> • Queue Shaper Excess 	Controls whether the queue is allowed to use excess bandwidth.
<ul style="list-style-type: none"> • Queue Scheduler 	Controls the weight for this queue.

Weight	This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to " Weighted ". The default value is " 17 ".
• 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. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps". The default value is 500.
• Port Shaper Unit	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

: Click to apply 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.

4.9.6 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 4-9-6](#) appears.

The screenshot shows a page titled "QoS Egress Port Tag Remarking" with a table containing the following data:

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified

Figure 4-9-6: 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 4-9-7](#) appears.

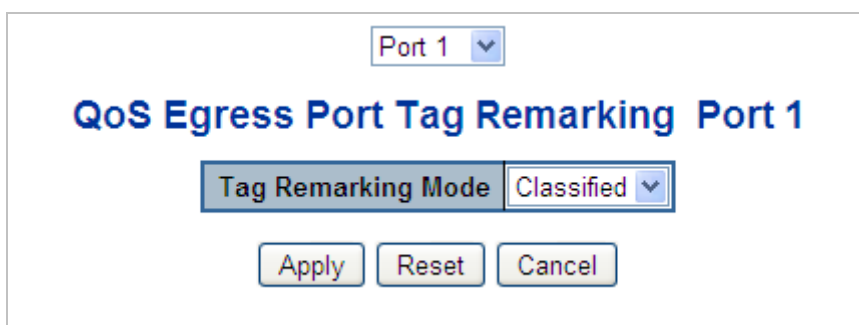



Figure 4-9-7: QoS Egress Port Tag Remarking Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • 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 	<p>Controls the default PCP and DEI values used when the mode is set to Default.</p>
<ul style="list-style-type: none"> • (QoS class, DP level) to (PCP, DEI) Mapping 	<p>Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.</p>

Buttons

: Click to apply changes

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

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 4-9-8](#) appears.

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 ▼


Figure 4-9-8: QoS Port DSCP Configuration Page Screenshot


The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
<ul style="list-style-type: none"> • Ingress 	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: <ul style="list-style-type: none"> ■ Translate ■ Classify
<ul style="list-style-type: none"> • Translate 	To Enable the Ingress Translation click the checkbox.
<ul style="list-style-type: none"> • Classify 	Classification for a port have 4 different values. <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.
<ul style="list-style-type: none"> • Egress 	Port Egress Rewriting can be one of - <ul style="list-style-type: none"> ■ Disable: No Egress rewrite. ■ Enable: Rewrite enable without remapped. ■ Remap DP Unaware: DSCP from analyzer is remapped and frame is

	<p>remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table.</p> <ul style="list-style-type: none"> ■ 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 apply 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 4-9-9](#) appears.

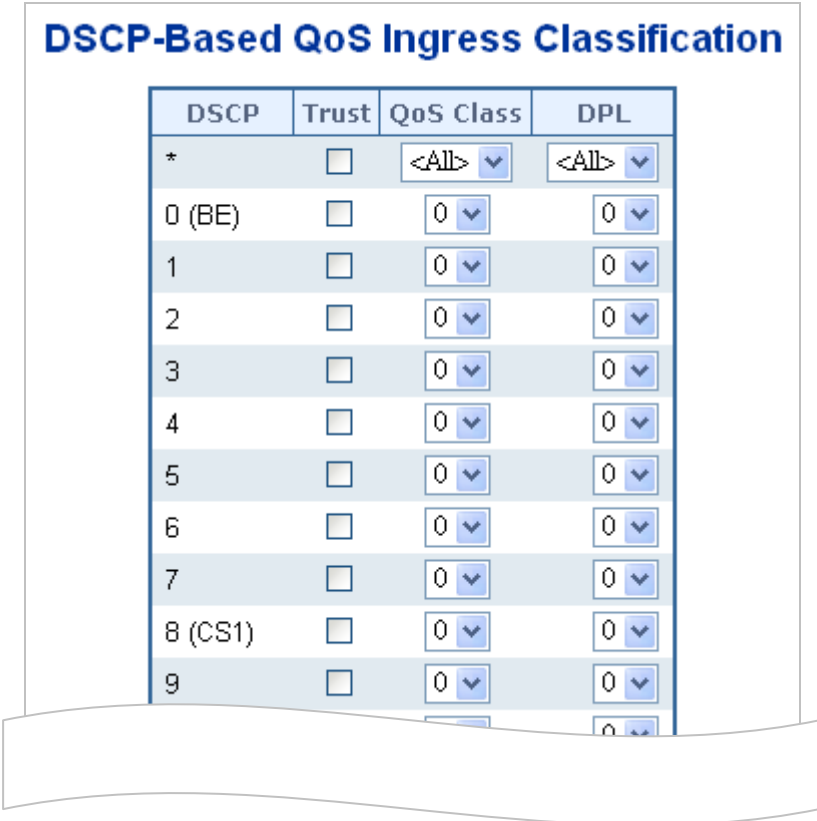


Figure 4-9-9: DSCP-based QoS Ingress Classification Page Screenshot

The page includes the following fields:

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

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 4-9-10](#) appears.

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 ▾
			10 (AF11) ▾

Figure 4-9-10: DSCP Translation Page Screenshot

The page includes the following fields:

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

• DSCP	Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
• Ingress	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation – <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	There is following configurable parameter for Egress side - <ul style="list-style-type: none"> ■ Remap
• Remap DP	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Buttons

Apply: Click to apply changes

Reset: 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.

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) ▼

Figure 4-9-11: DSCP Classification Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • QoS Class 	Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to followed parameters.
<ul style="list-style-type: none"> • DPL 	Actual Drop Precedence Level.
<ul style="list-style-type: none"> • 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.

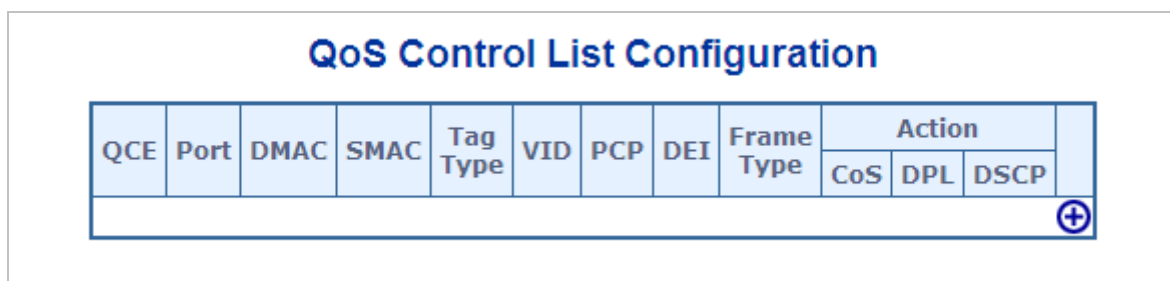








Figure 4-9-12: QoS Control List Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • QCE# 	Indicates the index of QCE.
<ul style="list-style-type: none"> • Port 	Indicates the list of ports configured with the QCE.
<ul style="list-style-type: none"> • DMAC 	Specify the type of Destination MAC addresses for incoming frame. Possible values are: <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.

	<ul style="list-style-type: none"> ■ Broadcast: Only Broadcast MAC addresses are allowed. The default value is 'Any'.
• SMAC	Displays the OUI field of Source MAC address, i.e. first three octet (byte) of MAC address.
• Tag Type	<p>Indicates tag type. Possible values are:</p> <ul style="list-style-type: none"> ■ Any: Match tagged and untagged frames. ■ Untagged: Match untagged frames. ■ Tagged: Match tagged frames. <p>C-Tagged: Match C-tagged frames. S-Tagged: Match S-tagged frames. 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'.
• 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.
• 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. ■ DPL: Classified Drop Precedence Level. ■ DSCP: Classified DSCP value.
• 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.

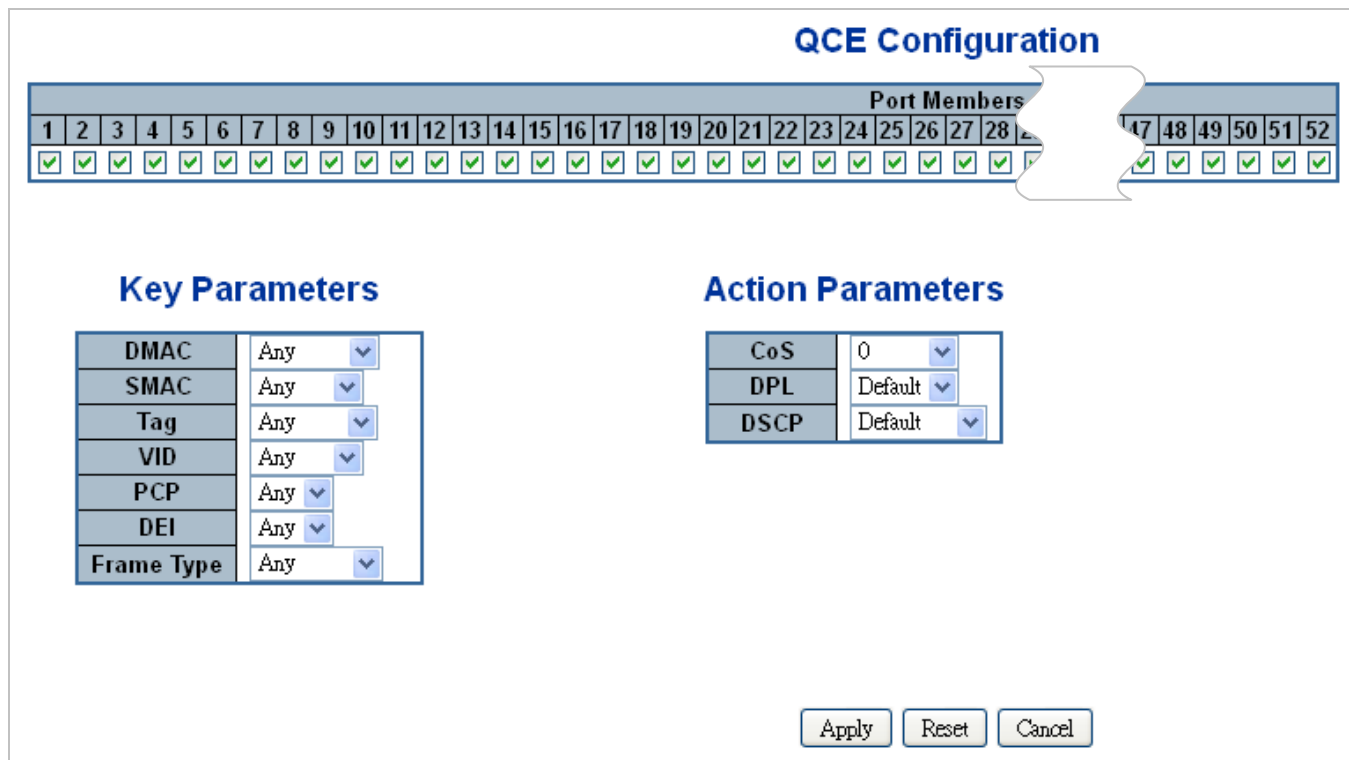


Figure 4-9-13: QCE Configuration Page Screenshot

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 are described as below:</p> <ul style="list-style-type: none"> ■ DMAC Type Destination MAC type: possible values are unicast(UC), multicast(MC), broadcast(BC) or 'Any' ■ SMAC Source MAC address: 24 MS bits (OUI) or 'Any' ■ Tag Value of Tag field can be 'Any', 'Untag' or 'Tag' ■ VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs ■ PCP Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or 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' ■ Frame Type Frame Type can have any of the following values <ol style="list-style-type: none"> 1. Any 2. Ethernet

	<p>3. LLC</p> <p>4. SNAP</p> <p>5. IPv4</p> <p>6. IPv6</p> <p>Note: all frame types are explained below.</p>
• Any	Allow all types of frames.
• EtherType	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> <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>
• Action Parameters	Class QoS class: (0-7) or 'Default'.

	<p>DPL Valid Drop Precedence Level can be (0-3) or 'Default'.</p> <p>DSCP Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.</p> <p>'Default' means that the default classified value is not modified by this QCE.</p>
--	--

Buttons

Apply: Click to apply changes

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

Cancel: Return to the previous page without saving the configuration change

4.9.12 QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is **256** on each switch. The QoS Control List Status screen in [Figure 4-9-14](#) appears.

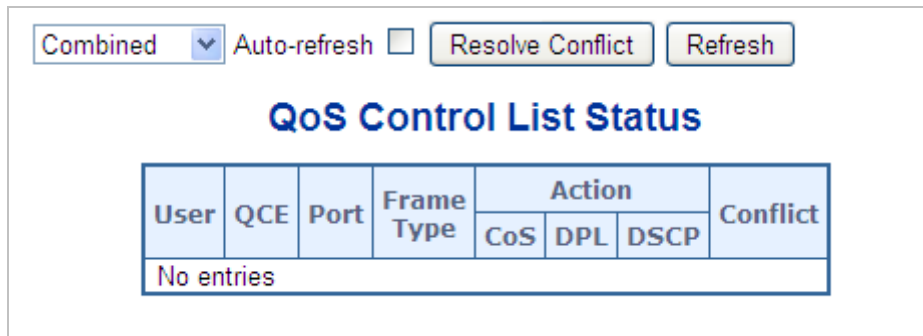


Figure 4-9-14: QoS Control List Status Page Screenshot

The page includes the following fields:

Object	Description
• User	Indicates the QCL user.
• QCE#	Indicates the index of QCE.
• Port	Indicates the list of ports configured with the 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 types. ■ Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. ■ LLC: Only (LLC) frames are allowed.

	<ul style="list-style-type: none"> ■ SNAP: Only (SNAP) frames are allowed. ■ IPv4: The QCE will match only IPV4 frames. ■ IPv6: The QCE will match only IPV6 frames.
<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • Conflict 	<p>Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'.</p> <p>Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' 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 the conflict status for any QCL entry is 'yes'.

: Click to refresh the page.

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 ▾

Figure 4-9-15: Storm Control Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Port	The port number for which the configuration below applies.
• Enable	Controls whether the storm control is enabled on this switch port.
• Rate	Controls the rate for the storm control. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-13200 when the "Unit" is "Mbps" or "kfps".
• Unit	Controls the unit of measure for the storm control rate as kbps, Mbps, fps or kfps . The default value is "kbps".

Buttons

: Click to apply changes

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

4.9.14 WRED

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 WRED screen in [Figure 4-9-16](#) appears.

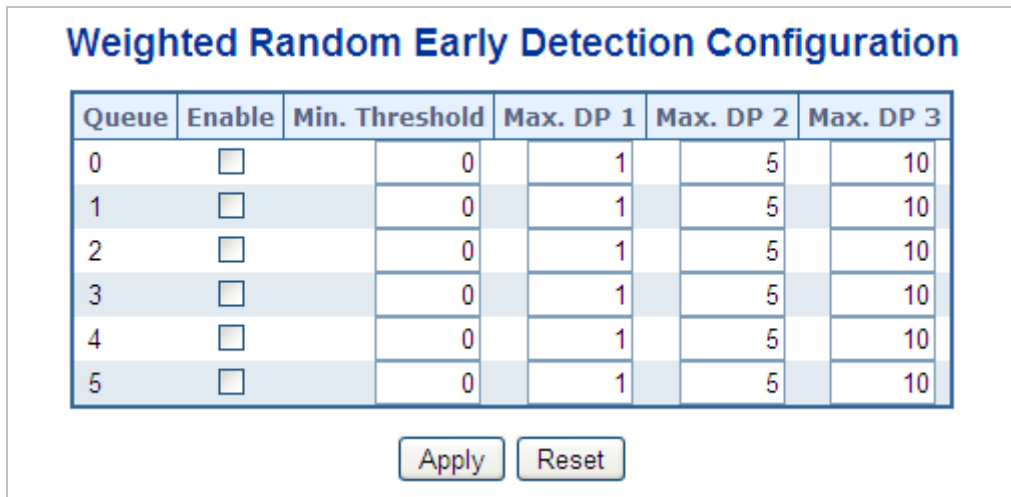


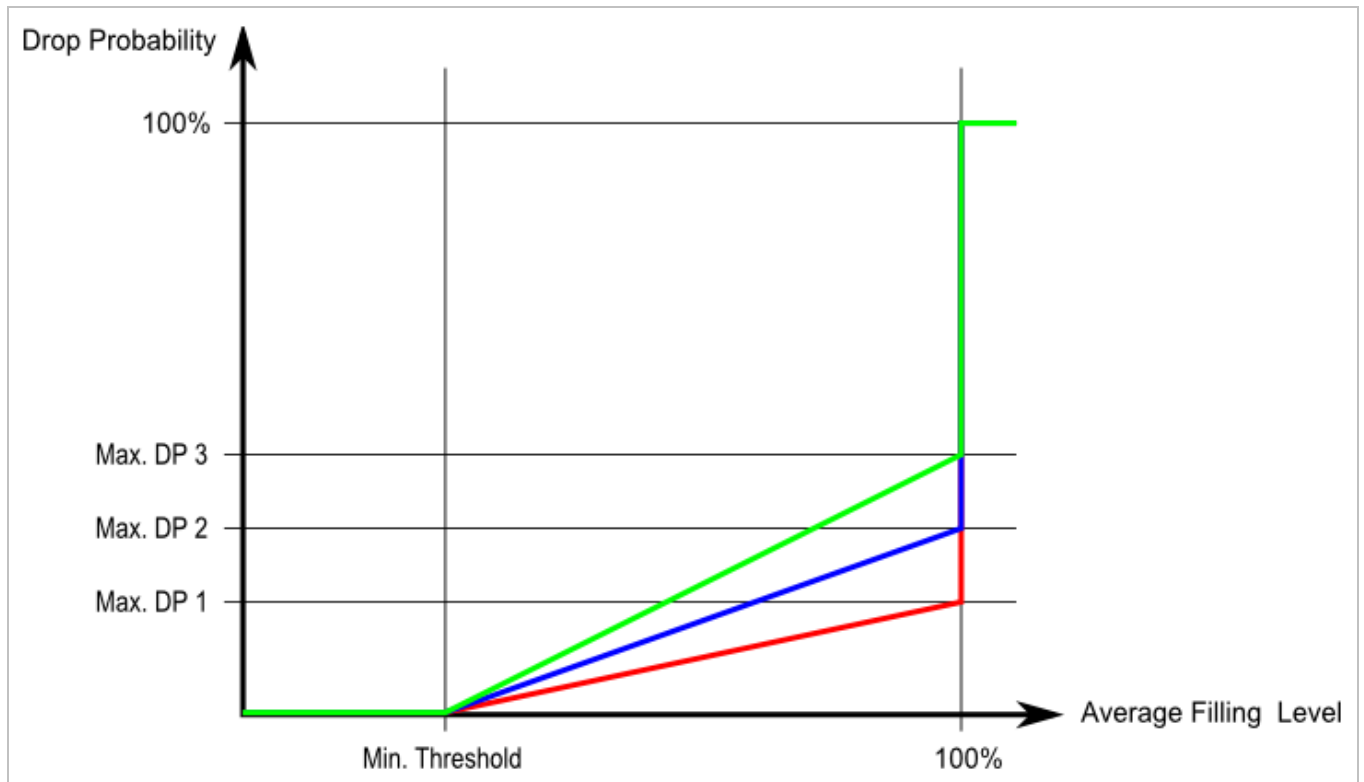
Figure 4-9-16 WRED Page Screenshot

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. DP 1	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.

RED Drop Probability Function

The following illustration shows the drop probability function with associated parameters.



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).

Buttons

: Click to apply 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.

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7		
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	
1	8016	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7808	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

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

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.

4.9.16 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 <input type="button" value="v"/>		
VLAN ID	1000 <input type="button" value="v"/>		
Aging Time	86400 <input type="button" value="v"/>	seconds	
Traffic Class	7 (High) <input type="button" value="v"/>		

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<All> <input type="button" value="v"/>	<All> <input type="button" value="v"/>	<All> <input type="button" value="v"/>
1	Disabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	OUI <input type="button" value="v"/>
2	Disabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	OUI <input type="button" value="v"/>
3	Disabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	OUI <input type="button" value="v"/>
4	Disabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	OUI <input type="button" value="v"/>
5	Disabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	OUI <input type="button" value="v"/>
6	Disabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	OUI <input type="button" value="v"/>
7	Disabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	OUI <input type="button" value="v"/>
8	Disabled <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	OUI <input type="button" value="v"/>

Figure 4-9-18: Voice VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> 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.</p> <p>The allowed range is 1 to 4095.</p>
<ul style="list-style-type: none"> Aging 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.</p> <p>The actual age time will be situated in the [age_time; 2 * age_time] interval.</p>

<ul style="list-style-type: none"> • Traffic Class 	<p>Indicates the Voice VLAN traffic class. All traffic on Voice VLAN will apply this class.</p>
<ul style="list-style-type: none"> • Mode 	<p>Indicates the Voice VLAN port mode.</p> <p>When the port mode isn't equal disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering.</p> <p>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 to the specific port and configures the Voice VLAN members automatically. ■ Forced: Force join to Voice VLAN.
<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • 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. ■ LLDP: Detect telephony device by LLDP. ■ Both: Both OUI and LLDP.

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.

Delete	Telephony OUI	Description
<input type="checkbox"/>	00-30-4f	PLANET phones
<input type="checkbox"/>	00-03-6b	Cisco phones
<input type="checkbox"/>	00-0f-e2	H3C phones
<input type="checkbox"/>	00-60-b9	Philips 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
<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">• 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).
<ul style="list-style-type: none">• Description	The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

Buttons

: Click to add a new access management entry.

: Click to apply changes

: 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 **512** on each switch. The Voice VLAN OUI Table screen in [Figure 4-10-1](#) appears.

ACL Status										
User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	CPU	CPU Once	Counter	Conflict	
DHCP	All	IPv4/UDP 67 DHCP Client	Deny	Disabled	Disabled	Yes	No	0	No	
DHCP	All	IPv4/UDP 68 DHCP Server	Deny	Disabled	Disabled	Yes	No	0	No	

Combined Auto-refresh

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

	<p>frames.</p> <ul style="list-style-type: none"> ■ 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	<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 port redirect operation of the ACE. Frames matching the ACE are redirected to the port number.</p> <p>The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.</p>
• Mirror	<p>Specify the mirror operation of this 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>
• CPU	<p>Forward packet that matched the specific ACE to CPU.</p>
• CPU Once	<p>Forward first packet that matched the specific ACE to CPU.</p>
• Counter	<p>The counter indicates the number of times the ACE was hit by a frame.</p>
• Conflict	<p>Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.</p>

Buttons

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

Click to refresh the page.

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 **512** on each switch.

Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest. The Access Control List Configuration screen in [Figure 4-10-2](#) appears.

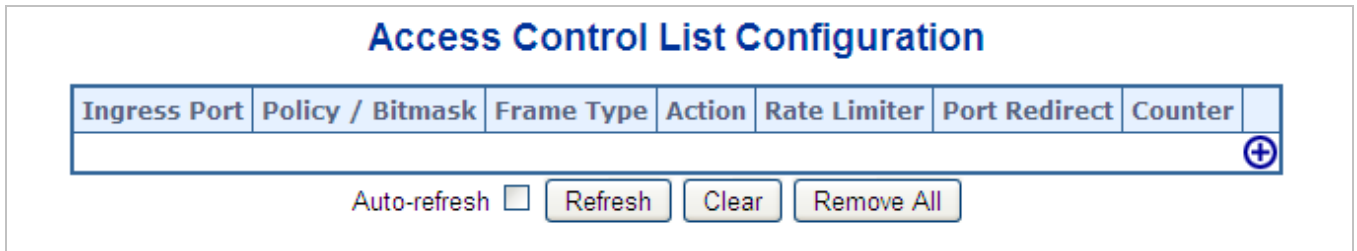








Figure 4-10-2: Access Control List Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Policy / Bitmask 	Indicates the policy number and bitmask of the ACE.
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> 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.

<ul style="list-style-type: none"> • 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>
<ul style="list-style-type: none"> • Port Redirect 	<p>Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number.</p> <p>The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.</p>
<ul style="list-style-type: none"> • Counter 	<p>The counter indicates the number of times the ACE was hit by a frame.</p>
<ul style="list-style-type: none"> • 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; any changes made locally will be undone.

: 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.

Figure 4-10-3: ACE Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Ingress Port 	Select the ingress port for which this ACE applies. <ul style="list-style-type: none"> ■ Any: The ACE applies to any port. ■ Port n: The ACE applies to this port number, where n is the number of the switch port.
<ul style="list-style-type: none"> Policy Filter 	Specify the policy number filter for this ACE. <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.
<ul style="list-style-type: none"> Policy Value 	When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255 .
<ul style="list-style-type: none"> Policy Bitmask 	When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff .
<ul style="list-style-type: none"> 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.

	<ul style="list-style-type: none"> ■ Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). ■ ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with Ethernet type. ■ IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with Ethernet type. ■ IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.
• Action	<p>Specify the action to take with a frame that hits this ACE.</p> <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	<p>Specify the rate limiter in number of base units.</p> <p>The allowed range is 1 to 16.</p> <p>Disabled indicates that the rate limiter operation is disabled.</p>
• Port Redirect	<p>Frames that hit the ACE are redirected to the port number specified here.</p> <p>The allowed range is the same as the switch port number range.</p> <p>Disabled indicates that the port redirect operation is disabled.</p>
• Logging	<p>Specify the logging operation of the ACE. The allowed values are:</p> <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. <p>Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.</p>
• Shutdown	<p>Specify the port shut down operation of the ACE. The allowed values are:</p> <ul style="list-style-type: none"> ■ Enabled: If a frame matches the ACE, the ingress port will be disabled. ■ Disabled: Port shut down is disabled for the ACE. <p>Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).</p>
• Counter	<p>The counter indicates the number of times the ACE was hit by a frame.</p>

■ 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" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). 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" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.</p>

■ VLAN Parameters

Object	Description
<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 ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.</p>
<ul style="list-style-type: none"> • Tag Priority 	<p>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".)</p>

■ ARP Parameters

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

Object	Description
<ul style="list-style-type: none"> • ARP/RARP 	<p>Specify the available ARP/RARP opcode (OP) flag for this ACE.</p> <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.
<ul style="list-style-type: none"> • Request/Reply 	<p>Specify the available ARP/RARP opcode (OP) flag for this ACE.</p> <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.
<ul style="list-style-type: none"> • Sender IP Filter 	<p>Specify the sender IP filter for this ACE.</p> <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.
<ul style="list-style-type: none"> • Sender IP Address 	<p>When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.</p>
<ul style="list-style-type: none"> • Sender IP Mask 	<p>When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.</p>
<ul style="list-style-type: none"> • Target IP Filter 	<p>Specify the target IP filter for this specific ACE.</p> <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.
<ul style="list-style-type: none"> • Target IP Address 	<p>When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.</p>
<ul style="list-style-type: none"> • Target IP Mask 	<p>When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.</p>
<ul style="list-style-type: none"> • ARP Sender MAC Match 	<p>Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.</p> <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").

<ul style="list-style-type: none"> • RARP Target MAC Match 	<p>Specify whether frames can hit the action according to their target hardware address field (THA) settings.</p> <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").
<ul style="list-style-type: none"> • IP/Ethernet Length 	<p>Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.</p> <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").
<ul style="list-style-type: none"> • IP 	<p>Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.</p> <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").
<ul style="list-style-type: none"> • Ethernet 	<p>Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.</p> <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").
<ul style="list-style-type: none"> • SIP Filter 	<p>Specify the source IP filter for this ACE.</p> <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.
<ul style="list-style-type: none"> • SIP Address 	<p>When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.</p>
<ul style="list-style-type: none"> • SIP Mask 	<p>When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.</p>
<ul style="list-style-type: none"> • DIP Filter 	<p>Specify the destination IP filter for this ACE.</p> <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.

■ IPv6 Parameters

Object	Description
• Next Header Filter	<p>Specify the IPv6 next header filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No IPv6 next header filter is specified ("don't-care"). ■ Specific: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears. ■ ICMP: Select ICMP to filter IPv6 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 IPv6 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 IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.
• Next Header Value	When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is 0 to 255 . A frame that hits this ACE matches this IPv6 protocol value.
• SIP Filter	<p>Specify the source IPv6 filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".) ■ Specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.
• SIP Address	When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.
• SIP BitMask	<p>When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care".</p> <p>The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.</p>

<ul style="list-style-type: none"> • Hop Limit 	<p>Specify the hop limit settings for this ACE.</p> <ul style="list-style-type: none"> ■ zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry. ■ non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry. ■ Any: Any value is allowed ("don't-care").
--	--

■ ICMP Parameters

Object	Description
<ul style="list-style-type: none"> • ICMP Type Filter 	<p>Specify the ICMP filter for this ACE.</p> <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.
<ul style="list-style-type: none"> • ICMP Type Value 	<p>When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value.</p> <p>The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.</p>
<ul style="list-style-type: none"> • ICMP Code Filter 	<p>Specify the ICMP code filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No ICMP code filter is specified (ICMP code filter status is "don't-care"). ■ Specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.
<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.</p> <p>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.

	<ul style="list-style-type: none"> ■ 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. 	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.
<ul style="list-style-type: none"> • TCP/UDP Source Range 	When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.
<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 	When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.
<ul style="list-style-type: none"> • TCP/UDP Destination Range 	When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.
<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").

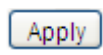
<ul style="list-style-type: none"> • TCP PSH 	<p>Specify the TCP "Push Function" (PSH) value for this ACE.</p> <ul style="list-style-type: none"> ■ 0: TCP frames where the PSH field is set must not be able to match this entry. ■ 1: TCP frames where the PSH field is set must be able to match this entry. ■ 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 this entry. ■ 1: TCP frames where the URG field is set must be able to match this entry. ■ Any: Any value is allowed ("don't-care").

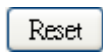
■ Ethernet Type Parameters

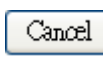
The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

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.</p> <p>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 apply 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.

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	9345
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


Figure 4-10-4: ACL Ports Configuration Page Screenshot


The page includes the following fields:

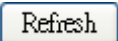
Object	Description
<ul style="list-style-type: none"> • Port 	The logical port for the settings contained in the same row.
<ul style="list-style-type: none"> • Policy ID 	Select the policy to apply to this port. The allowed values are 0 through 255 . The default value is 0.
<ul style="list-style-type: none"> • Action 	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
<ul style="list-style-type: none"> • Rate Limiter ID 	Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16 . The default value is "Disabled".
<ul style="list-style-type: none"> • Port Redirect 	Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".
<ul style="list-style-type: none"> • Logging 	Specify the logging operation of this port. The allowed values are: <ul style="list-style-type: none"> ■ 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 are limited.
<ul style="list-style-type: none"> • Shutdown 	Specify the port shut down operation of this port. The allowed values are: <ul style="list-style-type: none"> ■ Enabled: If a frame is received on the port, the port will be disabled.


	<ul style="list-style-type: none"> ■ Disabled: Port shut down is disabled. The default value is "Disabled".
<ul style="list-style-type: none"> • State 	<p>Specify the port state of this port. The allowed values are:</p> <ul style="list-style-type: none"> ■ 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. <p>The default value is "Enabled".</p>
<ul style="list-style-type: none"> • Counter 	Counts the number of frames that match this ACE.

Buttons

: Click to apply changes

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

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

: 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.

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

Figure 4-10-5: ACL Rate Limiter Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
• Rate (pps)	The allowed values are: 0-3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.

Buttons

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

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

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.

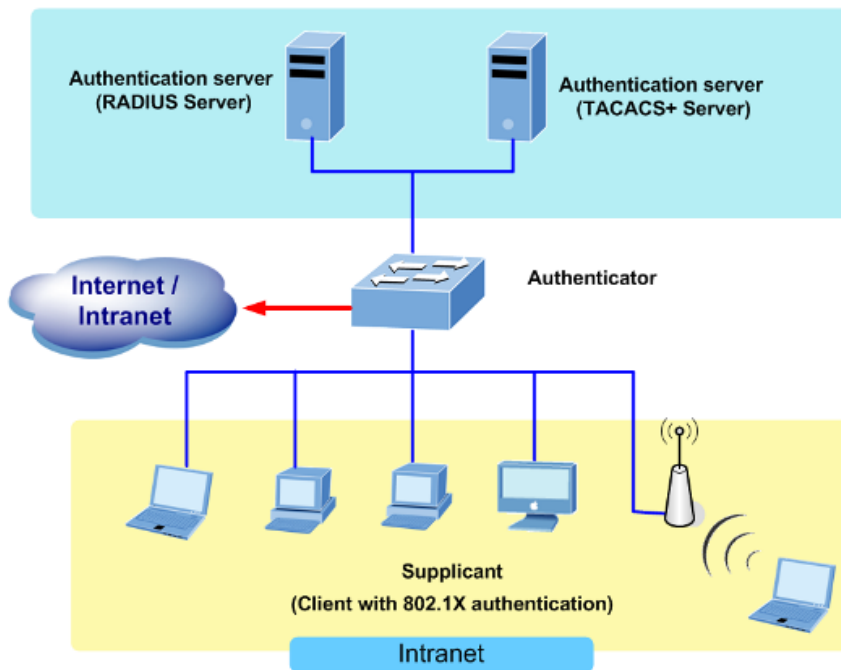


Figure 4-11-1

- **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.

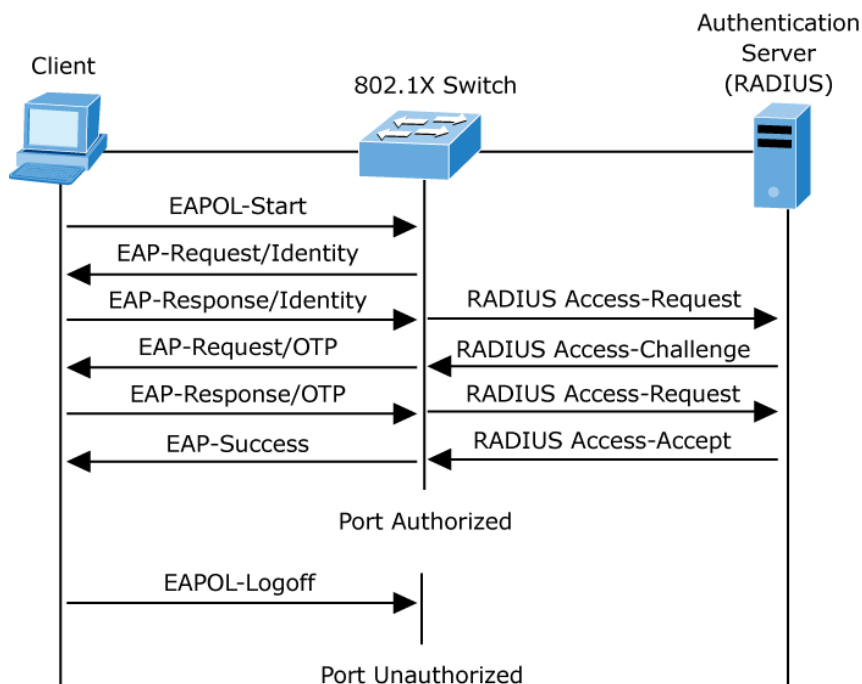


Figure 4-11-2: EAP Message Exchange

■ 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

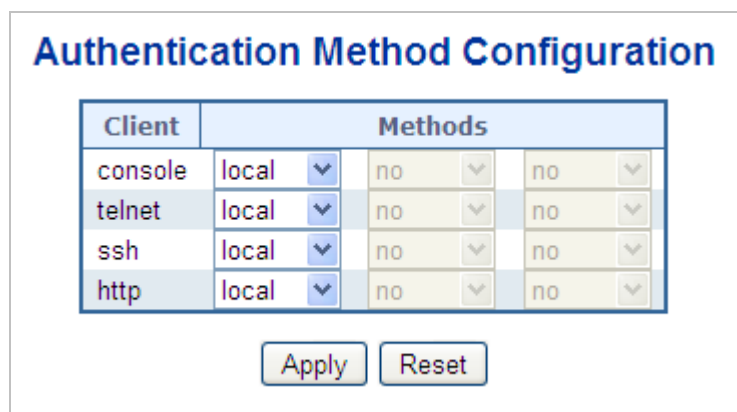
If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication 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.



The screenshot shows a configuration page titled "Authentication Method Configuration". It features a table with two main columns: "Client" and "Methods". The "Methods" column is subdivided into three columns, each with a "no" value and a dropdown arrow. Below the table are two buttons: "Apply" and "Reset".

Client	Methods		
console	local	no	no
telnet	local	no	no
ssh	local	no	no
http	local	no	no


Apply Reset

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	<p>Authentication Method can be set to one of the following values:</p> <ul style="list-style-type: none">■ None: authentication is disabled and login is not possible.■ Local: use the local user database on the switch for authentication.■ RADIUS: use a remote RADIUS server for authentication.■ TACACS+: use a remote TACACS+ server for authentication. <p>Methods that involve remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.</p>

Buttons

: Click to apply 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"/>			
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

Figure 4-11-4: Network Access Server Configuration Page Screenshot

The page includes the following fields:

System Configuration

Object	Description
<ul style="list-style-type: none"> • Mode 	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
<ul style="list-style-type: none"> • 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</p>

	switch and the client, and therefore doesn't imply that a client is still present on a port.
<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • EAPOL Timeout 	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.
<ul style="list-style-type: none"> • 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 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.</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 determines 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.</p> <p>The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled for that port. When unchecked, RADIUS-server assigned VLAN is disabled for all ports.</p>
<ul style="list-style-type: none"> • 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>
<ul style="list-style-type: none"> • 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.</p> <p>Valid values are in the range [1; 4095].</p>
<ul style="list-style-type: none"> • 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</p>

	<p>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>
<ul style="list-style-type: none"> • 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 and a number of columns, which are:

Object	Description
<ul style="list-style-type: none"> • Port 	<p>The port number for which the configuration below applies.</p>
<ul style="list-style-type: none"> • Admin State 	<p>If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:</p> <p>Force Authorized</p> <p>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.</p> <p>Force Unauthorized</p> <p>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.</p> <p>Port-based 802.1X</p> <p>In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames</p>

sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

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

Single 802.1X

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

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance.

Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X

Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

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

MAC-based Auth.

Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this


	<p>authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.</p> <p>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 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.</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>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> <ul style="list-style-type: none"> ● All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].
<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</p>


	<p>Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.</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 troubleshooting VLAN assignments, refer to 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 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; 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 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> <ul style="list-style-type: none">■ 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. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.■ Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.
--	---

Buttons

: Click to refresh the page.

: Click to apply 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.

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			-	

Figure 4-11-5: Network Access Server Switch Status Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	The switch port number. Click to navigate to detailed NAS statistics for this port.
<ul style="list-style-type: none"> • Admin State 	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
<ul style="list-style-type: none"> • Port State 	The current state of the port. Refer to NAS Port State for a description of the individual states.
<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • QoS Class 	QoS Class assigned to the port by the RADIUS server if enabled.
<ul style="list-style-type: none"> • 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

Click to refresh the page immediately.

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

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.

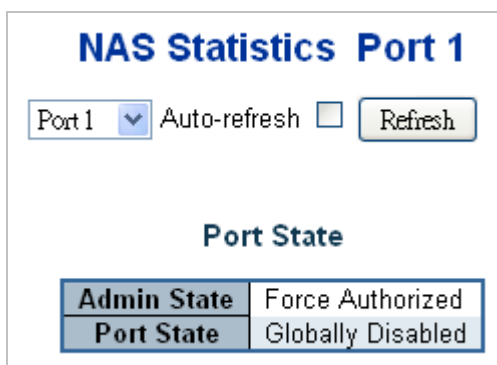


Figure 4-11-6: Network Access Statistics Page Screenshot

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	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Port Counters

Object	Description																																
<ul style="list-style-type: none"> EAPOL Counters 	<p>These supplicant frame counters are available for the following administrative states:</p> <ul style="list-style-type: none"> Force Authorized Force Unauthorized Port-based 802.1X Single 802.1X Multi 802.1X 																																
	<table border="1"> <thead> <tr> <th>Direction</th> <th>Name</th> <th>IEEE Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Rx</td> <td>Total</td> <td>dot1xAuthEapolFramesRx</td> <td>The number of valid EAPOL frames of any type that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Response ID</td> <td>dot1xAuthEapolRespIdFramesRx</td> <td>The number of valid EAPOL Response Identity frames that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Responses</td> <td>dot1xAuthEapolRespFramesRx</td> <td>The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Start</td> <td>dot1xAuthEapolStartFramesRx</td> <td>The number of EAPOL Start frames that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Logoff</td> <td>dot1xAuthEapolLogoffFramesRx</td> <td>The number of valid EAPOL Logoff frames that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Invalid Type</td> <td>dot1xAuthInvalidEapolFramesRx</td> <td>The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.</td> </tr> <tr> <td>Rx</td> <td>Invalid Length</td> <td>dot1xAuthEapLengthErrorFramesRx</td> <td>The number of EAPOL frames that have been received by the switch in</td> </tr> </tbody> </table>	Direction	Name	IEEE Name	Description	Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.	Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.	Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.	Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.	Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.	Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.	Rx	Invalid Length	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in
Direction	Name	IEEE Name	Description																														
Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.																														
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.																														
Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.																														
Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.																														
Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.																														
Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.																														
Rx	Invalid Length	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in																														

which the Packet Body Length field is invalid.

Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

• **Backend Server Counters**

These backend (RADIUS) frame counters are available for the following administrative states:

- **Port-based 802.1X**
- **Single 802.1X**
- **Multi 802.1X**
- **MAC-based Auth.**

Direction	Name	IEEE Name	Description
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	<p>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.</p> <p>MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).</p>

Rx	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	<p>802.1X-based:</p> <p>Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant.</p> <p>Indicates that the backend server chose an EAP-method.</p> <p>MAC-based:</p> <p>Not applicable.</p>
Rx	Auth. Successes	dot1xAuthBackendAuthSuccesses	<p>802.1X- and MAC-based:</p> <p>Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.</p>
Rx	Auth. Failures	dot1xAuthBackendAuthFails	<p>802.1X- and MAC-based:</p> <p>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.</p>
Tx	Responses	dot1xAuthBackendResponses	<p>802.1X-based:</p> <p>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.</p> <p>MAC-based:</p> <p>Counts all the backend server packets sent from the switch towards the backend server</p>

	<p>for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.</p>															
<ul style="list-style-type: none"> • Last Supplicant/Client Info 	<p>Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:</p> <ul style="list-style-type: none"> ■ Port-based 802.1X ■ Single 802.1X ■ Multi 802.1X ■ MAC-based Auth. <table border="1"> <thead> <tr> <th data-bbox="523 734 675 779">Name</th> <th data-bbox="675 734 938 779">IEEE Name</th> <th data-bbox="938 734 1495 779">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="523 779 675 902">MAC Address</td> <td data-bbox="675 779 938 902">dot1xAuthLastEapOfF rameSource</td> <td data-bbox="938 779 1495 902">The MAC address of the last supplicant/client.</td> </tr> <tr> <td data-bbox="523 902 675 1025">VLAN ID</td> <td data-bbox="675 902 938 1025">-</td> <td data-bbox="938 902 1495 1025">The VLAN ID on which the last frame from the last supplicant/client was received.</td> </tr> <tr> <td data-bbox="523 1025 675 1261">Version</td> <td data-bbox="675 1025 938 1261">dot1xAuthLastEapOfF rameVersion</td> <td data-bbox="938 1025 1495 1261"> 802.1X-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable. </td> </tr> <tr> <td data-bbox="523 1261 675 1552">Identity</td> <td data-bbox="675 1261 938 1552">-</td> <td data-bbox="938 1261 1495 1552"> 802.1X-based: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable. </td> </tr> </tbody> </table>	Name	IEEE Name	Description	MAC Address	dot1xAuthLastEapOfF rameSource	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	dot1xAuthLastEapOfF rameVersion	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.
Name	IEEE Name	Description														
MAC Address	dot1xAuthLastEapOfF rameSource	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	dot1xAuthLastEapOfF rameVersion	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</p>

	no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.
--	---

Attached MAC Address

Object	Description
<ul style="list-style-type: none"> • Identity 	<p>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.</p> <p>This column is not available for MAC-based Auth.</p>
<ul style="list-style-type: none"> • MAC Address 	<p>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.</p>
<ul style="list-style-type: none"> • VLAN ID 	<p>This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.</p>
<ul style="list-style-type: none"> • State 	<p>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.</p>
<ul style="list-style-type: none"> • Last Authentication 	<p>Shows the date and time of the last authentication of the client (successful as well as unsuccessful).</p>

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: This button is available in the following modes:

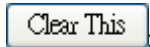
- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X

Click to clear the counters for the selected port.

Clear All: This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.

 Clear This

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
--------	----------	-----------	-----------	---------	------------	-----

Figure 4-11-7: RADIUS Server Configuration Page Screenshot

The page includes the following fields:

Global Configuration

These settings 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 from 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 	<p>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.</p> <p>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.</p>

• 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 settings are common for all of the TACACS+ 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 TACACS+ server before it is considered to be dead.
<ul style="list-style-type: none">• 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 Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.</p>
<ul style="list-style-type: none">• 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.

RADIUS Authentication Server Status Overview

#	IP Address	Status
<u>1</u>	0.0.0.0	Disabled
<u>2</u>	0.0.0.0	Disabled
<u>3</u>	0.0.0.0	Disabled
<u>4</u>	0.0.0.0	Disabled
<u>5</u>	0.0.0.0	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
<u>1</u>	0.0.0.0	Disabled
<u>2</u>	0.0.0.0	Disabled
<u>3</u>	0.0.0.0	Disabled
<u>4</u>	0.0.0.0	Disabled
<u>5</u>	0.0.0.0	Disabled

Auto-refresh **Refresh**

Figure 4-11-9: RADIUS Authentication/Accounting Server Overview Page Screenshot

The page includes the following fields:

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

RADIUS Accounting 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.

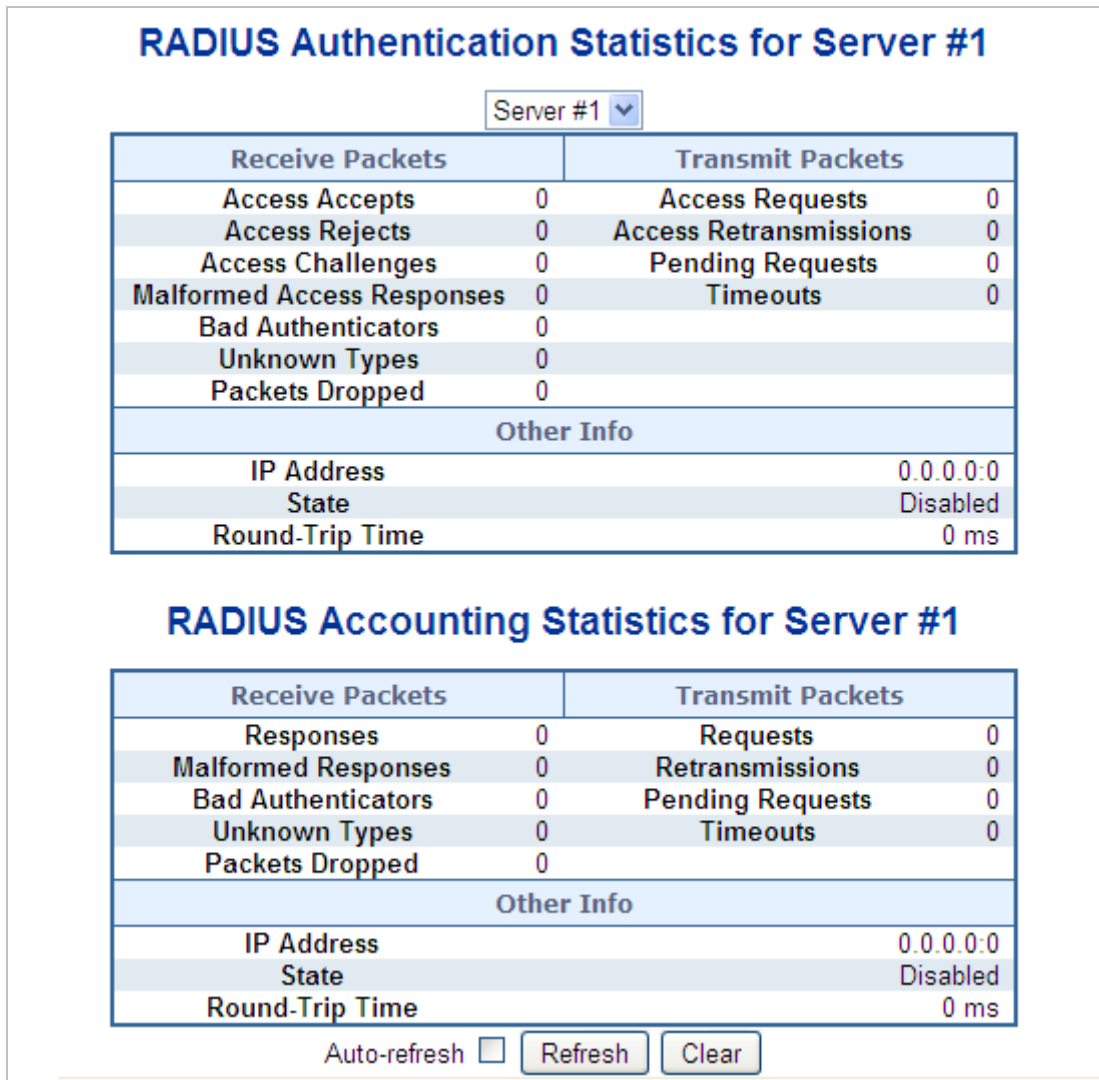


Figure 4-11-10: RADIUS Authentication/Accounting for Server Overview Screenshot

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.				
	<table border="1"> <thead> <tr> <th>Direction</th> <th>Name</th> <th>RFC4668 Name</th> <th>Description</th> </tr> </thead> <tbody> </tbody> </table>	Direction	Name	RFC4668 Name	Description
Direction	Name	RFC4668 Name	Description		

Rx	Access Accepts	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	Access Rejects	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	Access Challenges	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	Malformed Access Responses	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Rx	Bad Authenticators	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	Unknown Types	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Rx	Packets Dropped	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the

authentication port and dropped for some other reason.

Tx	Access Requests	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	Access Retransmissions	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	Pending Requests	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx	Timeouts	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

• **Other Info**

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port for the authentication server

in question.

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

- **Disabled**: The selected server is disabled.
- **Not Ready**: The server is enabled, but IP communication is not yet up and running.
- **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
- **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time 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.

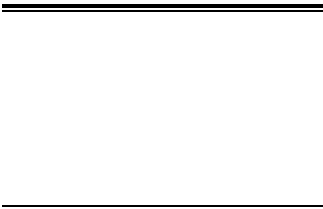
RADIUS Accounting Statistics

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 unknown types are not included as malformed access responses.
Rx	Bad Authenticators	radiusAccClientExt 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.												
<p>• Other Info</p> <p>This section contains information about the state of the server and the latest round-trip time.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>RFC4670 Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>IP Address</td> <td>-</td> <td>IP address and UDP port for the accounting server in question.</td> </tr> <tr> <td>State</td> <td>-</td> <td>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 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. </td> </tr> <tr> <td>Round-Trip Time</td> <td>radiusAccClientExtRo undTripTime</td> <td>■ The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server.</td> </tr> </tbody> </table>				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 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	radiusAccClientExtRo undTripTime	■ The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server.
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 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	radiusAccClientExtRo undTripTime	■ The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server.													



The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons

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.

4.11.10 Windows Platform RADIUS Server Configuration

Setup the RADIUS server and assign the client IP address to the Managed switch. In this case, field in the default IP Address of the Managed Switch with 192.168.0.100. And also make sure the shared **secret key** is as same as the one you had set at the Managed Switch's 802.1x system configuration – **12345678** at this case.

1. Configure the IP Address of remote RADIUS server and secret key.

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
<input type="checkbox"/>	123	1812	1813	10	33	12345678

Figure 4-11-11: RADIUS Server Configuration Screenshot

2. Add New RADIUS Client on the Windows 2003 server

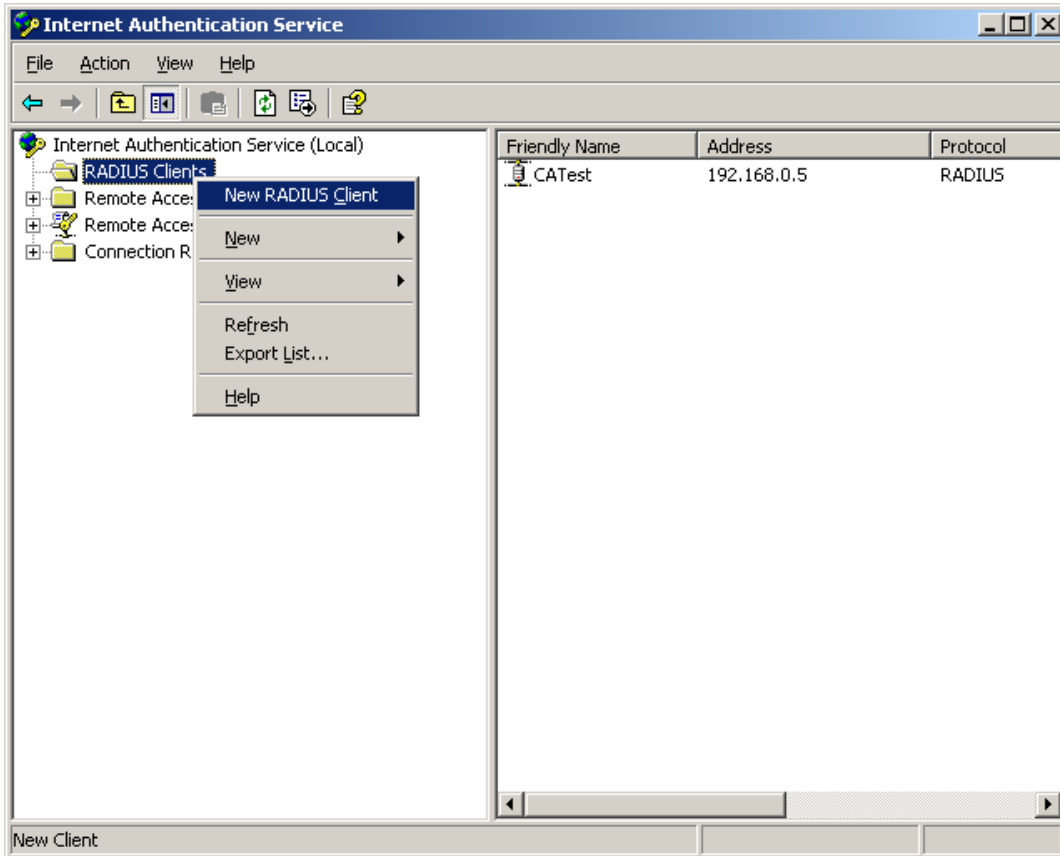


Figure 4-11-12: Windows Server – Add New RADIUS Client Setting

3. Assign the client IP address to the Managed Switch

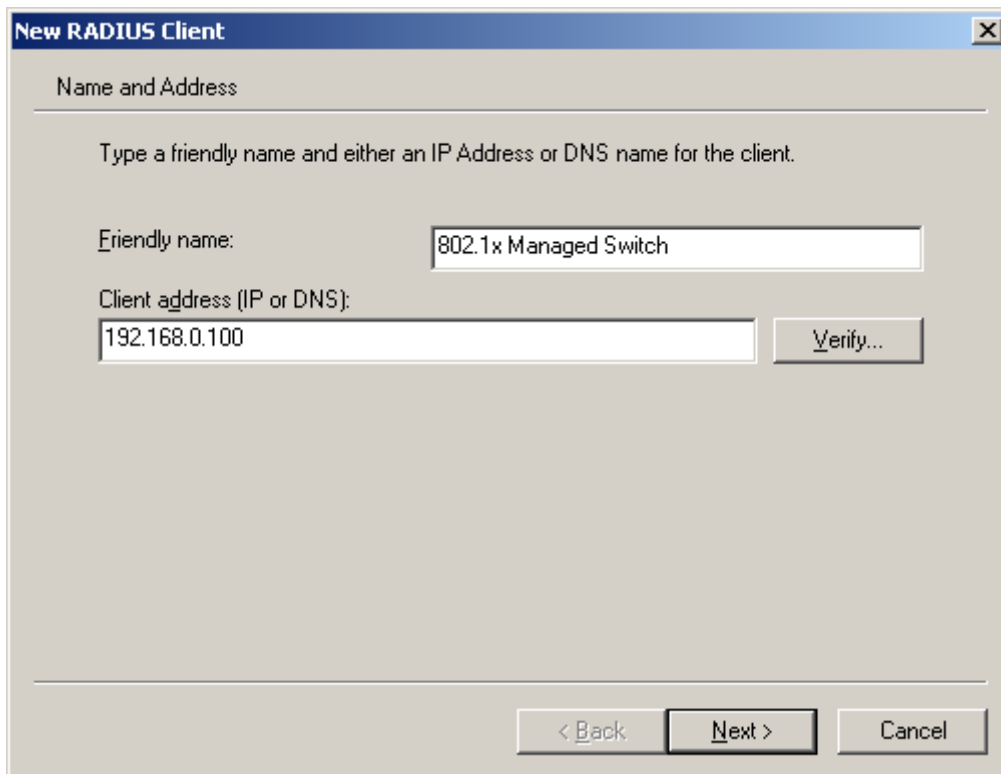


Figure 4-11-13: Windows Server RADIUS Server Setting

- The shared **secret key** should be as same as the key configured on the Managed Switch.

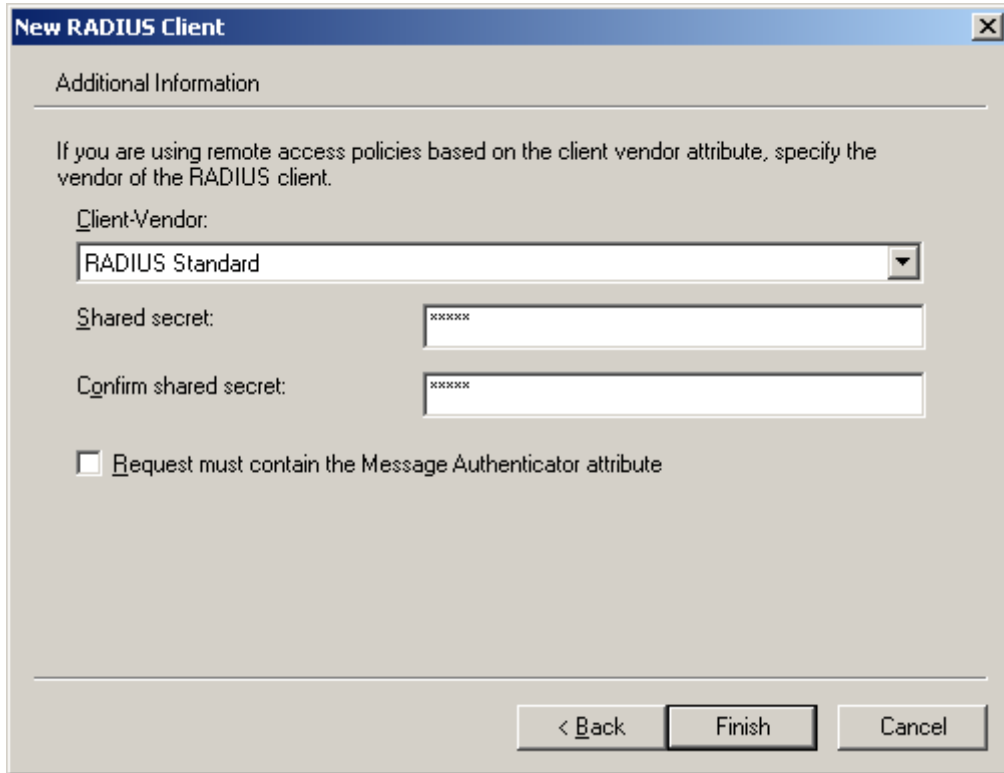


Figure 4-11-14: Windows Server RADIUS Server Setting

- Configure ports attribute of 802.1X, the same as “802.1X Port Configuration”.

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
1	Port-based 802.1X	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
2	Port-based 802.1X	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize

Figure 4-11-15: 802.1x Port Configuration

- Create user data. The establishment of the user data needs to be created on the Radius Server PC. For example, the Radius Server founded on Win2003 Server, and then:

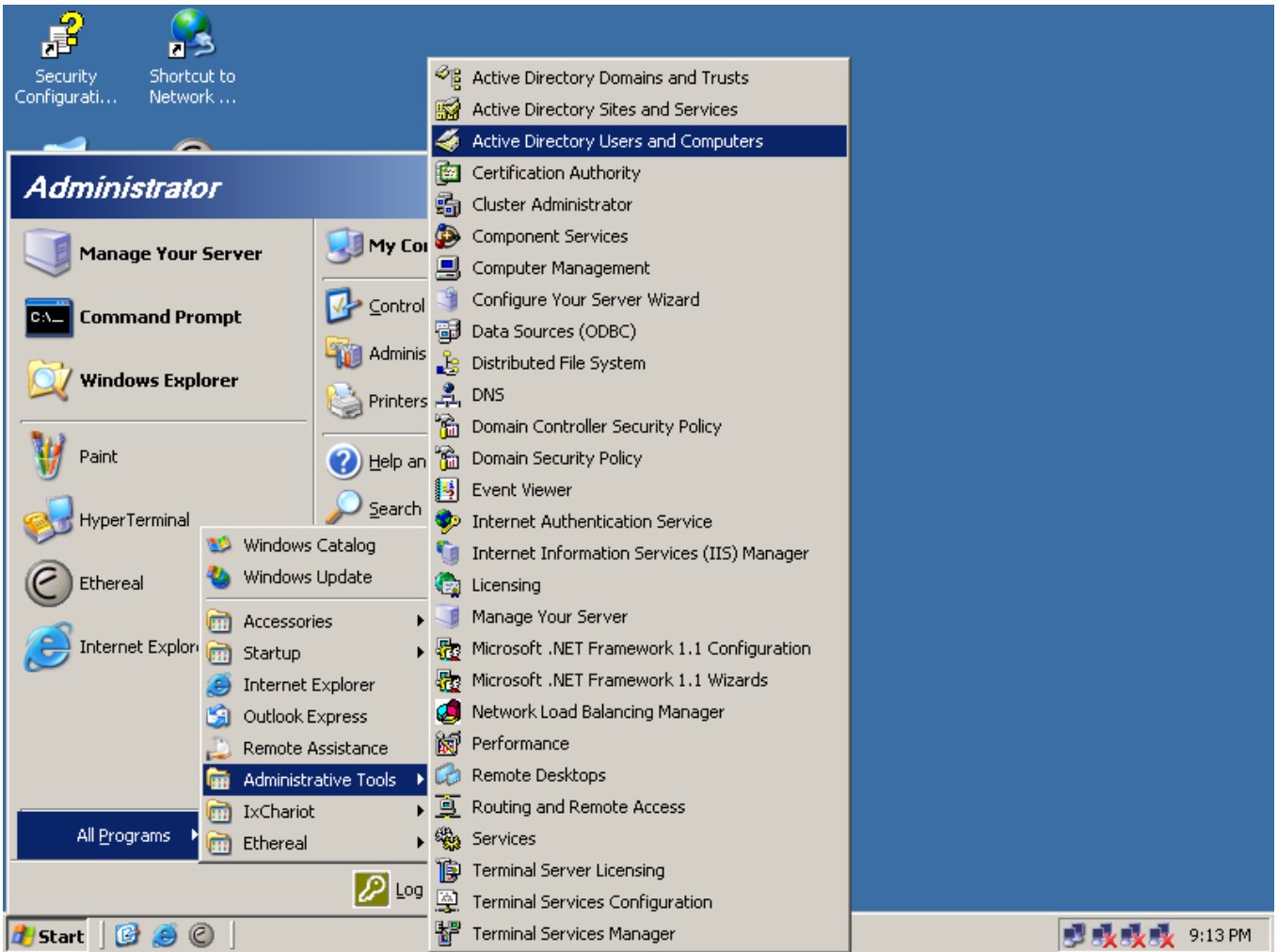


Figure 4-11-16: Windows 2003 AD Server Setting Path

7. Enter " **Active Directory Users and Computers**", create legal user data; next, right-click a user what you created to enter properties, and what to be noticed:

Figure 4-11-17: Add User Properties Screen

Figure 4-11-18: Add User Properties Screen



Set the Port Authenticate Status to **Force Authorized** if the port is connected to the RADIUS server or the port is an uplink port that is connected to another switch. Or once the 802.1X starts to work, the switch might not be able to access the RADIUS server.

4.11.11 802.1X Client Configuration

Windows XP is originally 802.1X support. As to other operating systems (windows 98SE, ME, 2000), an 802.1X client utility is needed. The following procedures show how to configure 802.1X Authentication in Windows XP.

Please note that if you want to change the 802.1x authentication type of a wireless client, i.e. switch to EAP-TLS from EAP-MD5, you must remove the current existing wireless network from your preferred connection first, and add it in again.

■ Configure Sample: EAP-MD5 Authentication

1. Go to **Start > Control Panel**, double-click on **"Network Connections"**.
2. Right-click on the Local Network Connection.
3. Click **"Properties"** to open up the Properties setting window.

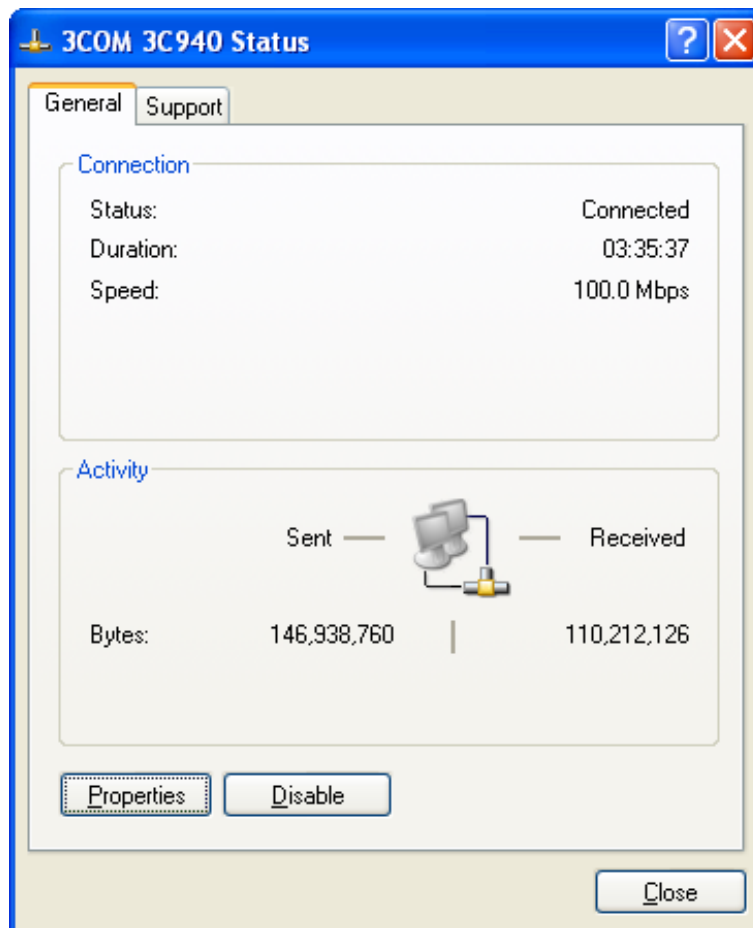


Figure 4-11-19

4. Select **"Authentication"** tab.
5. Select **"Enable network access control using IEEE 802.1X"** to enable 802.1x authentication.
6. Select **"MD-5 Challenge"** from the drop-down list box for EAP type.

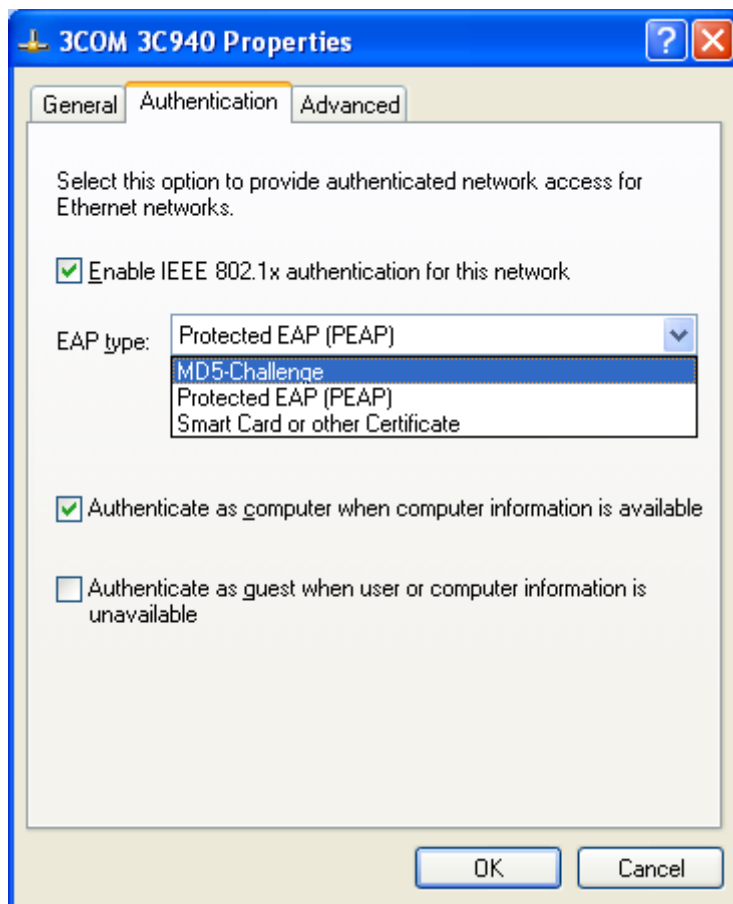


Figure 4-11-20

7. Click **“OK”**.
8. When client has associated with the Managed Switch, a user authentication notice appears in system tray. Click on the notice to continue.

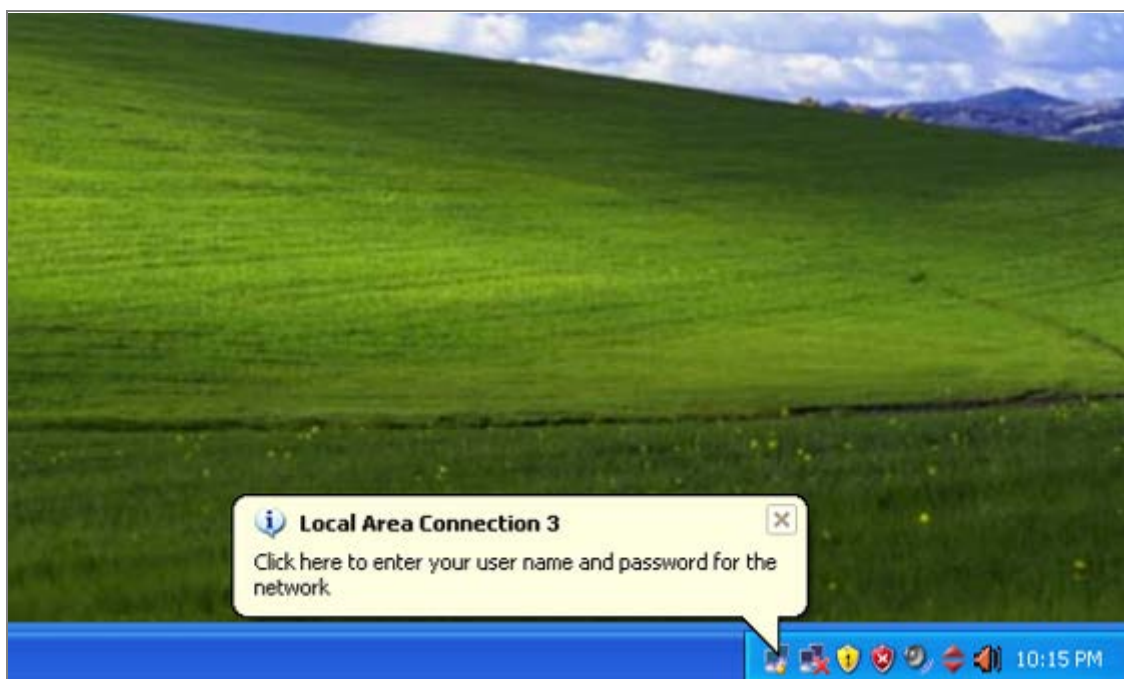


Figure 4-11-21: Windows Client Popup Login Request Message

9. Enter the user name, password and the logon domain that your account belongs.
10. Click **“OK”** to complete the validation process.

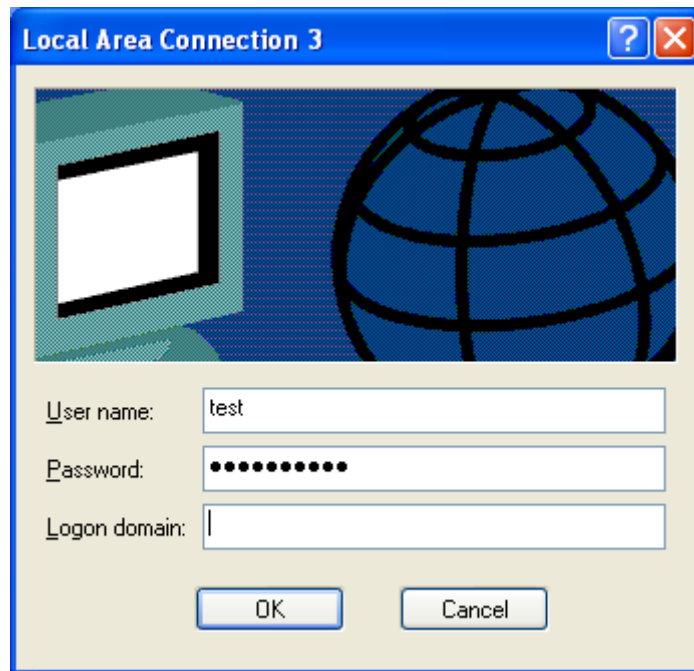


Figure 4-11-22

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**
- **HTTPs / SSH**
- **DHCP Snooping**
- **IP Source Guard**
- **ARP Inspection**

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 and Port Security module, which manage 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 <input type="button" value="v"/>
Aging Enabled	<input type="checkbox"/>
Aging Period	3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<All> <input type="button" value="v"/>	4	<All> <input type="button" value="v"/>		
1	Disabled <input type="button" value="v"/>	4	None <input type="button" value="v"/>	Disabled	<input type="button" value="Reopen"/>
2	Disabled <input type="button" value="v"/>	4	None <input type="button" value="v"/>	Disabled	<input type="button" value="Reopen"/>
3	Disabled <input type="button" value="v"/>	4	None <input type="button" value="v"/>	Disabled	<input type="button" value="Reopen"/>
4	Disabled <input type="button" value="v"/>	4	None <input type="button" value="v"/>	Disabled	<input type="button" value="Reopen"/>
5	Disabled <input type="button" value="v"/>	4	None <input type="button" value="v"/>	Disabled	<input type="button" value="Reopen"/>
6	Disabled <input type="button" value="v"/>	4	None <input type="button" value="v"/>	Disabled	<input type="button" value="Reopen"/>
7	Disabled <input type="button" value="v"/>	4	None <input type="button" value="v"/>	Disabled	<input type="button" value="Reopen"/>
8	Disabled <input type="button" value="v"/>	4	None <input type="button" value="v"/>	Disabled	<input type="button" value="Reopen"/>
9	Disabled <input type="button" value="v"/>	4	None <input type="button" value="v"/>	Disabled	<input type="button" value="Reopen"/>

Figure 4-12-1: Port Limit Control Configuration Overview Page Screenshot

The page includes the following fields:

System Configuration

Object	Description
<ul style="list-style-type: none"> • Mode 	<p>Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.</p>
<ul style="list-style-type: none"> • Aging Enabled 	<p>If checked, secured MAC addresses are subject to aging as discussed under Aging Period.</p>
<ul style="list-style-type: none"> • 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 and a number of columns, which are:


Object	Description
<ul style="list-style-type: none"> • Port 	<p>The port number for which the configuration below applies.</p>
<ul style="list-style-type: none"> • Mode 	<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</p>


	Control on a given port.
<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 switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.</p>
<ul style="list-style-type: none"> • Action 	<p>If Limit is reached, the switch can take one of the following actions:</p> <ul style="list-style-type: none"> ■ None: Do not allow more than Limit MAC addresses on the port, but take no further action. ■ Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded. ■ Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new 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: <ul style="list-style-type: none"> 1) Boot the switch, 2) Disable and re-enable Limit Control on the port or the switch, 3) Click the Reopen button. ■ Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.
<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> <ul style="list-style-type: none"> ■ Disabled: Limit Control is either globally disabled or disabled on the port. ■ Ready: The limit is not yet reached. This can be shown for all actions. ■ Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap. ■ Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap &

	Shutdown.
<ul style="list-style-type: none">• Re-open 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

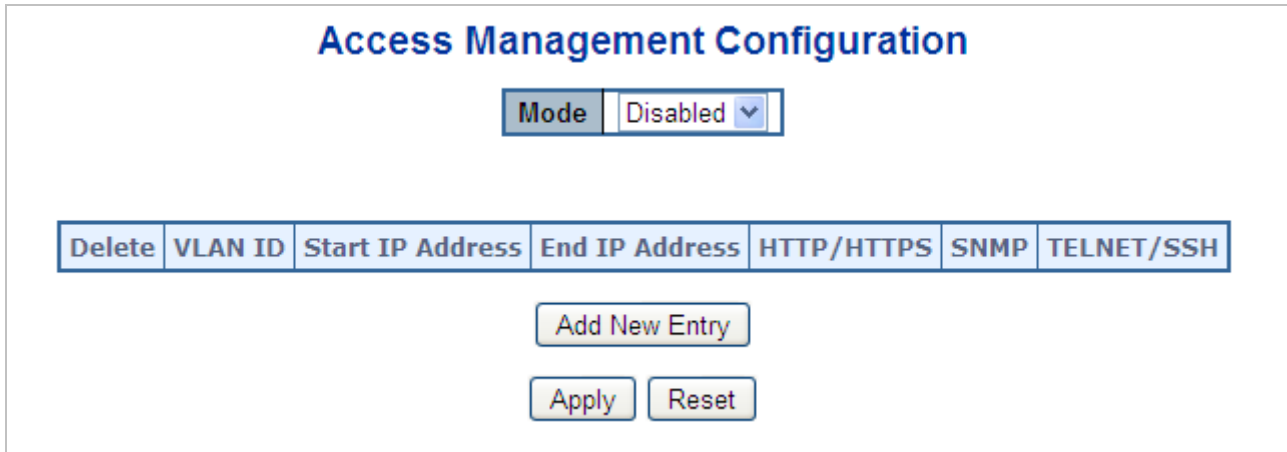
: Click to apply changes

: 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.



Access Management Configuration

Mode

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
--------	---------	------------------	----------------	------------	------	------------

Add New Entry

Apply Reset

Figure 4-12-2: Access Management Configuration Overview Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Mode	Indicates the access management mode operation. Possible modes are: Enabled: Enable access management mode operation. Disabled: Disable access management mode operation.
<ul style="list-style-type: none">• Delete	Check to delete the entry. It will be deleted during the next apply .
<ul style="list-style-type: none">• VLAN ID	Indicates the VLAN ID for the access management entry.
<ul style="list-style-type: none">• Start IP address	Indicates the start IP address for the access management entry.
<ul style="list-style-type: none">• End IP address	Indicates the end IP address for the access management entry.
<ul style="list-style-type: none">• HTTP/HTTPS	Indicates the host can access the switch from HTTP/HTTPS interface that the host IP address matched the entry.
<ul style="list-style-type: none">• SNMP	Indicates the host can access the switch from SNMP interface that the host IP address matched the entry.
<ul style="list-style-type: none">• Telnet/SSH	Indicates the host can access the switch from TELNET/SSH interface that the host IP address matched the entry.

Buttons

: Click to add a new access management entry.

: Click to apply changes

: 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.

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 switch.
• Receive Packets	The received packets number from the interface under access management mode is enabled.
• Allow Packets	The allowed packets number from the interface under access management mode is enabled.
• Discard Packets	The discarded packets number from the interface under access management mode is enabled.

Buttons

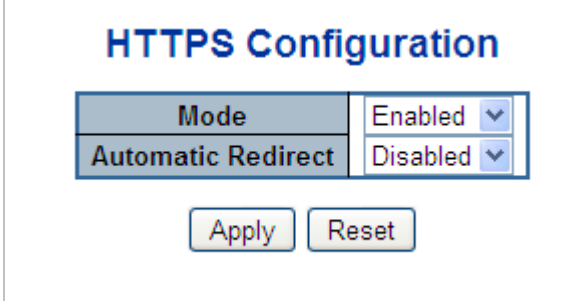
Auto-refresh Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

: Clears all statistics.

4.12.4 HTTPS

Configure HTTPS on this page. The HTTPS Configuration screen in [Figure 4-12-4](#) appears.




The screenshot shows a configuration interface titled "HTTPS Configuration". It contains two dropdown menus. The first dropdown, labeled "Mode", has "Enabled" selected. The second dropdown, labeled "Automatic Redirect", has "Disabled" selected. Below these dropdowns are two buttons: "Apply" and "Reset".


Figure 4-12-4: HTTPS Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Mode	<p>Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are:</p> <ul style="list-style-type: none">■ Enabled: Enable HTTPS mode operation.■ Disabled: Disable HTTPS mode operation.
<ul style="list-style-type: none">• Automatic Redirect	<p>Indicates the HTTPS redirect mode operation. It only significant if HTTPS mode "Enabled" is selected. Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled or redirects web browser to an HTTP connection when both are disabled. Possible modes are:</p> <ul style="list-style-type: none">■ Enabled: Enable HTTPS redirect mode operation.■ Disabled: Disable HTTPS redirect mode operation.

Buttons

: Click to apply 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.

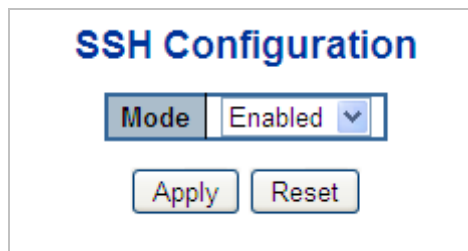
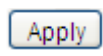



Figure 4-12-5: SSH Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none">• Mode	Indicates the SSH mode operation. Possible modes are: <ul style="list-style-type: none">■ Enabled: Enable SSH mode operation.■ Disabled: Disable SSH mode operation.

Buttons

: Click to apply 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.

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	---	Disabled	-	-
5	---	Disabled	-	-
6	---	Disabled	-	-
7	---	Disabled	-	-
8	---	Disabled	-	-

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
<ul style="list-style-type: none"> • User Module Name 	The full name of a module that may request Port Security services.
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • Port 	The port number for which the status applies. Click the port number to see the status for this particular port.

<ul style="list-style-type: none"> • Users 	<p>Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter has enabled port security.</p>
<ul style="list-style-type: none"> • State 	<p>Shows the current state of the port. It can take one of four values:</p> <ul style="list-style-type: none"> ■ 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.
<ul style="list-style-type: none"> • MAC Count (Current, Limit) 	<p>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.</p> <p>If no user modules are enabled on the port, the Current column will show a dash (-).</p> <p>If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).</p>

Buttons

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

Click to refresh the page immediately.

4.12.7 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.

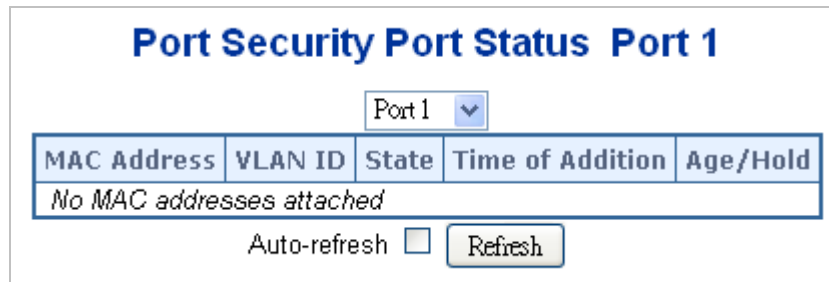


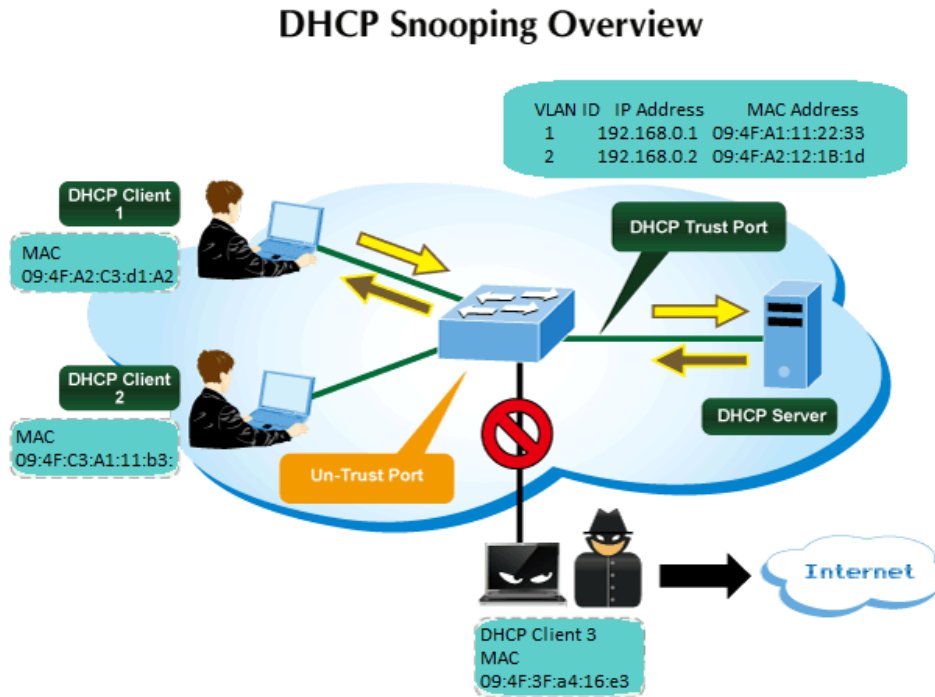
Figure 4-12-7: Port Security Detail Screen Page Screenshot

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 	<ul style="list-style-type: none"> ● If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. ● If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. ● If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. ● If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

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

Port Mode Configuration

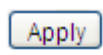
Port	Mode
*	<All>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted

Figure 4-12-8: DHCP Snooping Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Snooping Mode 	<p>Indicates the DHCP snooping mode operation. Possible modes are:</p> <ul style="list-style-type: none"> ■ 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 Configuration 	<p>Indicates the DHCP snooping port mode. Possible port modes are:</p> <ul style="list-style-type: none"> ■ Trusted: Configures the port as trusted sources of the DHCP message. ■ Untrusted: Configures the port as untrusted sources of the DHCP message.

Buttons

 : Click to apply changes

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

4.12.9 Snooping Table

This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page. The Dynamic DHCP Snooping Table screen in [Figure 4-12-9](#) appears.

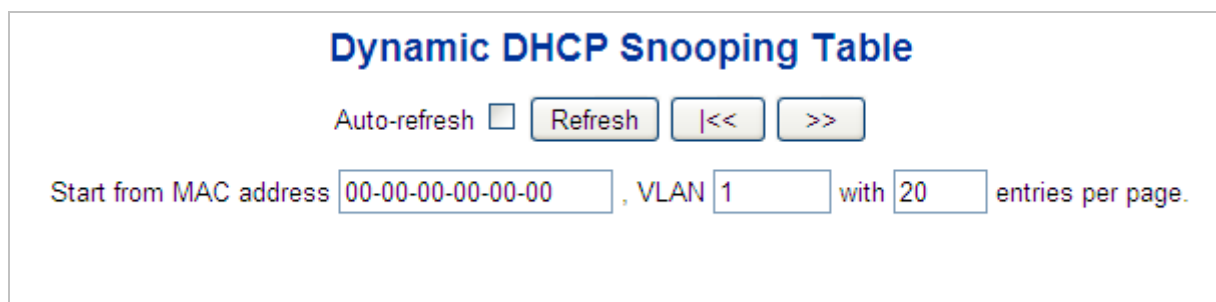



Figure 4-12-9: Dynamic DHCP Snooping Table Screen Page Screenshot

Buttons

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

 : It will use the last entry of the currently displayed table as a basis for the next lookup. When the end is

reached the text "No more entries" is shown in the displayed table

: To start over

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.

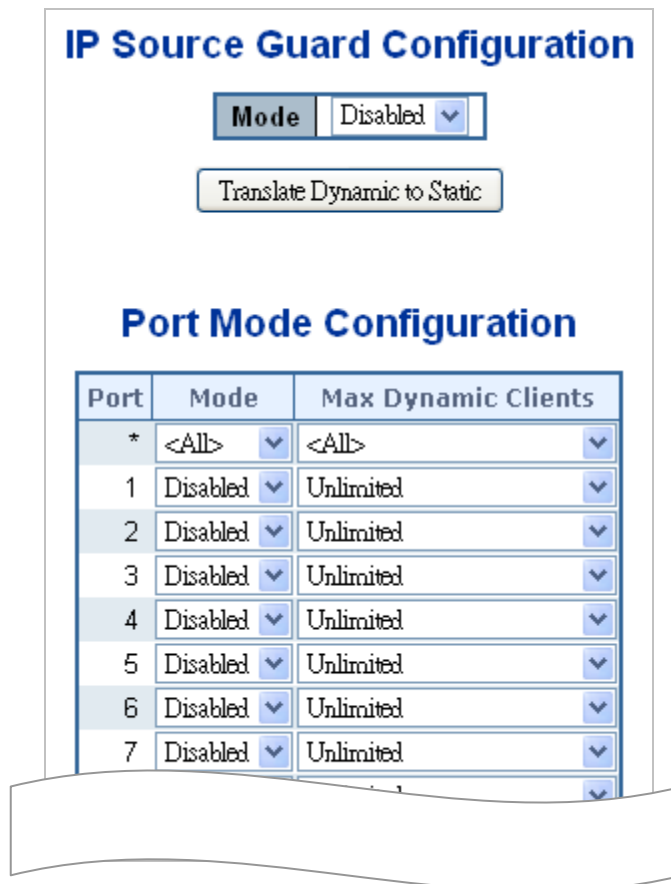


Figure 4-12-10: IP Source Guard Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • 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.

Buttons

Translate Dynamic to Static: Click to translate all dynamic entries to static entries.

Apply: Click to apply 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.

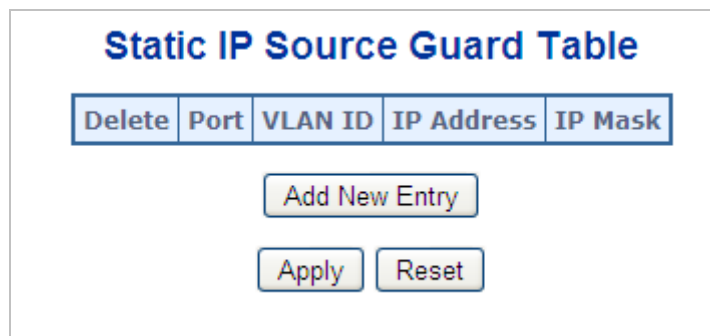


Figure 4-12-11: Static IP Source Guard Table Screen Page Screenshot

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"> • Port 	The logical port for the settings.
<ul style="list-style-type: none"> • VLAN ID 	The VLAN ID for the settings.
<ul style="list-style-type: none"> • IP Address 	Allowed Source IP address.
<ul style="list-style-type: none"> • MAC Address 	Allowed Source MAC address.

Buttons

Add New Entry: Click to add a new entry to the Static IP Source Guard table.

Apply: Click to apply changes

Reset: 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	Check VLAN	Log Type
*	<All>	<All>	<All>
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None
7	Disabled	Disabled	None

Figure 4-12-12: ARP Inspection Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Mode of ARP Inspection Configuration 	Enable the Global ARP Inspection or disable the Global ARP Inspection.
<ul style="list-style-type: none"> • Port Mode Configuration 	<p>Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:</p> <ul style="list-style-type: none"> ■ Enabled: Enable ARP Inspection operation. ■ Disabled: Disable ARP Inspection operation. <p>If you want to inspect the VLAN configuration, you have to enable the setting</p>

of **"Check VLAN"**. The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of **"Check VLAN"** are:

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

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

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

Buttons

- : Click to translate all dynamic entries to static entries.
- : Click to apply changes
- : 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.

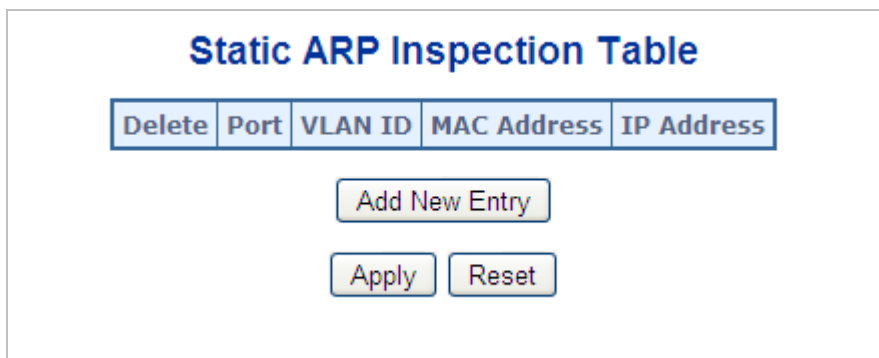


Figure 4-12-13: Static ARP Inspection Table Screen Page Screenshot

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

Add New Entry

: Click to add a new entry to the Static ARP Inspection table.

Apply

: Click to apply changes

Reset

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

4.12.14 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 4-12-14](#) appears.

Figure 4-12-14: Dynamic ARP Inspection Table Screenshot

Navigating the ARP Inspection Table

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

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

The ">>" 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	The port number for which the status applies. Click the port number to see the status for this particular port.
• VLAN ID	The VLAN ID of the entry.
• MAC Address	The MAC address of the entry.
• IP Address	The IP address of the entry.

Buttons

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 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 have been seen after a configurable age time.

4.13.1 MAC 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.

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
<ul style="list-style-type: none"> • Disable Automatic Aging 	Enables/disables the automatic aging of dynamic entries
<ul style="list-style-type: none"> • 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)
--	--

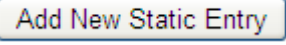
MAC Table Learning

If the learning mode for a given port is grayed 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
<ul style="list-style-type: none"> • Auto 	Learning is done automatically as soon as a frame with unknown SMAC is received.
<ul style="list-style-type: none"> • Disable 	No learning is done.
<ul style="list-style-type: none"> • 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
<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"> • VLAN ID 	The VLAN ID of the entry.
<ul style="list-style-type: none"> • MAC Address 	The MAC address of the entry.
<ul style="list-style-type: none"> • Port Members 	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
<ul style="list-style-type: none"> • Adding a New Static Entry 	Click  to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

Buttons

: Click to apply changes

: 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.

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.

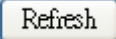
The ">>" will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "no more entries" is shown in the displayed table. Use the "<<" button to start over.


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 Automatic refresh occurs every 3 seconds.

 Refresh: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

 Clear: Flushes all dynamic entries.

 k<<: 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.

4.14 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

Port	Mode	CDP Aware	Optional TLVs				
			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"/>

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: (Transmission Interval * Hold Time Multiplier) ≤ 65536, and Transmission Interval ≥ (4 * 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: (Transmission Interval * Holdtime Multiplier) ≤ 65536. 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: (4 * Delay Interval) ≤ 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 switch, as reflected by the page header.

Object	Description
<ul style="list-style-type: none"> Port 	The switch port number of the logical LLDP port.
<ul style="list-style-type: none"> Mode 	<p>Select LLDP mode.</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.

	<ul style="list-style-type: none"> ■ 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.
<ul style="list-style-type: none"> • 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>
<ul style="list-style-type: none"> • Port Description 	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
<ul style="list-style-type: none"> • System Name 	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
<ul style="list-style-type: none"> • System Description 	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
<ul style="list-style-type: none"> • System Capabilities 	Optional TLV: When checked the "system capability" is included in LLDP information transmitted.
<ul style="list-style-type: none"> • Management Address 	Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons

: Click to apply 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 LLDPMED Configuration screen in [Figure 4-14-2](#) appears.

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count

Coordinates Location

Latitude ° Longitude ° Altitude Map Datum

Civic Address Location

Country code	State	County
<input type="text"/>	<input type="text"/>	<input type="text"/>
City	City district	Block (Neighborhood)
<input type="text"/>	<input type="text"/>	<input type="text"/>
Street	Leading street direction	Trailing street suffix
<input type="text"/>	<input type="text"/>	<input type="text"/>
Street suffix	House no.	House no. suffix
<input type="text"/>	<input type="text"/>	<input type="text"/>
Landmark	Additional location info	Name
<input type="text"/>	<input type="text"/>	<input type="text"/>
Zip code	Building	Apartment
<input type="text"/>	<input type="text"/>	<input type="text"/>
Floor	Room no.	Place type
<input type="text"/>	<input type="text"/>	<input type="text"/>
Postal community name	P.O. Box	Additional code
<input type="text"/>	<input type="text"/>	<input type="text"/>

Emergency Call Service

Emergency Call Service

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

Figure 4-14-2: LLDPMED 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 	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

	<p>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 neighbour has been detected in order share LLDP-MED information as fast as possible to new neighbours.</p> <p>Because there is a risk of an LLDP frame being lost during transmission between neighbours, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbours receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.</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 Network Connectivity Devices, or 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> <p>Meters: Representing meters of Altitude defined by the vertical datum specified.</p>

	<p>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.</p>
<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
<ul style="list-style-type: none"> • Country code 	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
<ul style="list-style-type: none"> • State 	National subdivisions (state, canton, region, province, prefecture).
<ul style="list-style-type: none"> • County 	County, parish, gun (Japan), district.
<ul style="list-style-type: none"> • City 	City, township, shi (Japan) - Example: Copenhagen
<ul style="list-style-type: none"> • City district 	City division, borough, city district, ward, chou (Japan)
<ul style="list-style-type: none"> • Block (Neighborhood) 	Neighborhood, block
<ul style="list-style-type: none"> • Street 	Street - Example: Poppelvej
<ul style="list-style-type: none"> • Leading street direction 	Leading street direction - Example: N
<ul style="list-style-type: none"> • Trailing street suffix 	Trailing street suffix - Example: SW
<ul style="list-style-type: none"> • Street suffix 	Street suffix - Example: Ave, Platz
<ul style="list-style-type: none"> • House no. 	House number - Example: 21
<ul style="list-style-type: none"> • House no. suffix 	House number suffix - Example: A, 1/2
<ul style="list-style-type: none"> • Landmark 	Landmark or vanity address - Example: Columbia University
<ul style="list-style-type: none"> • Additional location info 	Additional location info - Example: South Wing
<ul style="list-style-type: none"> • Name 	Name (residence and office occupant) - Example: Flemming Jahn

• Zip code	Postal/zip code - Example: 2791
• Building	Building (structure) - Example: Low Library
• Apartment	Unit (Apartment, suite) - Example: Apt 42
• Floor	Floor - Example: 4
• Room no.	Room number - Example: 450F
• Place type	Place type - Example: Office
• Postal community name	Postal community name - Example: Leonia
• P.O. Box	Post office box (P.O. BOX) - Example: 12345
• Additional code	Additional code - Example: 1320300003

Emergency Call Service

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

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

Policies

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

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

The network policy attributes advertised are:

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:

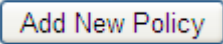
1. Voice
2. Guest Voice
3. Softphone Voice

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
<ul style="list-style-type: none"> • Delete 	Check to delete the policy. It will be deleted during the next save.
<ul style="list-style-type: none"> • Policy ID 	ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.
<ul style="list-style-type: none"> • Application Type 	Intended use of the application types: <ul style="list-style-type: none"> ■ Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. ■ Voice Signaling (conditional) - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy. ■ Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. ■ Guest Voice Signaling (conditional) - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy. ■ Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged'

	<p>VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.</p> <ul style="list-style-type: none"> ■ Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. ■ Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. ■ Video Signaling (conditional) - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.
<ul style="list-style-type: none"> • Tag 	<p>Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.</p> <ul style="list-style-type: none"> ■ Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. ■ Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.
<ul style="list-style-type: none"> • VLAN ID 	<p>VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003</p>
<ul style="list-style-type: none"> • L2 Priority 	<p>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.</p>
<ul style="list-style-type: none"> • DSCP 	<p>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.</p>
<ul style="list-style-type: none"> • Adding a new policy 	<p>Click  to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save". The number of policies supported is 32</p>

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
<ul style="list-style-type: none"> • Port 	The port number for which the configuration applies.
<ul style="list-style-type: none"> • 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

: Click to apply changes

: 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:

LLDP-MED Neighbour Information					
Port 1					
Device Type	Capabilities				
Endpoint Class III	LLDP-MED Capabilities, Network Policy, Extended Power via MDI - PD, Inventory				
Application Type	Policy	Tag	VLAN ID	Priority	DSCP
Voice	Defined	Untagged	-	-	46
Voice Signaling	Defined	Untagged	-	-	32
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities		MAU Type	
Supported	Enabled	1000BASE-T half duplex mode, 1000BASE-X, -LX, -SX, -CX full duplex mode, Asymmetric and Symmetric PAUSE for full-duplex inks, Symmetric PAUSE for full-duplex links		100BaseTXFD - 2 pair category 5 UTP, full duplex mode	

Figure 4-14-3: LLDP-MED Neighbor Information Page Screenshot

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 	LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices. LLDP-MED Network Connectivity Device Definition

LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (included for historical reasons)
4. IEEE 802.11 Wireless Access Point
5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. 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)

	<p>The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.</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. 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. The possible application types are shown below.</p> <ul style="list-style-type: none"> ■ Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. ■ Voice Signaling - for use in network topologies that require a different policy for the voice signaling than for the voice media. ■ Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. ■ Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. ■ Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. ■ Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. ■ Streaming Video - for use by broadcast or multicast based video content

	<p>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> <ul style="list-style-type: none"> ■ Video Signaling - for use in network topologies that require a separate policy for the video signaling than for the video media.
<ul style="list-style-type: none"> • Policy 	<p>Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown</p> <ul style="list-style-type: none"> ■ Unknown: The network policy for the specified application type is currently unknown. ■ Defined: The network policy is defined.
<ul style="list-style-type: none"> • TAG 	<p>TAG is indicating whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged</p> <ul style="list-style-type: none"> ■ Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. ■ Tagged: The device is using the IEEE 802.1Q tagged frame format
<ul style="list-style-type: none"> • 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>
<ul style="list-style-type: none"> • 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>
<ul style="list-style-type: none"> • 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>
<ul style="list-style-type: none"> • Auto-negotiation 	<p>Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.</p>
<ul style="list-style-type: none"> • 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 	<p>Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.</p>

Buttons

Click to refresh the page immediately.

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

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.



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.
• Port ID	The Port ID is the identification of the neighbor port.
• Port Description	Port Description is the port description advertised by the neighbor unit.
• System Name	System Name is the name 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. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. 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.

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 switch, while local counters refers to counters for the currently selected switch. The LLDP Statistics screen in [Figure 4-14-5](#) appears.

LLDP Global Counters								
Global Counters								
Neighbor entries were last changed 1970-01-01 Thu 00:00:00+00:00 (10496 secs. ago)								
Total Neighbors Entries Added 0								
Total Neighbors Entries Deleted 0								
Total Neighbors Entries Dropped 0								
Total Neighbors Entries Aged Out 0								

LLDP Statistics Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	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

Figure 4-14-5: LLDP Statistics Page Screenshot

The page includes the following fields:

Global Counters

Object	Description
• Neighbor entries were last changed	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.

LLDP Statistics Local Counters

The displayed table contains a row for each port. The columns hold the following information:

Object	Description
• Local Port	The port on which LLDP frames are received or transmitted.
• Tx Frames	The number of LLDP frames transmitted on the port.
• Rx Frames	The number of LLDP frames received on the port.
• Rx Errors	The number of received LLDP frames containing some kind of error.
• Frames Discarded	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
• TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
• TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
• Org. Discarded	The number of organizationally TLVs received.
• Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

Buttons

: Click to refresh the page immediately.

: Clears the local counters. All counters (including global counters) are cleared upon reboot.

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

4.15 Network 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 transmit ICMP packets, and the sequence number and roundtrip time are displayed upon reception of a reply.

Cable Diagnostics

The Cable Diagnostics 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.

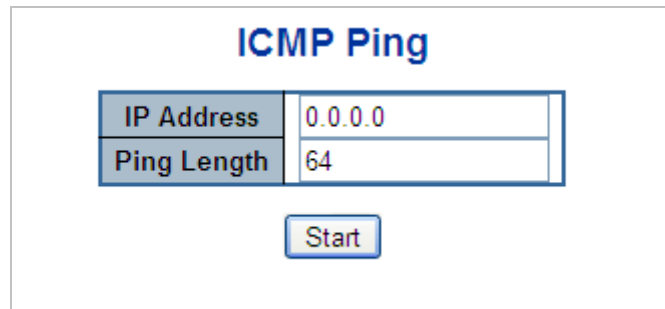
After the diagnostics are finished, the link is reestablished. And the following functions are available.

- 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.



ICMP Ping

IP Address	0.0.0.0
Ping Length	64

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.



Be sure the target IP Address is within the same network subnet of the Managed Switch, or you had setup the correct gateway IP address.

Buttons

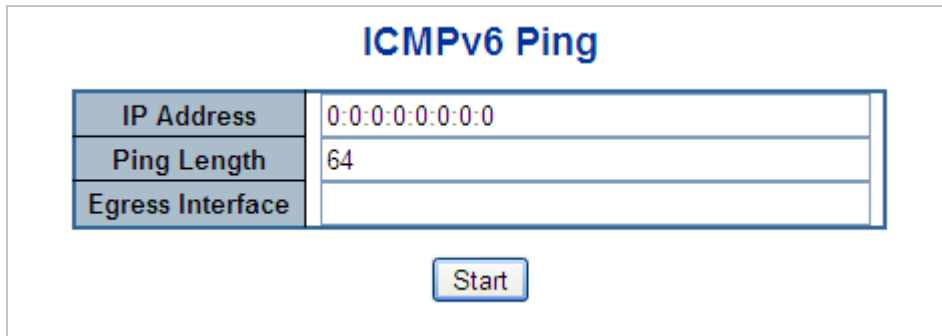
: Click to transmit ICMP packets.

: 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	64
Egress Interface	

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.
• Egress Interface	The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination. Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.

Buttons

Start: Click to transmit 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.

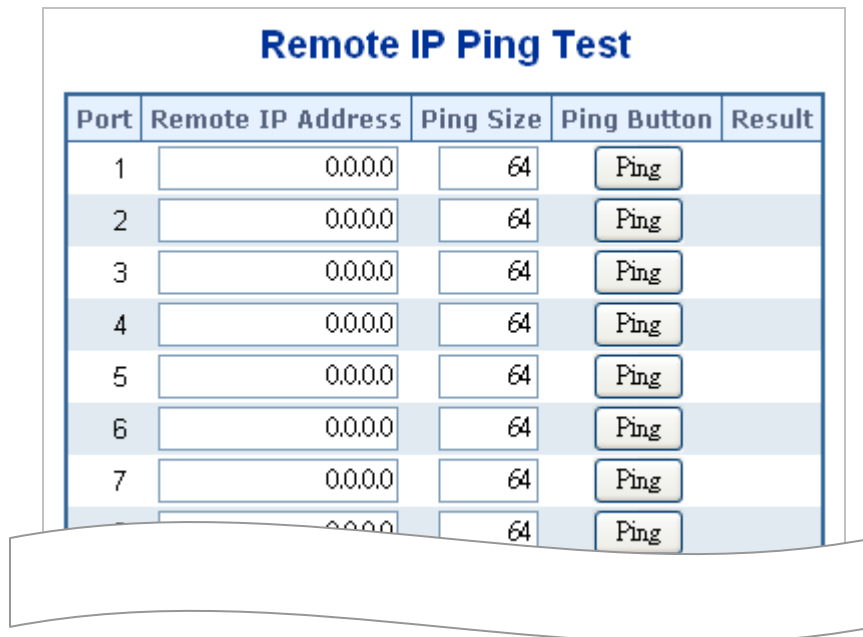


Figure 4-15-3: Remote IP Ping Test Page Screenshot

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

Apply: Click to apply changes

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

Clear: Clears the IP Address and the result of ping value.

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 VeriPHY Cable Diagnostics screen in [Figure 4-15-4](#) appears.

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		--	--	--	--	--	--	--	--
5		--	--	--	--	--	--	--	--
6		--	--	--	--	--	--	--	--
7		--	--	--	--	--	--	--	--

Figure 4-15-4: VeriPHY Cable Diagnostics Page Screenshot

The page includes the following fields:

Object	Description
• Port	The port where you are requesting Cable Diagnostics.
• Description	Display per port description.

- **Cable Status**

Port:

Port number.

Pair:

The status of the cable pair.

OK - Correctly terminated pair

Open - Open pair

Short - Shorted pair

Short A - Cross-pair short to pair A

Short B - Cross-pair short to pair B

Short C - Cross-pair short to pair C

Short D - Cross-pair short to pair D

Cross A - Abnormal cross-pair coupling with pair A

Cross B - Abnormal cross-pair coupling with pair B

Cross C - Abnormal cross-pair coupling with pair C

Cross D - Abnormal cross-pair coupling with pair D

Length:

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

Buttons

: Click to run the diagnostics.

4.16 Power over Ethernet

Providing up to 8 PoE, in-line power interfaces, the NS3502-8P-2T-2S PoE Switch can easily build a power that centrally controls IP phone system, IP Camera system, AP group for the enterprise. For instance, 8 cameras / APs can be easily installed around the corners of the company for surveillance demands or a wireless roaming environment in the office can be built. Without the power-socket limitation, the NS3502-8P-2T-2S PoE Switch makes the installation of cameras or WLAN AP easier and more efficient.

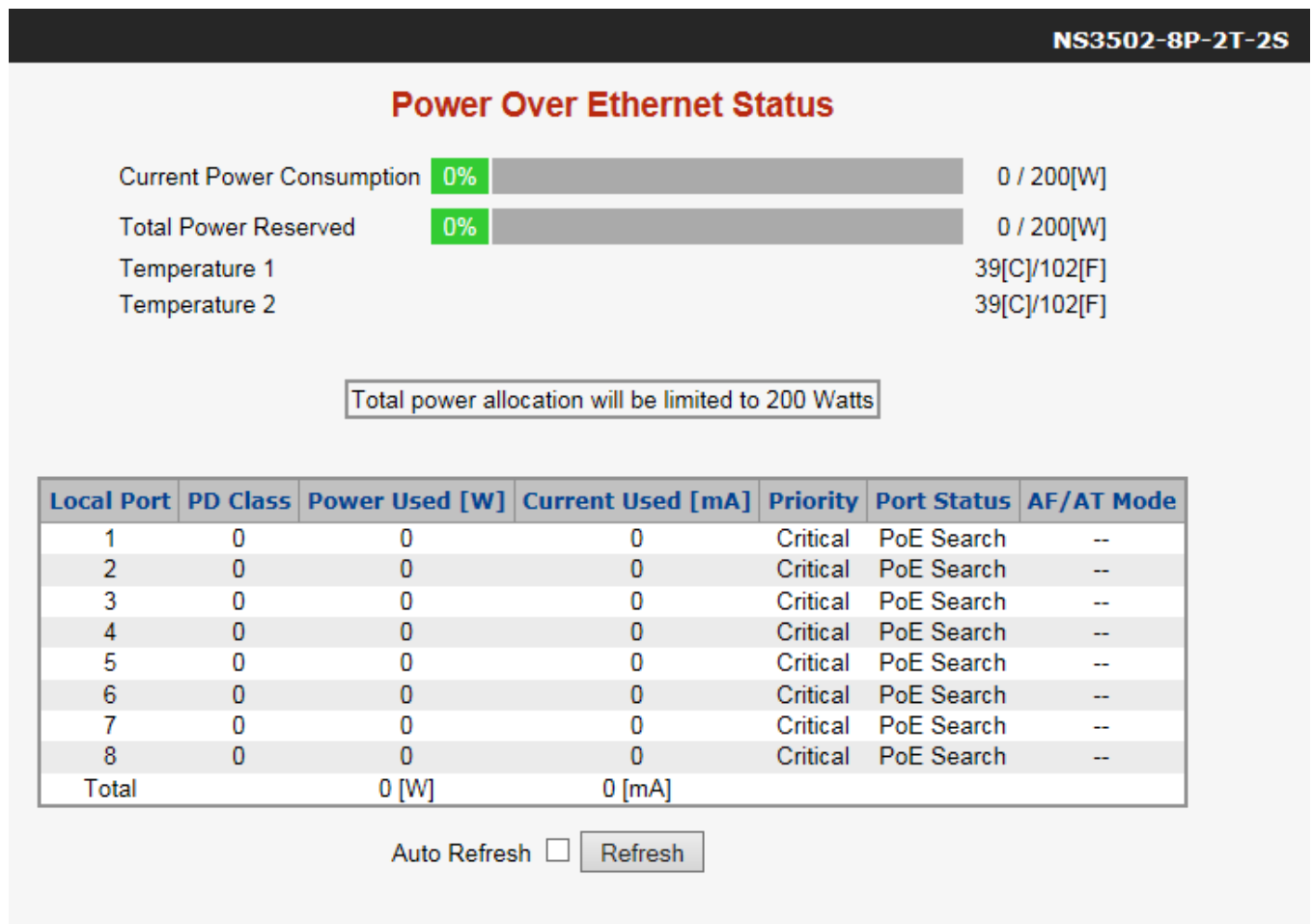








Figure 4-16-1: Power over Ethernet Status

4.16.1 Power over Ethernet Powered Device

 3~5 watts	<p>Voice over IP phones</p> <p>Enterprises can install PoE VoIP phones, ATA sand other Ethernet/non-Ethernet end-devices in the center where UPS is installed for un-interruptible power system and power control system.</p>
 6~12 watts	<p>Wireless LAN Access Points</p> <p>Access points can be installed at museums, sightseeing sites, airports, hotels, campuses, factories, warehouses, etc.</p>

 <p>10~12 watts</p>	<p>IP Surveillance</p> <p>IP cameras can be installed at enterprises, museums, campuses, hospitals, banks, etc. without worrying about electrical outlets.</p>
 <p>3~12 watts</p>	<p>PoE Splitter</p> <p>PoE Splitter split the PoE 56V DC over the Ethernet cable into 5/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.</p>
 <p>3~25 watts</p>	<p>High Power PoE Splitter</p> <p>High PoE Splitter split the PoE 56V DC over the Ethernet cable into 24/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.</p>
 <p>30 watts</p>	<p>High Power Speed Dome</p> <p>Its state-of-the-art design fits in various network environments like traffic centers, shopping malls, railway stations, warehouses, airports and production facilities for the most demanding outdoor surveillance applications. No electricians are needed to install AC sockets.</p>



Since the PoE port of NS3502-8P-2T-2S supports 54V DC PoE power output, please check and assure the powered device's (PD) acceptable DC power range is from 54V DC; otherwise, it will damage the PD.

4.16.2 System Configuration

In a power over Ethernet system, operating power is applied from a power source (PSU or power supply unit) over the LAN infrastructure to **powered devices (PDs)**, which are connected to ports. Under some conditions, the total output power required by PDs can exceed the maximum available power provided by the PSU. The system may come with a PSU capable of supplying less power than the total potential power consumption of all the PoE ports in the system. In order to maintain the activity of the majority of ports, power management is implemented.

The PSU input power consumption is monitored by measuring voltage and current. The input power consumption is equal to the system's aggregated power consumption. The power management concept allows all ports to be active and activates additional ports, as long as the aggregated power of the system is lower than the power level at which additional PDs cannot be connected. When this value is exceeded, ports will be deactivated, according to user-defined priorities. The power budget is managed according to the following user-definable parameters: maximum available power, ports priority, maximum allowable power per port.

Reserved Power determined by

There are five modes for configuring how the ports/PDs may reserve power and when to shut down ports.

■ Classification mode

In this mode, each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 and 30.8 watts.

Class	Usage	Range of maximum power used by the PD	Class Description
0	Default	0.44 to 12.95 watts	Classification unimplemented
1	Optional	0.44 to 3.84 watts	Very low power
2	Optional	3.84 to 6.49 watts	Low power
3	Optional	6.49 to 12.95 watts (or to 15.4 watts)	Mid power
4	Optional	12.95 to 25.50 watts (or to 30.8 watts)	High power



1. In this mode, the **Maximum Power fields** have no effect.
2. The PoE chip of PD69008 has been designed to Class level 0, meaning it will be assigned to 15.4 watts in AF mode and 30.8 watts in AT mode under the power limit classification. It is hardware limited.

■ **Allocation mode**

In this mode, the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields. The ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver.



In this mode, the port power will not be turned on if the PD requests more available power.

■ **LLDP mode**

In this mode, the ports of PoE power are managed and determined by LLDP Media Protocol.

4.16.3 Power Over Ethernet Configuration

This section allows the user to inspect and configure the current PoE configuration settings as [Figure 4-16-2](#) appears.

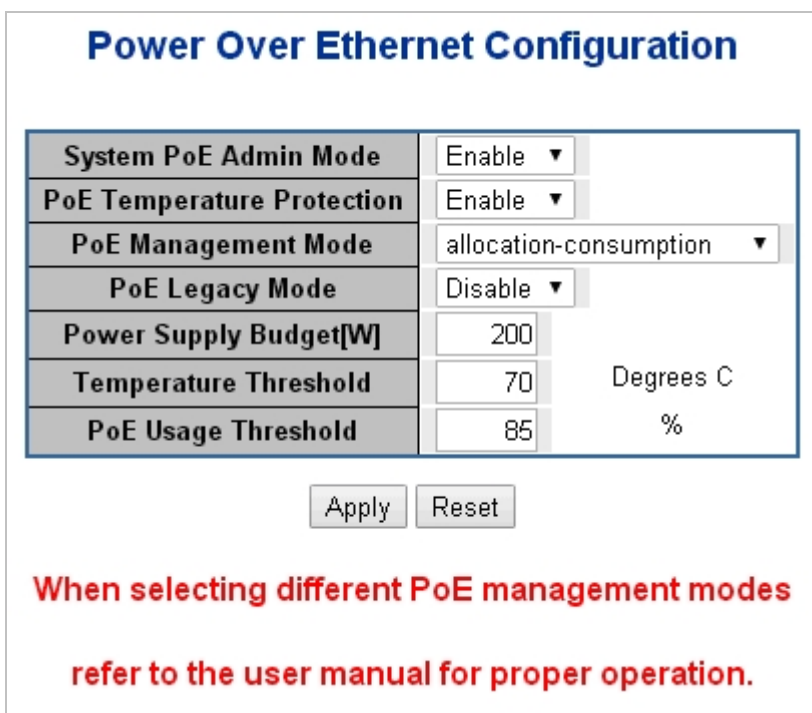



Figure 4-16-2: PoE Configuration Screenshot

The page includes the following fields:

Object	Description
• System PoE Admin Mode	Allows user to enable or disable PoE function. It will cause all of PoE ports to supply or not supply power.
• PoE Temperature Protection	Allows user to enable or disable PoE Temperature Protection.
• PoE Management Mode	There are Six modes for configuring how the ports/PDs may reserve power and when to shut down ports. ■ Class-Consumption mode: System offers PoE power according to PD real

	<p>power consumption.</p> <ul style="list-style-type: none"> ■ Class-Reserved-Power mode: System reserves PoE power to PD according to PoE class level. ■ Allocation-Consumption mode: System offers PoE power according to PD real power consumption. ■ Allocation-Reserved-Power mode: Users are allowed to assign how much PoE power for each port and system will reserve PoE power to PD. ■ LLDP-Consumption mode: System offers PoE power according to PD real power consumption. ■ LLDP-Reserved-Power mode: System reserves PoE power to PD according to LLDP configuration.
• Power Supply Budget [W]	Set limit value of the total PoE port providing power to the PDs. NS3502-8P-2T-2S available maximum value is 200 watts .
• Temperature Threshold	Allows setting over temperature protection threshold value. If its system temperature is over the threshold, the system will lower total PoE power budget automatically.
• PoE Usage Threshold	Allows setting how much PoE power budget could be limited.

Buttons

: Click to apply changes

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

PD Classifications

A PD may be classified by the PSE based on the classification information provided by the PD. The intent of PD classification is to provide information about the maximum power required by the PD during operation. However, to improve power management at the PSE, the PD provides a signature about **Class level**.

The PD is classified based on power. The classification of the PD is the maximum power that the PD will draw across all input voltages and operational modes.

A PD will return to Class 0 to 4 in accordance with the maximum power draw as specified by [Table 4-16-1](#).

Class	Usage	Range of maximum power used by the PD	Class Description
0	Default	12.95 watts (or to 15.4 watts for AF mode) 25.5 watts (or to 30.8 watts for AT mode)	Mid power or high power
1	Optional	0.44 to 3.84 watts	Very low power
2	Optional	3.84 to 6.49 watts	Low power
3	Optional	6.49 to 12.95 watts (or to 15.4 watts)	Mid power
4	Optional	12.95 to 25.50 watts (or to 30.8 watts)	High power

Table 4-16-1 Device Class

4.16.4 Port Sequential

This page allows the user to configure the PoE Ports started up interval time. The PoE Port will start up one by one as Figure 4-16-3 shows.

Port Sequential Power up Interval

Sequential Power up Option	Enable <input type="button" value="v"/>
Sequential Power up Interval	5 <input type="text"/> (1 ~ 30) seconds
Sequential Power up Port Option	By priority <input type="button" value="v"/>

Port Sequential Power up Interval

Sequential Power up Option	Enable <input type="button" value="v"/>
Sequential Power up Interval	5 <input type="text"/> (3 ~ 30) seconds
Sequential Power up Port Option	By port <input type="button" value="v"/>

Figure 4-16-3: PoE Port Sequential Power Up Interval Configuration Screenshot



The PoE port will start up after the whole system program has finished running.

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Sequential Power up Option 	Allows user to enable or disable Sequential Power up function.
<ul style="list-style-type: none"> • Sequential Power up Interval 	Allows user to configure the PoE Port Start Up interval time.
<ul style="list-style-type: none"> • Sequential Power up Port Option 	There are two modes for Starting Up the PoE Port By Port: The PoE Port will start up by following Port number. By Priority: The PoE Port will start up by following the PoE Priority.

Buttons

: Click to apply changes

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

4.16.5 Port Configuration

This section allows the user to inspect and configure the current PoE port settings as [Figure 4-16-4](#) shows.

Power Over Ethernet Configuration						
Port	PoE Mode	Schedule	AF/AT Mode	Priority	Power Allocation[W]	
*	<All>	<All>	<All>	<All>		36
1	Enable	Profile 1	802.3at	High		36
2	Enable	Profile 1	802.3at	High		36
3	Enable	Profile 1	802.3at	High		36
4	Enable	Profile 1	802.3at	High		36
5	Enable	Profile 1	802.3at	High		36
6	Enable	Profile 1	802.3at	High		36


Figure 4-16-4: Power over Ethernet Configuration Screenshot


The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • PoE Mode 	<p>There are three modes for PoE mode.</p> <ul style="list-style-type: none"> ■ Enable: enable PoE function.. ■ Disable: disable PoE function. ■ Schedule: enable PoE function in schedule mode.
<ul style="list-style-type: none"> • Schedule 	<p>Indicates the schedule profile mode. Possible profiles are:</p> <ul style="list-style-type: none"> ■ Profile1 ■ Profile2 ■ Profile3 ■ Profile4
<ul style="list-style-type: none"> • AF/AT Mode 	<p>Allows user to select 802.3at or 802.3af compatibility mode. The default value is 802.3at mode.</p> <p>This function will affect PoE power reservation under the power limit classification only. As in 802.3af mode, the system will reserve a maximum of 15.4W for PD that supports Class3 level. As in IEEE 802.3at mode, the system will reserve 30.8W for PD that supports Class4 level.</p> <p>From class1 to class3 level in the 802.3at mode, the PoE power will be reserved the same as that in 802.3af mode.</p>
<ul style="list-style-type: none"> • Priority 	<p>The Priority represents PoE ports priority. There are three levels of power priority named Low, High and Critical.</p>

	The priority is used in case the total power consumption is over the total power budget. In this case, the port with the lowest priority will be turned off, and power for the port of higher priority will be offered.
• Power Allocation	It can limit the port PoE supply wattage. Per port maximum value must be less than 30.8W watts ; total ports values must be less than the Power Reservation value. Once power overload is detected, the port will automatically shut down and continue to be in detection mode until Pad's power consumption is lower than the power limit value.

Buttons

: Click to apply changes

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

4.16.6 PoE Status

This page allows the user to inspect the total power consumption, total power reserved and current status for all PoE ports. The screen in [Figure 4-16-5](#) appears.

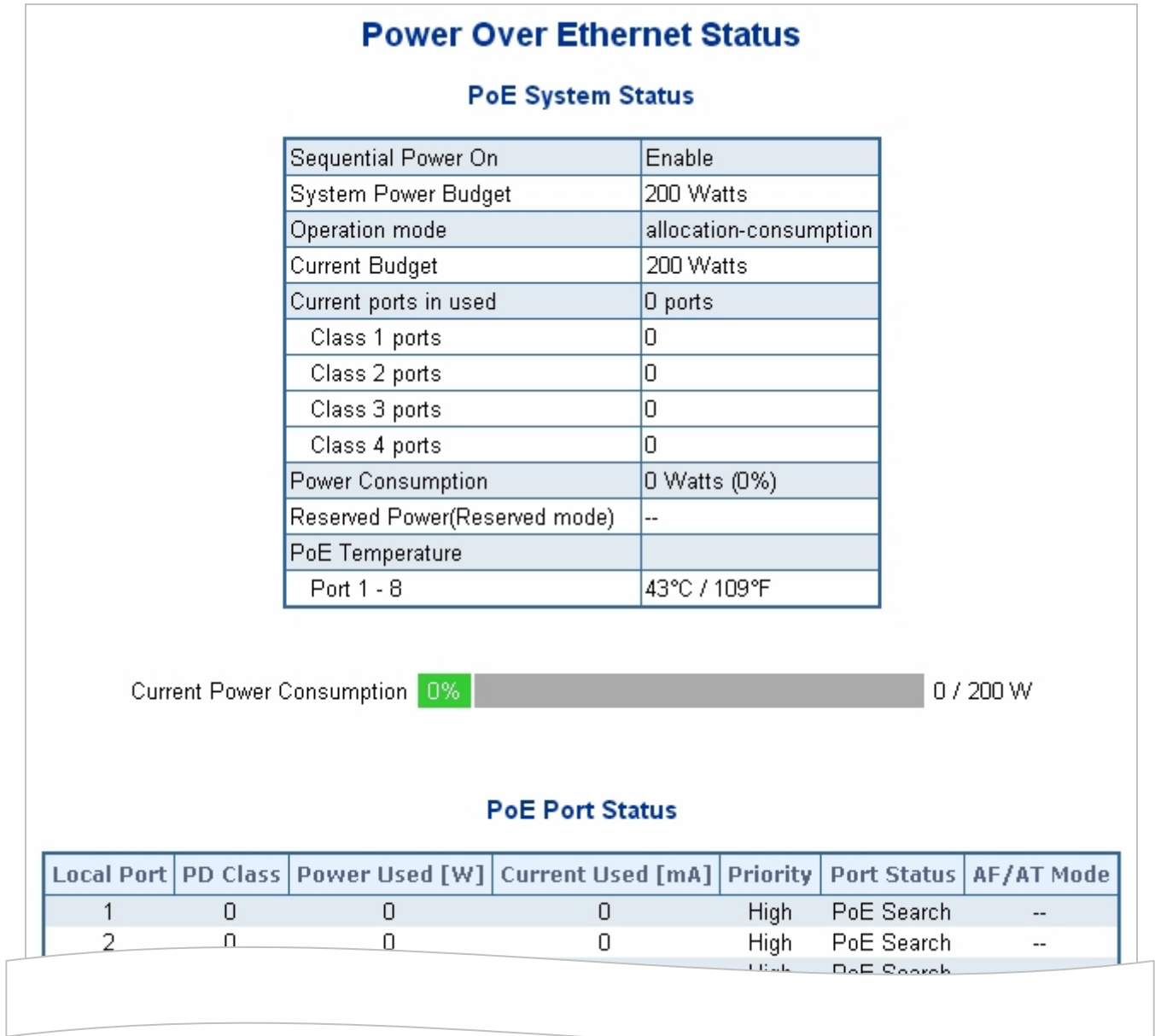


Figure 4-16-5:PoE Status Screenshot

The page includes the following fields:

Object	Description
• Sequential Power On	Displays the current sequential power on mode.
• System Power Budget	Displays the maximum PoE power budget.
• Operation Mode	Displays the current PoE operation mode.
• Current Budget	Displays the current maximum PoE budget.
• Current Ports in Use	Displays the current PoE ports in use.

• Class 1 ~ 4 ports	Displays the current PoE class 1 ~ 4 ports.
• Power Consumption	Displays the current power consumption (total watts and percentage)
• Reserved Power (Reserved mode)	Shows how much the total power is reserved for all PDs.
• PoE Temperature	Displays the current operating temperature of the first PoE chip unit.
• Current Power Consumption	Shows the total watts usage of Managed PoE Switch.
• Total Power Reserved	Shows how much the total power is reserved for all PDs.
• Temperature 1	Displays the current operating temperature of the first PoE chip unit.
• Temperature 2	Displays the current operating temperature of the second PoE chip unit.
• Local Port	This is the logical port number for this row.
• PD Class	Displays the class of the PD attached to the port, as established by the classification process. Class 0 is the default for PDs. The PD is powered based on PoE Class level if system is working in Classification mode. A PD will return Class to 0 to 4 in accordance with the maximum power drawn as specified by Table 4-16-1 .
• Power Used [W]	The Power Used shows how much power the PD currently is using.
• Current Used [mA]	The Power Used shows how much current the PD currently is using.
• Priority	The Priority shows the port's priority configured by the user.
• Port Status	The Port Status shows the port's status.
• AF / AT Mode	Displays per PoE port operating in 802.3af or 802.3at mode.
• Total	Shows the total power and current usage of all PDs.

Buttons

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

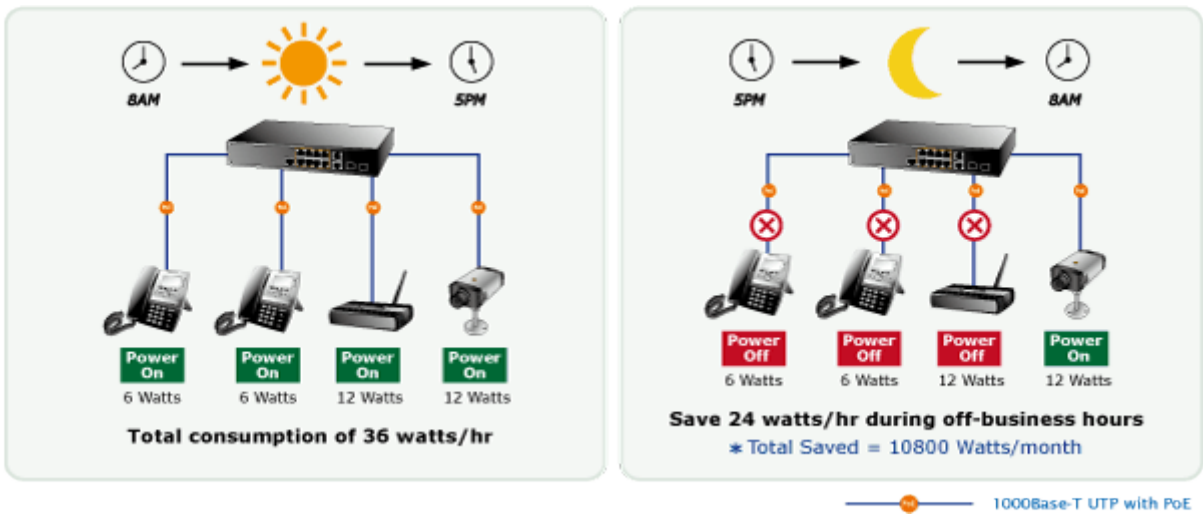
: Click to refresh the page immediately.

4.16.7 PoE Schedule

This page allows the user to define PoE schedule and schedule power recycle.

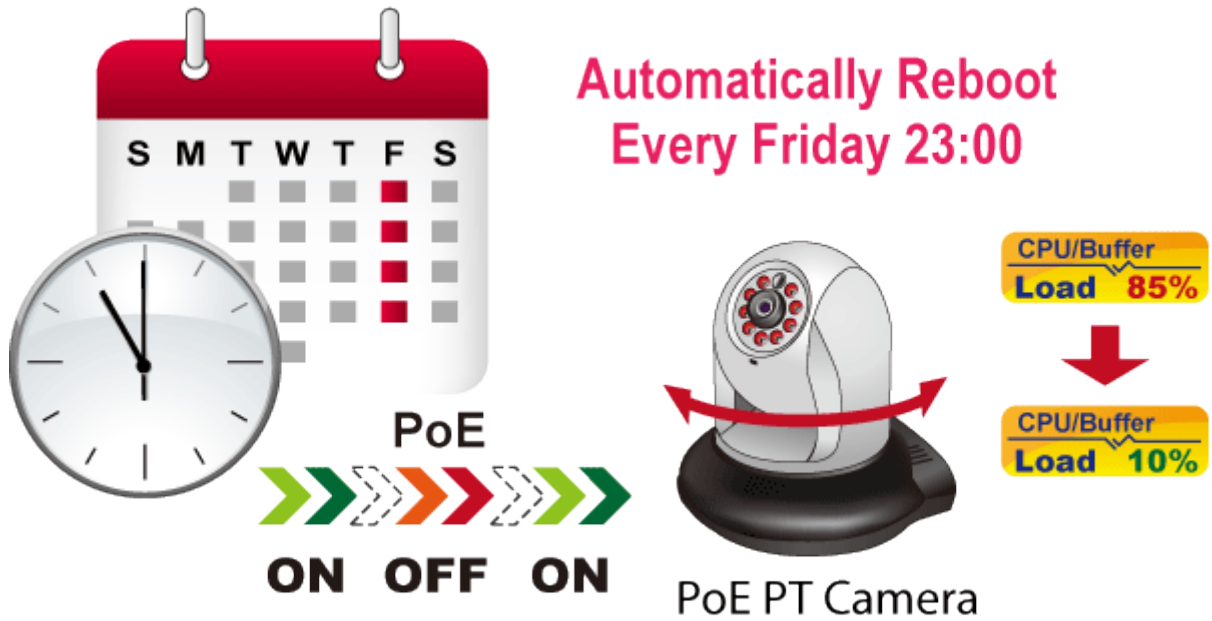
PoE Schedule

Besides being used as an IP Surveillance, the Managed PoE switch is certainly applicable to constructing any PoE network including VoIP and Wireless LAN. Under the trend of energy saving worldwide and contributing to the environmental protection on the Earth, the Managed PoE switch can effectively control the power supply besides its capability of giving high watts power. The **“PoE schedule”** function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is a powerful function to help SMBs or enterprises save power and budget.



Scheduled Power Recycling

The Managed PoE switch allows each of the connected PoE IP cameras to reboot in a specific time each week. Therefore, it will reduce the chance of IP camera crash resulting from buffer overflow.



The screen in Figure 4-16-6 appears.

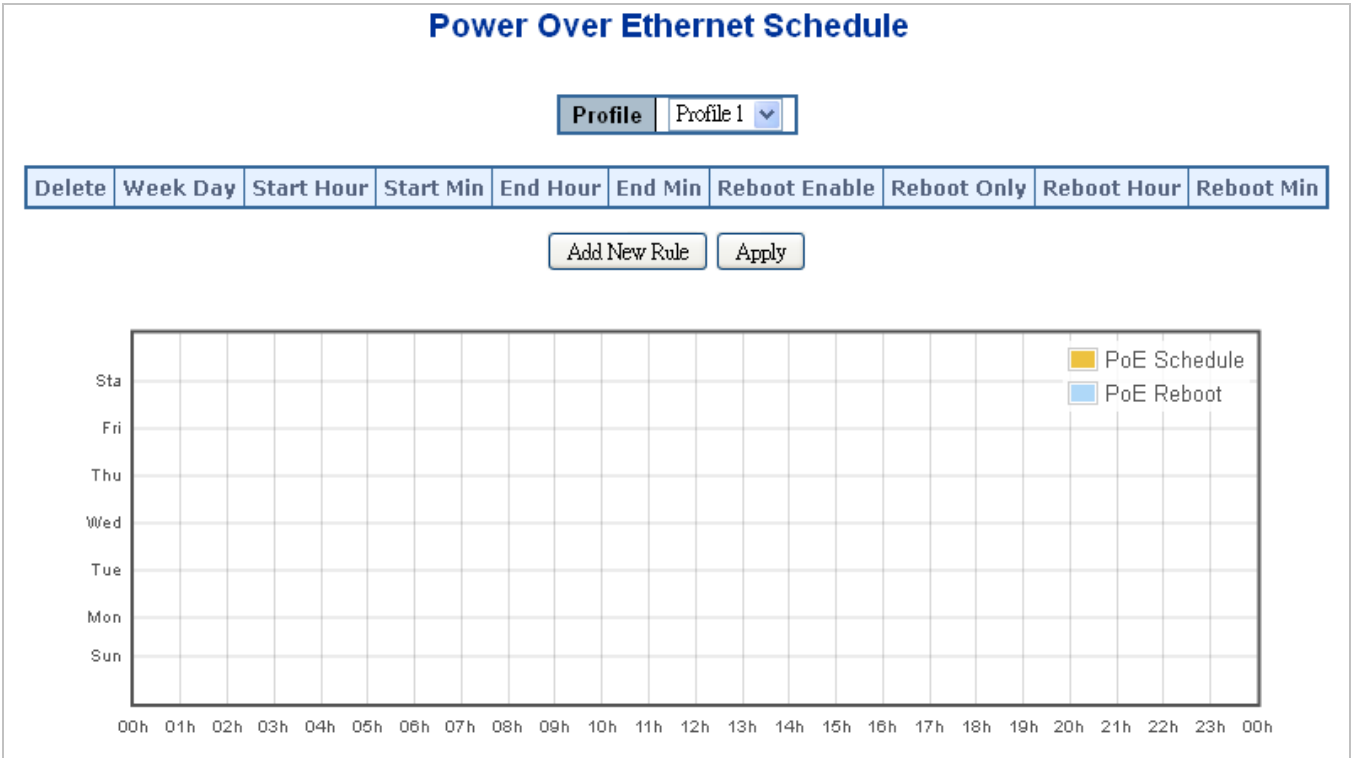


Figure 4-16-6: PoE Schedule Screenshot

Please press **Add New Rule** button to start setting PoE Schedule function. You have to set PoE schedule via profile and then go back to PoE Port Configuration, and select “**Schedule**” mode from per port “**PoE Mode**” option and then you can indicate which schedule profile could be apply to the PoE port.

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Profile 	Set the schedule profile mode. Possible profiles are: Profile1 Profile2 Profile3 Profile4
<ul style="list-style-type: none"> Week Day 	Allows user to set week day for defining PoE function (should be enabled on the day).
<ul style="list-style-type: none"> Start Hour 	Allows user to set at what hour PoE function starts when enabled.
<ul style="list-style-type: none"> Start Min 	Allows user to set at what minute PoE function starts when enabled.
<ul style="list-style-type: none"> End Hour 	Allows user to set at what hour PoE function ends when disabled.
<ul style="list-style-type: none"> End Min 	Allows user to set at what minute PoE function ends when disabled.
<ul style="list-style-type: none"> Reboot Enable 	Allows user to enable or disable whole PoE port reboot by PoE reboot schedule. Please note that if you want PoE schedule and PoE reboot schedule to work at the same time, please use this function. Don't use Reboot Only function. This function offers administrator to reboot PoE device at an indicated time if

	administrator has this kind of requirement.
<ul style="list-style-type: none"> • Reboot Only 	Allows user to reboot PoE function by PoE reboot schedule. Please note that if administrator enables this function, PoE schedule will not set time to profile. This function is only for PoE port reset at the indicated time.
<ul style="list-style-type: none"> • Reboot Hour 	Allows user to set at what hour PoE reboots. This function is only for PoE reboot schedule.
<ul style="list-style-type: none"> • Reboot Min 	Allows user to set at what minute PoE reboots. This function is only for PoE reboot schedule.

Buttons

Add New Rule: click to add new rule.

Apply: Click to apply changes

Delete: Click to delete the entry.

4.16.8 LLDP PoE Neighbours

This page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each port on which an LLDP PoE neighbor is detected. The columns hold the following information: The screen in Figure 4-16-7 appears.



Figure 4-16-7: LLDP PoE Neighbour Screenshot

Please note that administrator has to enable LLDP port from LLDP configuration; please refer to the following example (The screen in Figure 4-16-8 appears.). To enable LLDP function from port1 to port3, administrator has to plug a PD that supports PoE LLDP function, and then administrator is going to see the PoE information of the PD from LLDP.

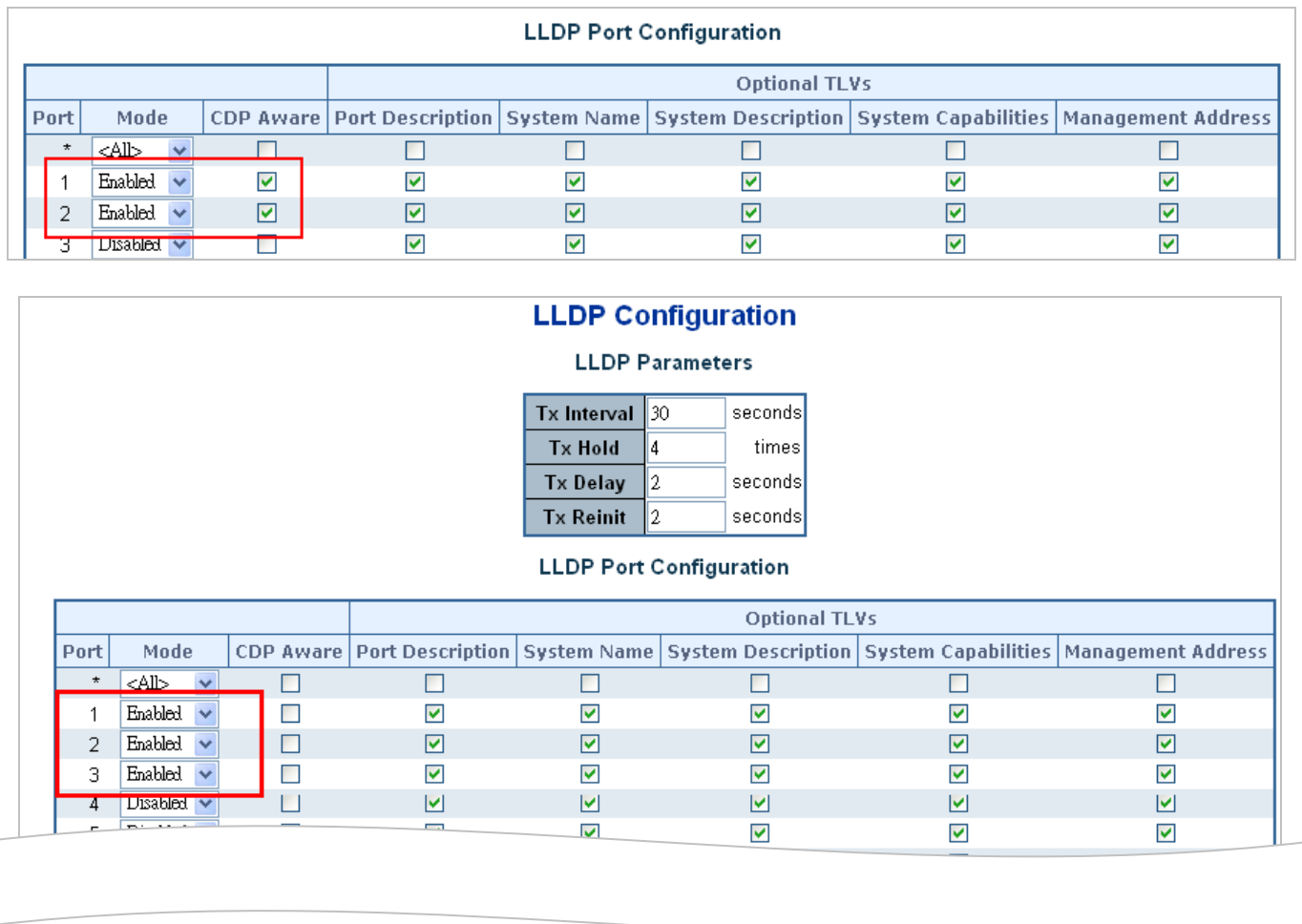


Figure 4-16-8: LLDP Configuration Screenshot

4.17 Loop Protection

This chapter describes enabling loop protection function that provides loop protection to prevent broadcast loops in Managed Switch.

4.17.1 Configuration

This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well as screen in [Figure 4-17-1](#) appears.

Loop Protection Configuration

General Settings

Global Configuration			
Enable Loop Protection	Disable ▾		
Transmission Time	5	seconds	
Shutdown Time	180	seconds	

Port Configuration

Port	Enable	Action	Tx Mode
*	<input type="checkbox"/>	<All> ▾	<All> ▾
1	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
2	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
3	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
4	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
5	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
6	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
7	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
8	<input type="checkbox"/>	Shutdown Port ▾	Enable ▾

Figure 4-17-1: Loop Protection Configuration Page Screenshot

The page includes the following fields:

General Settings


Object	Description
<ul style="list-style-type: none"> • Enable Loop Protection 	Controls whether loop protection 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.

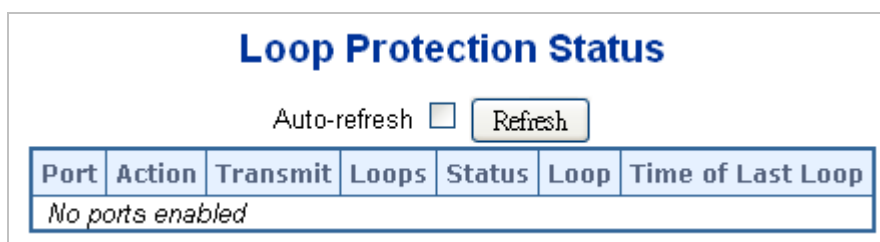
Buttons

: Click to apply changes

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

4.17.2 Loop Protection Status

This page displays the loop protection port status of the switch; screen in [Figure 4-17-2](#) appears.



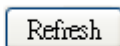
Loop Protection Status						
Auto-refresh <input type="checkbox"/> 						
Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
<i>No ports enabled</i>						

Figure 4-17-2: Loop Protection Status Screenshot

The page includes the following fields:

Object	Description
• Port	The Managed 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

: Click to refresh the page immediately.

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

4.18 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 groups 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).

4.18.1 RMON Alarm Configuration

Configure RMON Alarm table on this page. The entry index key is **ID**; screen in [Figure 4-18-1](#) appears.

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	Indicates the particular variable to be sampled; the possible variables are: <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

	<p>protocol.</p> <ul style="list-style-type: none"> ■ InNUcastPkts: The number of broadcast 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 contains errors preventing them from being deliverable to a higher-layer protocol. ■ InUnknownProtos: the number of the inbound packets that is 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 requests to transmit. ■ OutNUcastPkts: The number of broadcast and multi-cast packets that requests to transmit. ■ OutDiscards: The number of outbound packets that is discarded even the packets are normal. ■ OutErrors: The number of outbound packets that could not be transmitted because of errors. ■ OutQLen: The length of the output packet queue (in packets).
• Sample Type	<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	<p>The value of the statistic during the last sampling period.</p>
• 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	<p>Rising threshold value (-2147483648-2147483647).</p>
• Rising Index	<p>Rising event index (1-65535).</p>
• Falling Threshold	<p>Falling threshold value (-2147483648-2147483647)</p>
• Falling Index	<p>Falling event index (1-65535).</p>

Buttons

Add New Entry: Click to add a new community entry.

Apply: Click to apply changes

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

4.18.2 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 4-18-2](#) appears.



Figure 4-18-2: RMON Alarm 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

: Click to refresh the page immediately.

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

: 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.

4.18.3 RMON Event Configuration

Configure RMON Event table on this page. The entry index key is **ID**; screen in [Figure 4-18-3](#) appears.

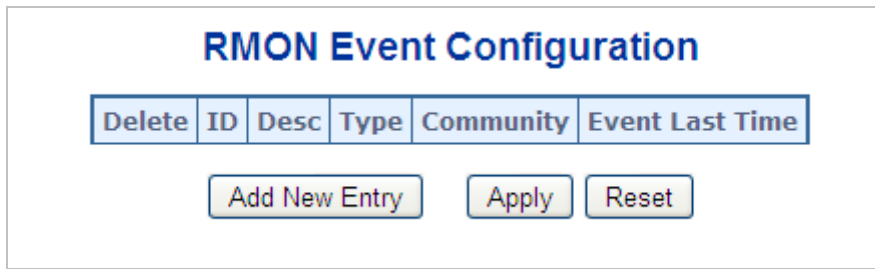


Figure 4-18-4: RMON Event Configuration Page Screenshot

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.

Apply: Click to apply changes

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

4.18.4 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 4-18-5](#) appears.

RMON Event Overview

Auto-refresh Refresh << >>

Start from Control Index and Sample Index with entries per page.

Event Index	LogIndex	LogTime	LogDescription
<i>No more entries</i>			

Figure 4-18-5: 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.
• Longtime	Indicates Event log time.
• Log Description	Indicates the Event description.

Buttons

: Click to refresh the page immediately.

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

: 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.

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

4.18.5 RMON History Configuration

Configure RMON History table on this page. The entry index key is **ID**; screen in [Figure 4-18-6](#) appears.

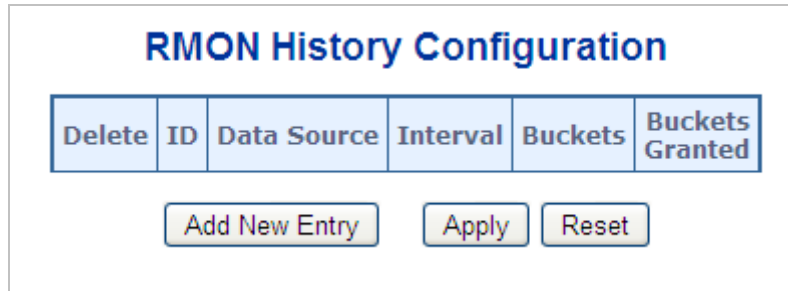


Figure 4-18-6: RMON History Configuration Page Screenshot

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.
• Data Source	Indicates the port ID which wants to be monitored.
• Interval	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
• Buckets	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.
• Buckets Granted	The number of data will be saved in the RMON.

Buttons

Add New Entry: Click to add a new community entry.

Apply: Click to apply changes

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

4.18.6 RMON History Status

This page provides an detail of RMON history entries; screen in [Figure 4-18-7](#) appears.

RMON History Overview

Auto-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
<i>No more entries</i>														


Figure 4-18-7: 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 value of sysUpTime at the start of the interval over which this sample was measured.
• Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
• Octets	The total number of octets of data (including those in bad packets) received on the network.
• Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
• Broadcast	The total number of good packets received that were directed to the broadcast address.
• Multicast	The total number of good packets received that were directed to a multicast address.
CRC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
• Undersize	The total number of packets received that were less than 64 octets.
• Oversize	The total number of packets received that were longer than 1518 octets.
• Frag.	The number of frames whose size is less than 64 octets received with invalid CRC.
• Jabb.	The number of frames whose size is larger than 64 octets received with invalid CRC.
• Coll.	The best estimate of the total number of collisions in this Ethernet segment.


<ul style="list-style-type: none"> • Utilization 	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
--	---

Buttons

: Click to refresh the page immediately.

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

: Updates the table, starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index

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

4.18.7 RMON Statistics Configuration

Configure RMON Statistics table on this page. The entry index key is **ID**; screen in [Figure 4-18-8](#) appears.





Figure 4-18-8: RMON Statistics 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.

Buttons

: Click to add a new community entry.

: Click to apply changes

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

4.18.8 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 4-18-9](#) appears.

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 4-18-9: RMON Statistics Status Overview Page Screenshot

The page includes the following fields:


Object	Description
• ID	Indicates the index of Statistics entry.
• Data Source (ifIndex)	The port ID which wants to be monitored.
• Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
• Octets	The total number of octets of data (including those in bad packets) received on the network.
• Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
• Broadcast	The total number of good packets received that were directed to the broadcast address.
• Multicast	The total number of good packets received that were directed to a multicast address.
• CRC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.
• Undersize	The total number of packets received that were less than 64 octets.
• Oversize	The total number of packets received that were longer than 1518 octets.
• Frag.	The number of frames whose size is less than 64 octets received with invalid CRC.
• Jabb.	The number of frames whose size is larger than 64 octets received with invalid CRC.


• Coll.	The best estimate of the total number of collisions in this Ethernet segment.
• 64 Bytes	The total number of packets (including bad packets) received that were 64 octets in length.
• 65~127	The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
• 128~255	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
• 256~511	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
• 512~1023	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
• 1024~1518	The total number of packets (including bad packets) received that were between 1024 to 1518 octets in length.

Buttons

: Click to refresh the page immediately.

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

: 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.

5. SWITCH OPERATION

5.1 Address Table

The **Managed Switch** is implemented with an address table. This address table is composed of many entries. Each entry is used to store the address information of some nodes in the network, including MAC address, port no, etc. This information 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 look up the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, 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 a 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 and do the complete error checking before transmission. Therefore, no error packets occur; 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 provided 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. However, the switch is most commonly used to segment existence hubs, which nearly always improves the overall performance. An Ethernet switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using the 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 in 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 Fforward**"; 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 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 both connected devices are 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 issues. If the Managed Switch is not functioning properly, make sure the Managed Switch was set up according to instructions in this manual.

■ The Link LED is not lit.

Solution:

Check the cable connection and remove duplex mode of the Managed Switch.

■ Some stations cannot talk to other stations located on the other port.

Solution:

Please check the VLAN settings, trunk settings, or port enabled/disabled status.

■ Performance is bad.

Solution:

Check the full duplex status of the Managed Switch. If the Managed Switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

■ Why the Switch doesn't connect to the network.

Solution:

1. Check the LNK/ACT LED on the switch.
2. Try another port on the Switch.
3. Make sure the cable is installed properly.
4. Make sure the cable is the right type.
5. Turn off the power. After a while, turn on power again.

■ 1000BASE-T port link 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.

■ Switch does not power up.

Solution:

1. AC power cord is not inserted or faulty.
2. Check that the AC power cord is inserted correctly.
3. Replace the power cord if the cord is inserted correctly; check that the AC power source is working by connecting a different device in place of the switch.
4. If that device works, refer to the next step.
5. If that device does not work, check the AC power.

APPENDIX A: Networking Connection

A.1 Switch's Data RJ45 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-

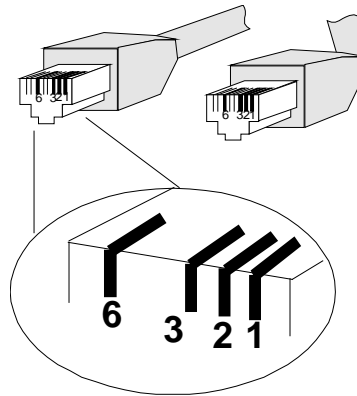
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100BASE-TX

When connecting your Switch to another Fast Ethernet 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 RJ45 receptacle/ connector and their pin assignments:

RJ45 Connector pin assignment		
PIN NO	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, RJ45 pin assignment



The standard RJ45 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-through cable and crossover cable connection:

Straight Cable		SIDE 1	SIDE 2							
1	2	3	4	5	6	7	8	SIDE 1	1 = White / Orange	1 = White / Orange
1	2	3	4	5	6	7	8		2 = Orange	2 = Orange
1	2	3	4	5	6	7	8	SIDE 2	3 = White / Green	3 = White / Green
1	2	3	4	5	6	7	8		4 = Blue	4 = Blue
1	2	3	4	5	6	7	8	SIDE 1	5 = White / Blue	5 = White / Blue
1	2	3	4	5	6	7	8		6 = Green	6 = Green
1	2	3	4	5	6	7	8	SIDE 2	7 = White / Brown	7 = White / Brown
1	2	3	4	5	6	7	8		8 = Brown	8 = Brown
Crossover Cable		SIDE 1	SIDE 2							
1	2	3	4	5	6	7	8	SIDE 1	1 = White / Orange	1 = White / Green
1	2	3	4	5	6	7	8		2 = Orange	2 = Green
1	2	3	4	5	6	7	8	SIDE 2	3 = White / Green	3 = White / Orange
1	2	3	4	5	6	7	8		4 = Blue	4 = Blue
1	2	3	4	5	6	7	8	SIDE 1	5 = White / Blue	5 = White / Blue
1	2	3	4	5	6	7	8		6 = Green	6 = Orange
1	2	3	4	5	6	7	8	SIDE 2	7 = White / Brown	7 = White / Brown
1	2	3	4	5	6	7	8		8 = Brown	8 = Brown

Figure A-1: Straight-through and Crossover Cable

Please make sure your connected cables are with the 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 **A**ccess **C**ontrol **E**ntry. It describes access permission associated with a particular ACE ID.

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

ACL

ACL is an acronym for **A**ccess **C**ontrol **L**ist. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

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

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

There are 3 web pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that policy can be associated with a group of ports under the "Ports" web page. There are number of parameters that can be configured with an ACE. Read the web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Port 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". 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: On this page, you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1 to 1024K packets per second. Under "Ports" and "Access Control List", 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 802.1x 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 an 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 switching that is done bidirectional in both ends of a protection group, as defined in G.8031.

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(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. 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.

DSCP

DSCP is an acronym for **D**ifferentiated **S**ervices **C**ode **P**oint. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

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

IGMP snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

H

HTTP

HTTP is an acronym for **H**ypertext **T**ransfer **P**rotocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested web page. The other main standard that controls how the World Wide Web works is HTML, which covers how web pages are formatted and displayed.

Any Web server machine contains, in addition to the web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for **H**ypertext **T**ransfer **P**rotocol over **S**ecure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for **I**nternet **C**ontrol **M**essage **P**rotocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for **I**nternet **G**roup **M**anagement **P**rotocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for 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 a internet network.

IP is a "best effort" system, which means that no packet of information sent over it is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an 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.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol allows bundling several physical ports together to form a single logical port.

LLDP

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 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).

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 a switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address 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 **M**ulticast **L**istener **D**iscovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

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 Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for **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

OAM

OAM is an acronym for **O**peration **A**dministration and **M**aintenance. It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.

Optional TLVs.

An LLDP frame contains multiple TLVs. For some TLVs it is configurable if the switch includes the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLV 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 **P**owered **D**evice. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that 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 **P**ost **O**ffice **P**rotocol 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, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

PTP

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for **Q**oS **C**ontrol **E**ntry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for **Q**oS **C**ontrol **L**ist. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for **Q**uality **o**f **S**ervice. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

R

RARP

RARP is an acronym for **R**everse **A**ddress **R**esolution **P**rotocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for **R**emote **A**uthentication **D**ial In **U**ser **S**ervice. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network

service.

RDI

RDI is an acronym for **R**emote **D**efect **I**ndication. It is an OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

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 **S**ecure **H**ash **A**lgorithm. 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 **S**imple **M**ail **T**ransfer **P**rotocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The 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 **S**imple **N**etwork **M**anagement **P**rotocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for **S**imple **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack **P**rotocol using **R**outing **T**echnology. 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 **S**et **I**dentifier 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 **S**ecure **S**Hell. 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 **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for **T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for **T**ransmission **C**ontrol **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for **T**eletype **N**etwork. 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 provides directory service and security features.

Toss

Toss is an acronym for **T**ype **o**f **S**ervice. It is implemented as the IPv4 Toss priority control. It is fully decoded to determine the priority from the 6-bit Toss field in the IP header. The most significant 6 bits of the Toss 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 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.

V

VLAN

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 **W**ired **E**quivalent **P**rivacy. 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).

Wi-Fi

Wi-Fi is an acronym for **W**ireless **F**idelity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for **W**i-Fi **P**rotected **A**ccess. 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 **W**i-Fi **P**rotected **A**ccess - **P**re **S**hared **K**ey. 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 **W**i-Fi **P**rotected **A**ccess - 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 **W**i-Fi **P**rotected **S**etup. 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 **W**eighted **R**andom **E**arly **D**etection. 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 **W**ait **T**o **R**estore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.