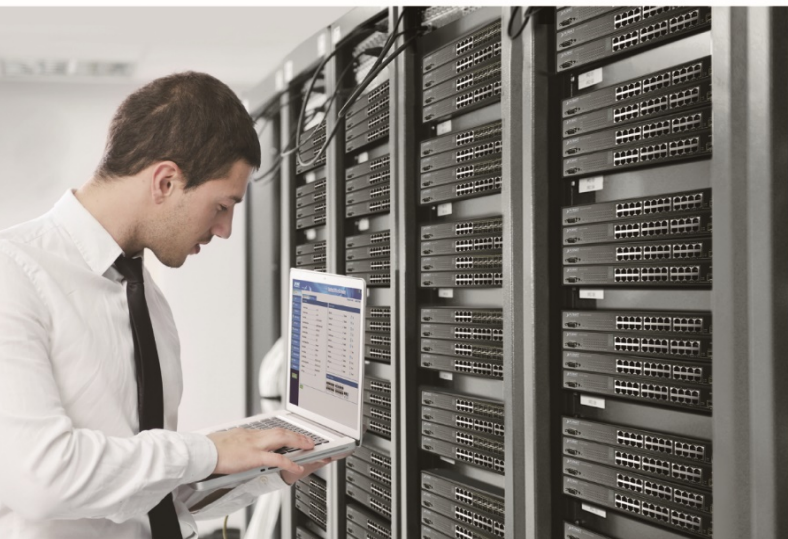


User's Manual

L2+ Stackable Managed Gigabit Ethernet Switch with 10GbE Uplink

▶ SGS-5240 Switch Series



Trademarks

Copyright © PLANET Technology Corp. 2020.

Contents are subject to revision without prior notice.

PLANET is a registered trademark of PLANET Technology Corp. All other trademarks belong to their respective owners.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Instruction manual, may cause harmful interference 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.

CE Mark Warning

This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

Energy Saving Note of the Device

This power required device does not support Standby mode operation. For energy saving, please remove the power cable to disconnect the device from the power circuit. In view of saving the energy and reducing the unnecessary power consumption, it is strongly suggested to remove the power connection for the device if this device is not intended to be active.

WEEE Warning



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

PLANET SGS-5240 Series User's Manual

Models: SGS-5240-24T4X, SGS-5240-24P4X, SGS-5240-20S4C4XR, SGS-5240-48T4X

Revision: 1.0 (September, 2020)

Part No: EM-SGS-5240 series_v1.0

TABLE OF CONTENTS

1. INTRODUCTION	11
1.1 Packet Contents	11
1.2 Product Description	12
1.3 How to Use This Manual	17
1.4 Product Features	18
1.5 Product Specifications	21
2. INSTALLATION	26
2.1 Hardware Description	26
2.1.1 Switch Front Panel	26
2.1.2 LED Indications	28
2.1.3 Switch Rear Panel	28
2.2 Installing the Switch.....	30
2.2.1 Desktop Installation	30
2.2.2 Rack Mounting.....	31
2.2.3 Installing the SFP/SFP+ Transceiver.....	32
3. SWITCH MANAGEMENT	35
3.1 Requirements	35
3.2 Management Access Overview.....	36
3.3 Administration Console.....	37
3.4 Web Management.....	38
3.5 SNMP-based Network Management	39
3.6 PLANET Smart Discovery Utility	39
4. WEB CONFIGURATION	41
4.1 System Information.....	43
4.1.1 System Info	43
4.1.2 System Description	43
4.1.3 User Accounts	44
4.2 Switch Management.....	45
4.2.1 Jumbo Frame	45
4.2.2 Interface.....	45
4.2.2.1 Port.....	45
4.2.2.2 sFlow	46
4.2.2.3 Transceiver.....	48

4.2.2.4 Cable Test	49
4.2.2.5 Green Ethernet.....	50
4.2.2.6 Port Isolate	50
4.2.3 Statistics.....	51
4.2.3.1 Current Statistics	51
4.2.3.2 History Management	51
4.2.3.3 History Info	52
4.2.4 VLAN.....	52
4.2.4.1 VLAN Overview	52
4.2.4.2 Static VLAN.....	57
4.2.4.3 GVRP	59
4.2.4.4 Protocol VLAN.....	59
4.2.4.5 IP Subnet VLAN	61
4.2.4.6 MAC-Based VLAN.....	62
4.2.4.7 VLAN Translation	63
4.2.4.8 QinQ.....	64
4.2.4.9 Voice VLAN	66
4.2.4.10 L2PT.....	69
4.2.5 MAC Address	70
4.2.5.1 Dynamic MAC Learning.....	70
4.2.5.2 Static Mac Setting	72
4.2.5.3 MAC Notification.....	73
4.2.6 Port Mirror	74
4.2.6.1 Local Port Mirror.....	74
4.2.6.2 RSPAN	74
4.2.7 Static Link Aggregation	76
4.2.7.1 Static Group	76
4.2.7.2 Static Group Member	76
4.2.7.3 Static Trunk Management.....	77
4.2.8 LACP.....	78
4.2.8.1 Group Member	78
4.2.8.2 Group Link Configuration.....	79
4.2.8.3 Group LACP Configuration.....	79
4.2.8.4 Counter.....	80
4.2.8.5 Show Dynamic Group Member	80
4.2.9 Trunk Group Load Balance.....	81
4.2.10 Spanning Tree Protocol	82
4.2.10.1 Theory	82
4.2.10.2 STP Global Setting.....	88
4.2.10.3 STP-RSTP.....	89
4.2.10.4 MSTP	95
4.2.10.5 Loopback Detection.....	100
4.2.11 IGMP Snooping	101
4.2.11.1 Global Setting	105
4.2.11.2 Current Multicast Router	106
4.2.11.3 Static Multicast Router.....	107
4.2.11.4 Static Member.....	108

4.2.11.5 VLAN Information	109
4.2.11.6 Configure Interface	112
4.2.11.7 Forwarding Entry	113
4.2.11.8 Query Statistics.....	114
4.2.11.9 VLAN Statistics.....	115
4.2.11.10 Port Statistics.....	116
4.2.11.11 Group Statistics.....	117
4.2.12 IGMP Filtering and Throttling	118
4.2.12.1 Global Setting.....	118
4.2.12.2 Filter Profile	118
4.2.12.3 Filter Range.....	119
4.2.11.4 Configure Filter Interface	120
4.2.13 MLD Snooping	121
4.2.13.1 Global Setting.....	121
4.2.13.2 Immediate Leave Status.....	122
4.2.13.3 Current Multicast Router.....	123
4.2.13.4 Static Multicast Router.....	123
4.2.13.5 Current Member	124
4.2.13.6 Static Member	124
4.2.13.7 Group Information.....	125
4.2.13.8 Statistics	126
4.2.14 MVR For IPv4	129
4.2.14.1 Configure Global	130
4.2.14.2 Configure Domain.....	131
4.2.14.3 Show Configure Profile.....	132
4.2.14.4 Add Configure Profile.....	132
4.2.14.5 Show Associate Profile	133
4.2.14.6 Add Associate Profile.....	133
4.2.14.7 Configure Interface.....	134
4.2.14.8 Show Static Group Member	135
4.2.14.9 Add Static Group Member	135
4.2.14.10 Show Member	136
4.2.14.11 Show Query Statistics.....	136
4.2.14.12 Show VLAN Statistics.....	138
4.2.14.13 Show Port Statistics.....	139
4.2.14.14 Show Group Statistics	140
4.2.15 MVR For IPv6	141
4.2.15.1 Configure Global	141
4.2.15.2 Configure Domain.....	142
4.2.15.3 Show Configure Profile.....	143
4.2.15.4 Add Configure Profile.....	144
4.2.15.5 Show Associate Profile	144
4.2.15.6 Add Associate Profile.....	145
4.2.15.7 Configure Interface.....	145
4.2.15.8 Show Static Group Member	146
4.2.15.9 Add Static Group Member	146
4.2.15.10 Show Member	147

4.2.15.11 Show Query Statistics.....	147
4.2.15.12 Show VLAN Statistics.....	149
4.2.15.13 Show Port Statistics.....	150
4.2.15.14 Show Group Statistics	151
4.2.16 LLDP	153
4.2.16.1 Global Configuration.....	153
4.2.16.2 Interface Configuration	154
4.2.16.3 Civil Address Type	156
4.2.16.4 Local Information	157
4.2.16.5 Peer Information	159
4.2.16.6 Statistics	164
4.2.17 ERPS.....	165
4.2.17.1 Global Configuration.....	166
4.2.17.2 Domain Configuration.....	166
4.2.17.3 Statistics	170
4.2.18 Loopback Detection	171
4.2.18.1 Global Configuration.....	171
4.2.18.2 Interface Configuration	172
4.2.19 UDLD	173
4.2.19.1 Global Configuration.....	173
4.2.19.2 Interface Configuration	174
4.2.19.3 Neighbor Info.....	175
4.2.20 Rate Limit	176
4.2.21 Storm Control	177
4.2.22 Stacking.....	178
4.2.22.1 Global Configuration.....	178
4.2.22.2 Master Configuration	178
4.2.23 Pepo.....	179
4.2.23.1 Global Configuration.....	179
4.2.23.2 Interface Configuration	179
4.2.23.3 Statistics	179
4.3 Route Management	180
4.3.1 IPv4 Interface Configuration.....	180
4.3.2 IPv6 Interface Configuration.....	181
4.3.2.1 Global Configuration.....	181
4.3.2.2 Interface Configuration	181
4.3.2.3 RA-Guard	183
4.3.2.4 Address Configuration	184
4.3.2.5 Neighbor List	185
4.3.2.6 Statistics	185
4.3.2.7 MTU.....	186
4.3.3 ARP	186
4.3.3.1 Global Configuration.....	186
4.3.3.2 Proxy ARP	186
4.3.3.3 Static Arp	187
4.3.3.4 ARP Address List.....	187

4.3.4 Routing Table.....	188
4.4 ACL	189
4.4.1 ACL Configuration.....	189
4.4.2 Rule Configuration	190
Standard Ipv4 Acl	190
Extended Ipv4 Acl.....	191
Standard Ipv6 Cal.....	192
Extended Ipv6 Acl.....	193
Mac Acl.....	194
Arp Acl.....	194
4.4.3 Bind Interface.....	196
4.5 CoS	197
4.6 Qu's.....	198
4.6.1 Egress Queue	198
4.6.2 Trust Mode	199
4.6.3 Qu's Map	199
DHCP to PHB/DP	200
CoS to PHB/DP	200
PHB/DP to CoS	201
IP Precedence to PHB/DP.....	203
TCP/UDP Port to DSCP	204
PHB to Queue	204
4.6.4 Class.....	205
4.6.5 Class Match.....	206
4.6.6 Policy.....	207
4.6.7 Policy Map.....	208
4.6.8 Bind Interface.....	209
4.7 Security	210
4.7.1 AAA.....	210
4.7.1.1 Global Configuration.....	214
4.7.1.2 Server Configuration.....	215
4.7.1.3 Server List	215
4.7.1.4 Accounting Strategy.....	216
4.7.1.5 Interface Accounting.....	216
4.7.1.6 Authorization Strategy	217
4.7.1.7 Authorization configuration	217
4.7.2 Web Authentication	218
4.7.2.1 Global Configuration.....	218
4.7.2.2 Interface Configuration	218
4.7.2.3 Host List	218
4.7.3 802.1X	219
4.7.3.1 Global Configuration.....	219
4.7.3.2 Interface Configuration	220
4.7.3.3 Statistics	220
4.7.4 MAC Authentication	221

4.7.4.1 Global Configuration.....	221
4.7.4.2 Interface Configuration	222
4.7.4.3 MAC Filter	222
4.7.4.4 MAC Authentication Information	223
4.7.5 HTTPS.....	223
4.7.5.1 Global Configuration.....	223
4.7.5.2 Update Certificate.....	223
4.7.6 SSH.....	224
4.7.6.1 Global Configuration.....	224
4.7.6.2 Key of Switch.....	224
4.7.6.3 Key of User.....	225
4.7.7 Port Security	226
4.7.8 DAI – Dynamic ARP Inspection	227
4.7.8.1 Global Configuration.....	227
4.7.8.2 VLAN Configuration.....	227
4.7.8.3 Interface Configuration	228
4.7.8.4 Statistics	229
4.7.8.5 Log	229
4.7.9 Login IP Management.....	230
4.7.9.1 Login IP Management	230
4.7.10 DoS Protection.....	231
4.7.11 IPv4 DHCP Snooping.....	232
4.7.11.1 Global Configuration	232
4.7.11.2 VLAN Configuration	233
4.7.11.3 Interface Configuration	233
4.7.11.4 Legal Client Table	234
4.7.12 IPv6 DHCP Snooping.....	235
4.7.12.1 Global Configuration.....	235
4.7.12.2 VLAN Configuration.....	236
4.7.12.3 Interface Configuration	237
4.7.12.4 Legal Client Table.....	237
4.7.13 IPv4 Source Guard	238
4.7.13.1 Interface Configuration	238
4.7.13.2 Static Table.....	239
4.7.13.3 Dynamic Binding	239
4.7.14 IPv6 Source Guard	240
4.7.14.1 Interface Configuration	240
4.7.14.2 Static Table.....	241
4.7.14.3 Dynamic Binding	241
4.7.15 Application Filter	242
4.7.16 CPU Guard	243
4.8 Device Management.....	244
4.8.1 SNMP	244
4.8.1.1 Global Configuration.....	245
4.8.1.2 Community	245
4.8.1.3 View Configuration	246

4.8.1.4 Group Configuration	246
4.8.1.5 Local User	247
4.8.1.6 Remote User	248
4.8.1.7 Trap	248
4.8.1.8 Statistics	250
4.8.2 RMON	251
4.8.2.1 Alarm Group	251
4.8.2.2 Event Group	252
4.8.2.3 History Group	253
4.8.2.4 Statistics Group	253
4.8.3 Cluster	254
4.8.3.1 Global Configuration.....	254
4.8.3.2 Member Configuration.....	255
4.8.3.3 Candidate Information	255
4.8.4 DNS.....	255
4.8.4.1 Global Configuration.....	255
4.8.4.2 Domain Names.....	256
4.8.4.3 Name Servers	256
4.8.4.4 Static Table.....	256
4.8.4.5 Current DNS Information.....	257
4.8.5 DHCP	257
4.8.5.1 DHCP Options.....	257
4.8.5.2 Relay	258
4.8.5.3 Relay Option82.....	258
4.8.5.4 Dynamic Provision.....	258
4.8.6 OAM	259
4.8.6.1 Interface	259
4.8.6.2 Statistics	260
4.8.6.3 Event Log	260
4.8.6.4 Peer Information	260
4.8.6.5 Loopback Result.....	261
4.8.6.6 Loopback Test	262
4.8.7 CFM.....	263
4.8.7.1 Global Configuration.....	263
4.8.7.2 Interface Configuration	265
4.8.7.3 MD Management.....	265
4.8.7.4 MD Details.....	266
4.8.7.5 MA Management	267
4.8.7.6 MA Details	268
4.8.7.7 MEP Management.....	269
4.8.7.8 Remote MEP Management	269
4.8.7.9 Transmit Link Trace	270
4.8.7.10 Transmit Loopback	271
4.8.7.11 Transmit Delay Measure.....	272
4.8.7.12 Show Local MEP	273
4.8.7.13 Show Local MEP Details	273
4.8.7.14 Show Local MIP	274

4.8.7.15 Show Remote MEP	274
4.8.7.16 Show Remote MEP Details	275
4.8.7.17 Show Link Trace Cache.....	276
4.8.7.18 Show Fault Notification Generator.....	276
4.8.7.19 Show Continuity Check Error	277
4.8.8 Time Setting	278
4.8.8.1 Time Configuration	278
4.8.8.2 SNTP Server	278
4.8.8.3 NTP Server.....	279
4.8.8.4 NTP authentication Key.....	279
4.8.8.5 Time Zone Configuration	280
4.8.8.6 Summer Time	280
4.8.9 Event Log	281
4.8.9.1 Log Information	281
4.8.9.2 Global Configuration.....	281
4.8.9.3 Remote Log Server	282
4.8.9.4 SMTP	283
4.8.10 File Management	284
4.8.10.1 File download	284
4.8.10.2 Saving Configuration	285
4.8.10.3 Setting The BOOT File	285
4.8.11 Ping.....	286
4.8.12 Trace Route.....	286
4.8.13 System Reboot	287
5. SWITCH OPERATION	288
5.1 Address Table	288
5.2 Learning	288
5.3 Forwarding & Filtering	288
5.4 Store-and-Forward	288
5.5 Auto-Negotiation	288
6. TROUBLESHOOTING.....	289
APPENDIX A: Networking Connection	290
A.1 Switch's Data RJ45 Pin Assignments - 1000Mbps, 1000BASE-T	290
A.2 10/100Mbps, 10/100BASE-TX	290
APPENDIX B : GLOSSARY	292

1. INTRODUCTION

1.1 Packet Contents

Thank you for purchasing PLANET SGS-5240 L2+ Multi-Port Gigabit Stackable Managed Switch series. The descriptions of these models are as follows:

SGS-5240-24T4X	Layer 2+ 24-Port 10/100/1000T + 4-Port 10G SFP+ Stackable Managed Switch
SGS-5240-24P4X	Layer 2+ 24-Port 10/100/1000T 802.3at PoE + 4-Port 10G SFP+ Stackable Managed Switch
SGS-5240-48T4X	Layer 2+ 48-Port 10/100/1000T + 4-Port 10G SFP+ Stackable Managed Switch
SGS-5240-20S4C4XR	Layer 2+ 20-Port 100/1000X SFP + 4-Port Gigabit TP/SFP + 4-Port 10G SFP+ Stackable Managed Switch with Redundant Power

“**Managed Switch**” mentioned in this Quick Installation Guide refers to the above models.

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

- The Managed Switch x 1
- Quick Installation Guide x 1
- RJ45-to-DB9 Console Cable x 1
- Power Cord x 1
- Rubber Feet x 4
- Two Rack-mounting Brackets with Attachment Screws x 1
- Grounding Cable x 1
- SFP Dust Cap

Model	SFP Dust Caps
SGS-5240-24T4X	4
SGS-5240-24P4X	4
SGS-5240-48T4X	4
SGS-5240-20S4C4XR	28

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

High-density, Resilient Deployment Switch Solution for Gigabit Networks of Enterprises and Campuses

PLANET SGS-5240 series is a Layer 2+ Stackable Managed Gigabit Switch that provides high-density performance, **Layer 3 static routing** with **10Gbps uplink** interfaces delivered in a rugged, strong case.



Whether It's Standalone or Stackable, It Suits Enterprises & Campuses

L3 Static Routing **ERPS Ring** **Stackable** **IP Cluster**

4x 10G SFP+

Value-added Standalone Switch **High-density Stackable Switches**

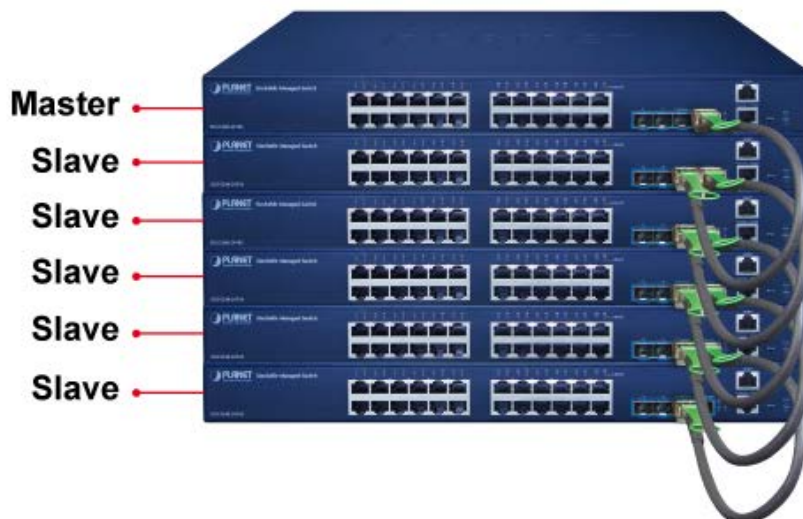
One IP Management
6 Units
12 SFP+
144 Copper

One Solution Fits All Difficult Applications

The administrator can flexibly choose the suitable SFP/SFP+ transceiver according to the transmission distance or the transmission speed required to extend the 10G network efficiently. Besides, with **128/178Gbps switching fabric**, the SGS-5240 series can handle extremely large amounts of data in a secure topology linking to backbone or high capacity servers for ISP and enterprise VoIP, video streaming, and multicast applications.

High Reliability Hardware Stacking

Two of the 10G SFP+ ports are used to connect several SGS-5240 series, enabling to build a virtually logical facility. The SGS-5240 series gives the enterprises, service providers and telecoms flexible control over port density, uplinks and switch stack performance. The SGS-5240 series can be connected as a ring for redundancy and ensures that data integrity is retained even if one switch in the stack fails. You can even hot-swap switches without disrupting the network, which greatly simplifies the tasks of upgrading the LAN for catering to increasing bandwidth demands.

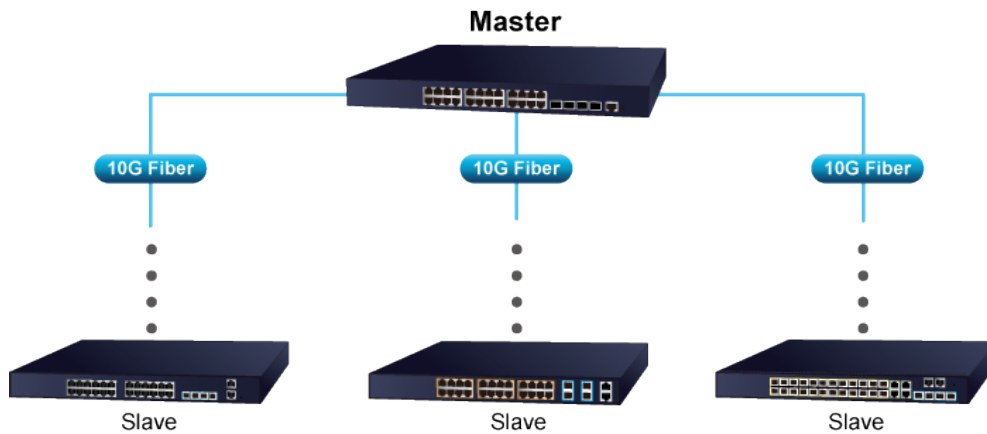


Central IP Stacking Management

Positioned as the distribution or aggregation layer switch for large networks, the SGS-5240 series supports IP stacking function that helps network managers to easily configure up to 16 switches in the same series via one single IP address instead of connecting and setting each unit one by one. The IP Stacking technology groups PLANET SGS-5240 switch series together to enable centralized management through a single unit, regardless of physical location or switch type, as long as they are connected to the same local network.

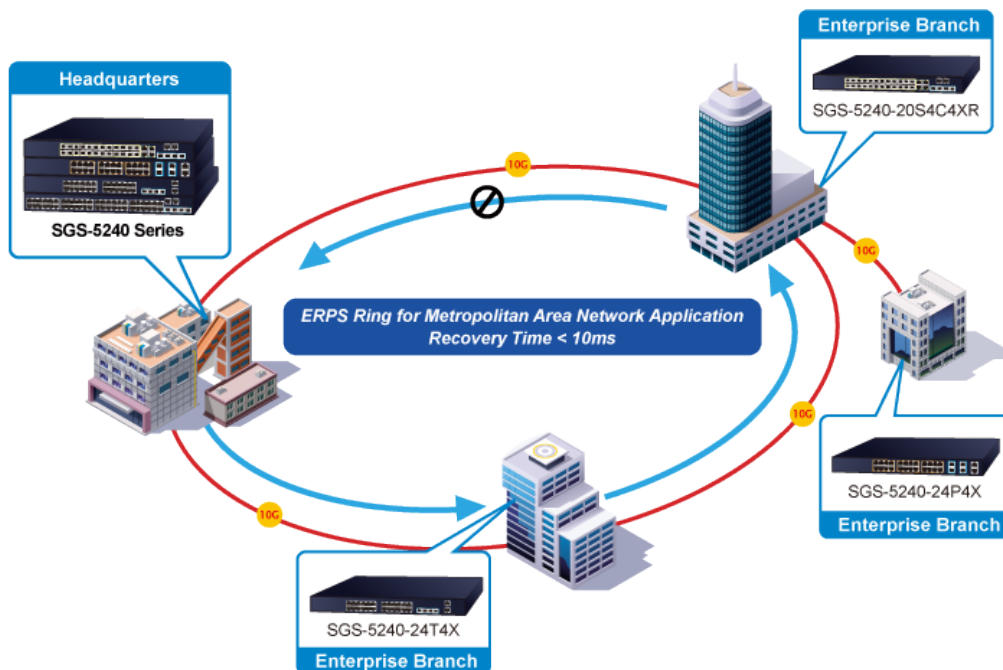
IP Stacking/Cluster

Up to 16 units with SGS-5240 Series



Redundant Ring, Fast Recovery for Critical Network Applications

The SGS-5240 series supports redundant ring technology and features strong, rapid self-recovery capability to prevent interruptions and external intrusions. It incorporates advanced ITU-T **G.8032 ERPS (Ethernet Ring Protection Switching)** technology and **Spanning Tree Protocol (802.1s MSTP)** into customer's network to enhance system reliability and uptime in harsh environments. In a certain simple Ring network, the recovery time could be less than 50ms to quickly bring the network back to normal operation.



High Performance 10Gbps Ethernet Capacity

The four SFP+ slots built in the SGS-5240 series support **dual speed** and **10GBASE-SR/LR or 1000BASE-SX/LX**. With its 4 ports, 10Gbps and 1Gbps Ethernet link capability, the administrator now can flexibly choose the suitable SFP/SFP+ transceiver according to the transmission distance or the transmission speed required to extend the network efficiently. The IGS-6325 Series provides broad bandwidth and powerful processing capacity.

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

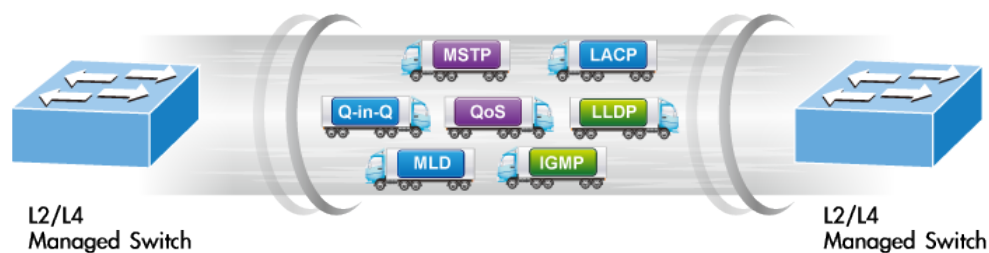
The SGS-5240 series supports IPv4/IPv6 VLAN routing feature which allows to cross over different VLANs and different IP addresses for the purpose of having a highly-secure, flexible management and simpler networking application.

Strong Multicast

The SGS-5240 series supports abundant multicast features. In Layer 2, it features IPv4 IGMPv1/v2/v3 snooping and IPv6 MLD v1/v2 snooping. With Multicast VLAN Register (MVR), multicast receiver/sender control and illegal multicast source detection functions, the SGS-5240 series provides great application experience for customers.

Robust Layer 2 Features

The SGS-5240 series can be programmed for basic switch management functions such as port speed configuration, port aggregation, VLAN, Multiple Spanning Tree Protocol and bandwidth control. This switch provides 802.1Q tagged VLAN, Q-in-Q, voice VLAN and GVRP Protocol functions. By supporting port aggregation, the SGS-5240 series allows the operation of a high-speed trunk combined with multiple ports.



Powerful Network Security

The SGS-5240 series offers comprehensive Layer 2 to Layer 4 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, MAC-based and web-based user and device authentications.

Advanced IP Network Protection

The SGS-5240 series 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-secure corporate networks with considerably less time and effort than before.

Efficient and Secure Management

For efficient management, the SGS-5240 series is equipped with console, Web and SNMP management interfaces.

- With the built-in **Web-based** management interface, the SGS-5240 series offers an easy-to-use, platform-independent management and configuration facility.
- For **text-based** management, it can be accessed via Telnet and the console port.
- For standard-based monitor and management software, it offers SNMPv3 connection which encrypts the packet content at each session for secure remote management.



SGS-5240 Series

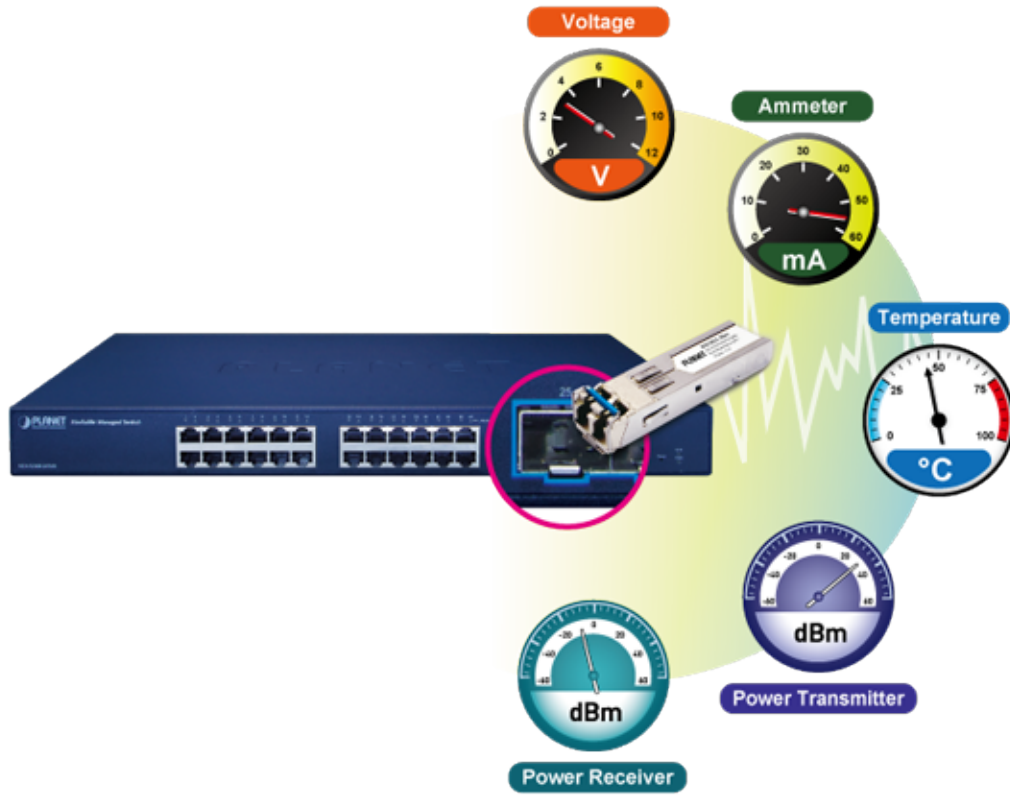
Moreover, the SGS-5240 series offers secure remote management by supporting SSHv2 and SSLv3 connection which encrypts the packet content at each session.



Intelligent SFP Diagnosis Mechanism

The SGS-5240 series supports SFP-DDM (Digital Diagnostic Monitor) function that greatly helps network administrator to easily monitor real-time parameters of the SFP and SFP+ transceivers, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.

Digital Diagnostic Monitor (DDM)



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, 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 Ports

- 24/48 10/100/1000BASE-T RJ45 copper ports
- 24 100/1000BASE-X SFP slots (SGS-5240-20S4C4XR)
- 4 10GBASE-SR/LR SFP+ slots, compatible with 1000BASE-SX/LX/BX SFP
- RJ45 to DB9 console interface for switch basic management and setup
- One 10/100BASE-TX Management port

➤ Stacking Features

- IP Stacking
 - Connects with stack member via Gigabit TP, SFP and 10G SFP+ interfaces
 - Single IP address management, supporting up to 16 IP units stacked together
- Hardware Stacking
 - Virtualized multiple SGS-5240 switch series stacked into one logical device
 - Connects with stack member via assigned 10G SFP+ interfaces
 - Single IP address stack management, supporting up to 6 hardware units stacked together
 - Stacking architecture supports redundant ring mode

➤ IP Routing Features

- IPv4/IPv6 hardware static routing
- Routing interface provides per VLAN routing mode

➤ Layer 2 Features

- Supports VLAN
 - IEEE 802.1Q tag-based VLAN
 - Provider Bridging (VLAN Q-in-Q, IEEE 802.1ad) supported
 - GVRP for dynamic VLAN management
 - Protocol-based VLAN
 - MAC-based VLAN
 - IP subnet-based VLAN
 - Voice VLAN
- Supports Link Aggregation
 - 802.3ad Link Aggregation Control Protocol (LACP)
 - Cisco ether-channel (static trunk)
- Supports Spanning Tree Protocol
 - STP, IEEE 802.1D (Classic Spanning Tree Protocol)
 - RSTP, IEEE 802.1w (Rapid Spanning Tree Protocol)
 - MSTP, IEEE 802.1s (Multiple Spanning Tree Protocol, spanning tree by VLAN)
 - Supports BPDU & root guard
- Port mirroring to monitor the incoming or outgoing traffic on a particular port (many to one)
- Supports G.8032 ERPS (Ethernet Ring Protection Switching)
- Loop protection to avoid broadcast loops
- Link Layer Discovery Protocol (LLDP)
- Compatible with Cisco uni-directional link detection (UDLD) that monitors a link between two switches and blocks the ports on both ends of the link if the link fails at any point between the two devices

➤ **Quality of Service**

- Input and output rate limit per port bandwidth control
- 8 priority queues on all switch ports
 - IEEE 802.1p CoS/DSCP/IP Precedence
 - VLAN ID
 - ACL
 - Policy-based ingress and egress QoS

➤ **Multicast**

- Supports IPv4 IGMP snooping v1, v2 and v3
- Supports IPv6 MLD snooping v1 and v2
- Querier mode support
- IPv4 IGMP snooping port filtering
- IPv6 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
 - Guest VLAN assigns clients to a restricted VLAN with limited services
- Access Control List
 - IP-based Access Control List (ACL)
 - MAC-based Access Control List (ACL)
 - Time-based ACL
- 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 and Telnet Command Line Interface
 - HTTP web switch management
 - SNMP v1 and v2c switch management
 - SSHv2, SSLv3 and SNMP v3 secure access
- SNMP Management
 - Four RMON groups (history, statistics, alarms, and events)
 - SNMP trap for interface Link Up and Link Down notification
- Built-in Trivial File Transfer Protocol (TFTP) client
- BOOTP and DHCP for IP address assignment
- System Maintenance
 - Firmware upload/download via HTTP
 - Reset button for system reboot or reset to factory default

- Dual images
 - DHCP Functions:
 - DHCP Relay
 - DHCP Option 82
 - DHCP Server
 - User Privilege levels control
 - Network Time Protocol (NTP) and SNTP
 - Network Diagnostic
 - SFP-DDM (Digital Diagnostic Monitor)
 - Cable diagnostic technology provides the mechanism to detect and report potential cabling issues
 - ICMPv6/ICMPv4 remote ping
 - Syslog remote alarm
 - System Log
- **Power over Ethernet** (SGS-5240-24P4X)
- Complies with IEEE 802.3at Power over Ethernet Plus
 - Up to 24 ports of IEEE 802.3at PoE devices powered
 - 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
 - PD classification detection

1.5 Product Specifications

Product	SGS-5240-24T4X	SGS-5240-24P4X	SGS-5240-20S4C4XR	SGS-5240-48T4X
Hardware Specifications				
10/100/1000BASE-T RJ45 Ports	24	24	4 (combo)	48
1000BASE-X SFP Slots	-	-	20+4	-
10GBASE-X SFP+ Slots	4 10GBASE-SR/LR SFP+ interfaces Compatible with 1000BASE-SX/LX/BX SFP transceiver			
Console	1 x RJ45-to-RS232 serial port (115200, 8, N, 1)			
CPU	ARM A9 800MHz			
RAM	512Mbytes			
Flash Memory	64Mbytes			
Dimensions (W x D x H)	440 x 280 x 44 mm	440 x 280 x 44 mm	440 x 280 x 44 mm	440 x 330 x 44 mm
Weight	3.0kg	4.1kg	3.3kg	4.0kg
Power Consumption	21 watts/71.65 BTU	432 watts/1474 BTU	43W/146.72 BTU	45W/153.55 BTU
Power Requirements - AC	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz
Power Requirements - DC	-	-	DC 36-75V	-
Fan	-	2	1	1
Switching				
Switch Architecture	Store-and-forward			
Switch Fabric	128Gbps/ non-blocking	128Gbps/ non-blocking	128Gbps/ non-blocking	176Gbps/ non-blocking
Switch Throughput	95.23Mpps	95.23Mpps	95.23Mpps	130.95Mpps
Address Table	16K MAC address table with auto learning function			
ARP Table	1024			
ACL Table	900			
Shared Data Buffer	1.5MB			
Jumbo Frame	9KB			
Flow Control	Back pressure for half duplex IEEE 802.3x pause frame for full duplex			
Power over Ethernet Specifications				
PoE Standard	-	IEEE 802.3at Power over Ethernet Plus PSE	-	-
PoE Power Supply Type	-	End-span	-	-
PoE Power Output	-	Per port 54V DC, maximum 30 watts	-	-
Power Pin Assignment	-	1/2(+), 3/6(-)	-	-
PoE Power Budget	-	370 watts (max.)	-	-

Layer 3 Functions	
IP Interfaces	Max. 32 VLAN interfaces
Routing Table	IPv4 256 entries IPv6 128 entries
Routing Protocols	IPv4 hardware static routing IPv6 hardware static routing
Layer 2 Functions	
Port Configuration	Port disable/enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Flow control disable/enable Port loopback detect
Port Status	Display each port's speed duplex mode, link status, flow control status and auto negotiation status
Port Mirroring	TX/RX/Both Remote port mirror (RSPAN) Many-to-1 monitor
VLAN	IEEE 802.1Q tagged based VLAN, up to 4K VLAN groups IEEE 802.1ad Q-in-Q VLAN stacking/tunneling IEEE 802.1v Protocol-based VLAN Port-based VLAN MAC-based VLAN IP Subnet-based VLAN Voice VLAN GVRP for VLAN management, up to 256 VLAN
Spanning Tree Protocol	IEEE 802.1D Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) BPDU Guard, BPDU filtering and BPDU transparent Root Guard STP-based loopback detection
Multicast	IPv4 IGMP v1/v2/v3 snooping IPv4 Querier mode support IGMP Filtering and IGMP Throttling IGMP Proxy reporting IGMP mroute-forward mode Up to 255 multicast groups
	IPv6 MLD v1/v2 snooping Up to 255 multicast groups
	Multicast VLAN Register (MVR), supports 5 multicast VLANs
Link Aggregation	IEEE 802.3ad Ling Aggregation Control Protocol (LACP) Static trunk link aggregation Supports 26 groups with 8 ports per trunk group Up to 80Gbps bandwidth (full duplex mode) Load Balance Algorithm:

	<ul style="list-style-type: none"> - Source IP/destination IP/Source + destination IP - Source MAC/destination MAC/Source + destination MAC
Storm Control	<p>Broadcast/Multicast/Unicast storm control Rate: 64Kbps-10,000Mbps</p>
Bandwidth Control	<p>Input/Output/Both Per port bandwidth control Gigabit port: 64Kbps-1,000Mbps 10Gigabit port: 64Kbps-10,000Mbps</p>
QoS	<p>8 priority queues on all switch ports Scheduling for priority queues</p> <ul style="list-style-type: none"> - Weighted Round Robin (WRR) - Strict priority - Hybrid (DRR/WRR + strict) <p>Traffic classification:</p> <ul style="list-style-type: none"> - IEEE 802.1p CoS/DSCP/IP Precedence - VLAN ID - ACL - Policy-based ingress and egress QoS
Ring	ITUT G.8032 ERPS v1 and v2
Security Functions	
Access Control List	<p>Supports Standard and Expanded ACL</p> <ul style="list-style-type: none"> - IP-based ACL - MAC-based ACL - ARP ACL - Time-based ACL <p>ACL based on:</p> <ul style="list-style-type: none"> - MAC Address - IPv4/IPv6 IP Address - Ethertype - Protocol-number/UDP - sport/dport - DSCP - 802.1p Priority <p>Up to 900 entries</p>
Security	<p>Port security Supports static MAC + port binding Defend against DoS or TCP attacks DHCP Snooping, DHCP Option 82 IP source guard Dynamic ARP inspection Command line authority control based on user levels</p>
AAA	<p>RADIUS client TACACS+ client</p>
Network Access Control	<p>IEEE 802.1x port-based network access control MAC-based authentication</p>

	<p>Web authentication</p> <p>Local/RADIUS authentication</p>
Management Functions	
System Configuration	<p>Console and Telnet</p> <p>Web browser</p> <p>SNMP v1, v2c</p>
Secure Management Interfaces	<p>IPv4/IPv6 SSHv2, SSLv3, SNMPv3</p> <p>Maximum 8 sessions for SSH and telnet connection</p>
System Management	<p>IPv4 and IPv6 dual stack management</p> <p>SNMP MIB and TRAP</p> <p>SNMP RMON 1, 2, 3, 9 four groups</p> <p>Firmware upgrade by HTTP/TFTP/FTP protocol through Ethernet network</p> <p>Configuration upload/download through HTTP/TFTP/FTP protocol</p> <p>Supports dual images and multiple configuration files</p> <p>Supports IEEE 802.1ab LLDP protocol</p> <p>NTP/SNTP client</p> <p>RADIUS authentication for IPv4/IPv6 login user name and password</p> <p>Security IP safety net management function: avoid unlawful landing at nonrestrictive area</p>
Event Management	<p>Remote Syslog</p> <p>System log</p> <p>SMTP</p>
IP Clustering	<p>16 members</p>
IP Clustering Compatibility List	<p>SGS-5240-24T4X</p> <p>SGS-5240-24P4X</p> <p>SGS-5240-20S4C4XR</p> <p>SGS-5240-48T4X</p>
Hardware Stacking	<p>6 members max.</p> <p>Last 2 10G SFP+ slots are functioned as Stacking Up and Down interfaces</p>
Hardware Stacking Compatibility List	<p>Require the same models for hardware stacking</p>
SNMP MIBs	<p>RFC 1213 MIB-II</p> <p>RFC 1215 Internet Engineering Task Force</p> <p>RFC 1271 RMON</p> <p>RFC 1354 IP-Forwarding MIB</p> <p>RFC 1493 Bridge MIB</p> <p>RFC 1643 Ether-like MIB</p> <p>RFC 1907 SNMP v2</p> <p>RFC 2011 IP/ICMP MIB</p> <p>RFC 2012 TCP MIB</p> <p>RFC 2013 UDP MIB</p> <p>RFC 2096 IP forward MIB</p> <p>RFC 2233 if MIB</p> <p>RFC 2452 TCP6 MIB</p> <p>RFC 2454 UDP6 MIB</p> <p>RFC 2465 IPv6 MIB</p>

	<p>RFC 2466 ICMP6 MIB RFC 2573 SNMP v3 notify RFC 2574 SNMP v3 vacm RFC 2674 Bridge MIB Extensions (IEEE 802.1Q MIB) RFC 2674 Bridge MIB Extensions (IEEE 802.1P MIB)</p>
Standard Conformance	
Regulatory Compliance	FCC Part 15 Class A, CE
Standards Compliance	<p>IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3z Gigabit 1000BASE-SX/LX IEEE 802.3ab Gigabit 1000BASE-T IEEE 802.3ae 10Gb/s Ethernet IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging IEEE 802.1ad Q-in-Q VLAN stacking/tunneling IEEE 802.1v Protocol-based VLAN IEEE 802.1X port authentication network control IEEE 802.1ab LLDP 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 FRC 3810 MLD v2 ITU-T G.8032 ERPS Ring</p>
Environments	
Operating	<p>Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 90% (non-condensing)</p>
Storage	<p>Temperature: -10 ~ 70 degrees C Relative Humidity: 5 ~ 90% (non-condensing)</p>

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 to Figures 2-1-4](#) show the front panels of the Managed Switches.

SGS-5240-24T4X Front Panel

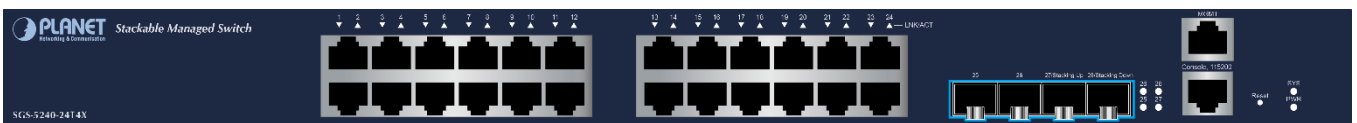


Figure 2-1-1: Front Panel of SGS-5240-24T4X

SGS-5240-24P4X Front Panel



Figure 2-1-2: Front Panel of SGS-5240-24P4X

SGS-5240-20S4C4XR Front Panel

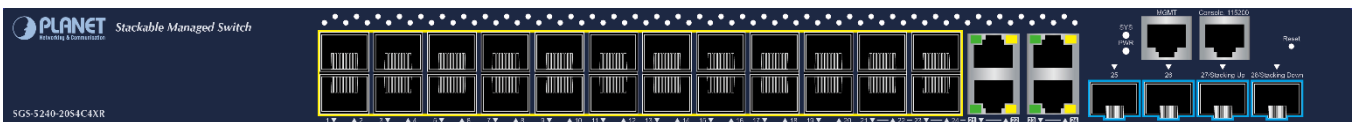


Figure 2-1-3: Front Panel of SGS-5240-20S4C4XR

SGS-5240-48T4X Front Panel



Figure 2-1-4: Front Panel of SGS-5240-48T4X

■ **Gigabit TP interface**

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

■ **10 Gigabit SFP+ slot**

1/10GBASE-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 SGS-5240 Series 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.
>10 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 SGS-5240 Series is located at the front of the switch.



The SGS-5240-48T4X doesn't support factory default function via reset button.

2.1.2 LED Indications

The front panel LEDs indicate instant status of power and system status, port links and data activity; they help monitor and troubleshoot when needed.

■ LED Definition

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
SYS	Green	Lights to indicate that the system is working.
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.

2.1.3 Switch Rear Panel

The rear panel of the Managed Switch consists of the AC inlet power socket. [Figures 2-1-5](#) to [Figure 2-1-8](#) show the rear panels of the Managed Switches.

SGS-5240-24T4X Rear Panel



Figure 2-1-5: Rear Panel of SGS-5240-24T4X

SGS-5240-24P4X Rear Panel



Figure 2-1-6: Rear Panel of SGS-5240-24P4X

SGS-5240-20S4C4XR Rear Panel



Figure 2-1-7: Rear Panel of SGS-5240-20S4C4XR

SGS-5240-48T4X Rear Panel

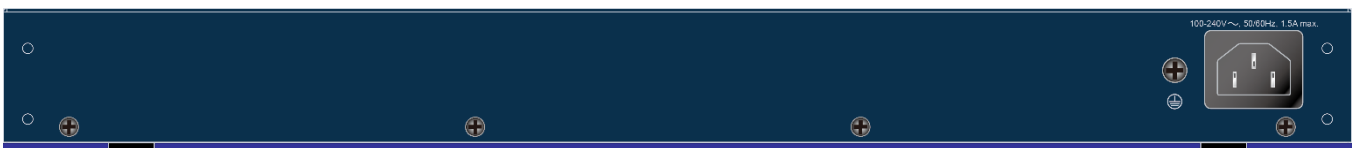


Figure 2-1-8: Rear Panel of SGS-5240-48T4X

■ 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.

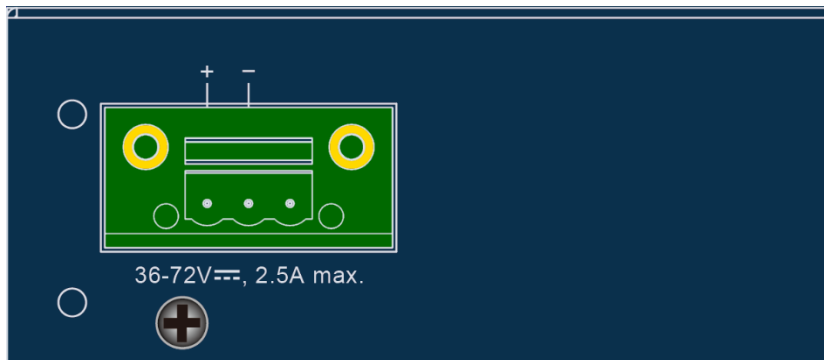
Plug the female end of the power cord firmly into the receptacle on the rear panel of the Managed Switch and the other end of the power cord into an electrical outlet and the power will be ready.

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.

■ DC Power Connector (SGS-5240-20S4C4XR)

The rear panel of the SGS-5240-20S4C4XR contains a DC power connector, which accepts DC power input voltage from 36V to 72V DC. Connect the power cable to the Managed Switch at the input terminal block.



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.



In the installation steps below, this manual uses the SGS-5240-48T4X as an example. However, the steps for PLANET SGS-5240 series are similar.

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.

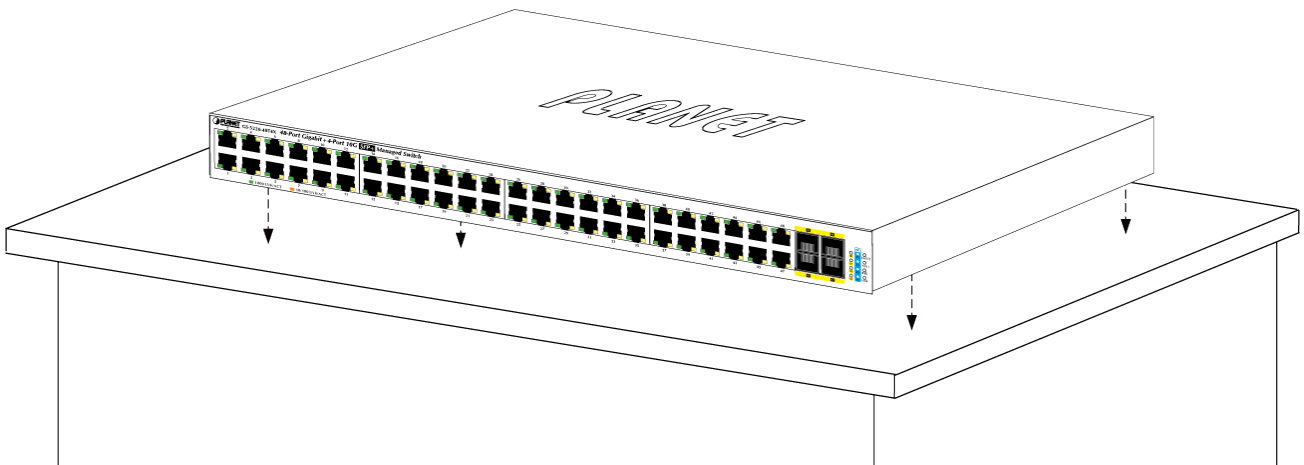


Figure 2-2-1: Place the Managed Switch on the Desktop

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



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.



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.

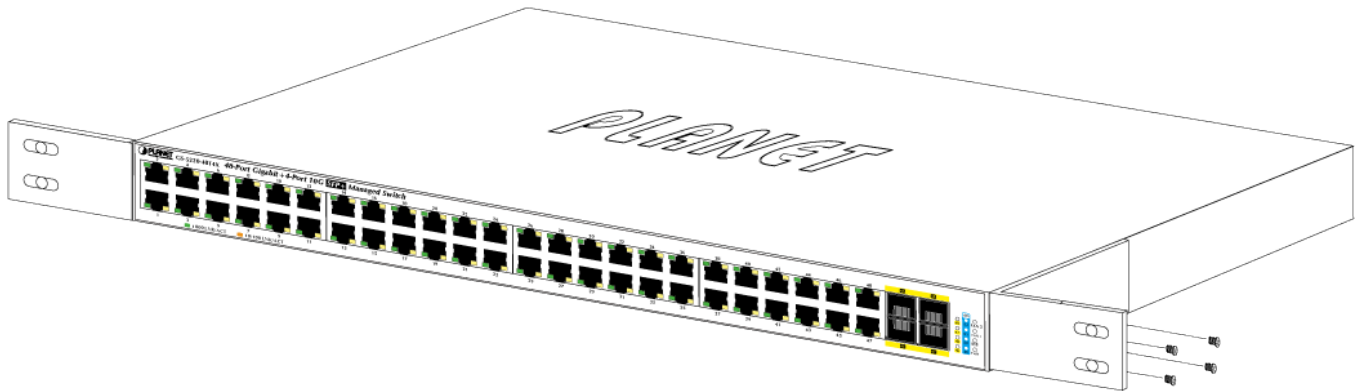


Figure 2-2-2: Attach Brackets to the Managed Switch.



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.

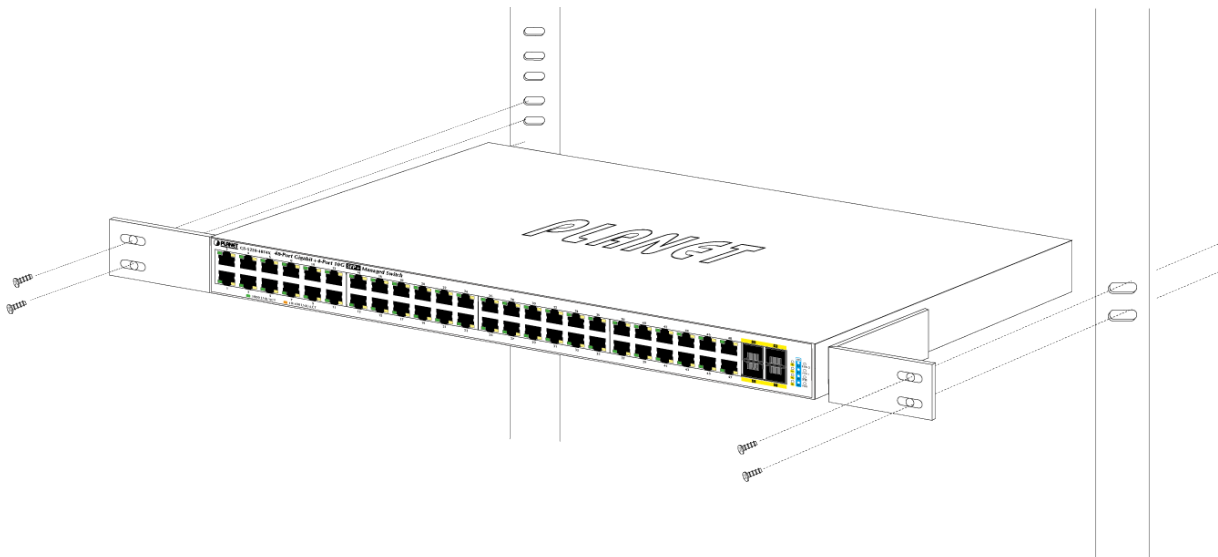


Figure 2-2-3: Mounting Managed Switch in a Rack

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..

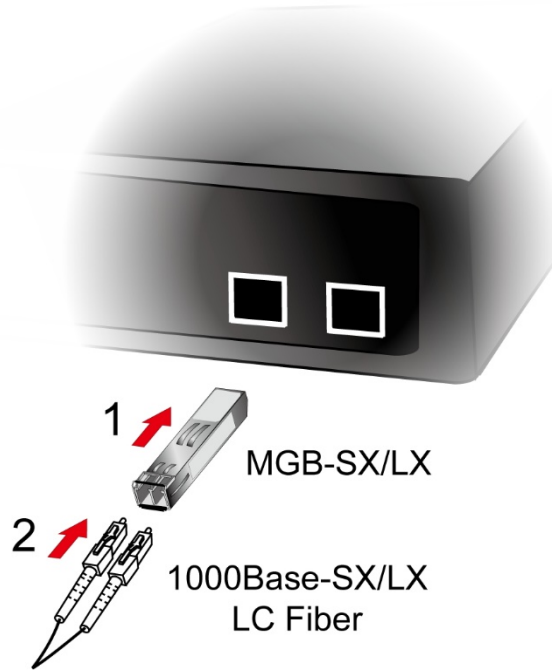


Figure 2-2-4: Plug-in the SFP/SFP+ Transceiver

■ Approved PLANET SFP/SFP+ Transceivers

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

Gigabit Ethernet Transceiver (1000BASE-X SFP)

Model	DDM	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (nm)	Operating Temp.
MGB-GT	--	1000	Copper	--	100m	--	0 ~ 60 °C
MGB-SX(V2)	YES	1000	LC	Multi Mode	550m	850nm	0 ~ 60 °C
MGB-SX2(V2)	YES	1000	LC	Multi Mode	2km	1310nm	0 ~ 60 °C
MGB-LX(V2)	YES	1000	LC	Single Mode	20km	1310nm	0 ~ 60 °C
MGB-L40	YES	1000	LC	Single Mode	40km	1310nm	0 ~ 60 °C
MGB-L80	YES	1000	LC	Single Mode	80km	1550nm	0 ~ 60 °C
MGB-L120(V2)	YES	1000	LC	Single Mode	120km	1550nm	0 ~ 60 °C
MGB-TSX	YES	1000	LC	Multi Mode	550m	850nm	-40 ~ 75 °C
MGB-TSX2	YES	1000	LC	Multi Mode	2km	1310nm	-40 ~ 75 °C
MGB-TLX(V2)	YES	1000	LC	Single Mode	20km	1310nm	-40 ~ 75 °C
MGB-TL40	YES	1000	LC	Single Mode	40km	1310nm	-40 ~ 75 °C
MGB-TL80	YES	1000	LC	Single Mode	80km	1550nm	-40 ~ 75 °C

Gigabit Ethernet Transceiver (1000BASE-BX, Single Fiber Bi-directional SFP)

Model	DDM	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (TX)	Wavelength (RX)	Operating Temp.
MGB-LA10(V2)	YES	1000	WDM(LC)	Single Mode	10km	1310nm	1550nm	0 ~ 60 °C
MGB-LB10(V2)		1000	WDM(LC)	Single Mode	10km	1550nm	1310nm	0 ~ 60 °C
MGB-LA20(V2)	YES	1000	WDM(LC)	Single Mode	20km	1310nm	1550nm	0 ~ 60 °C
MGB-LB20(V2)		1000	WDM(LC)	Single Mode	20km	1550nm	1310nm	0 ~ 60 °C
MGB-LA40(V2)	YES	1000	WDM(LC)	Single Mode	40km	1310nm	1550nm	0 ~ 60 °C
MGB-LB40(V2)		1000	WDM(LC)	Single Mode	40km	1550nm	1310nm	0 ~ 60 °C
MGB-LA80	YES	1000	WDM(LC)	Single Mode	80km	1490nm	1550nm	0 ~ 60 °C
MGB-LB80		1000	WDM(LC)	Single Mode	80km	1550nm	1490nm	0 ~ 60 °C
MGB-TLA10(V2)	YES	1000	WDM(LC)	Single Mode	10km	1310nm	1550nm	-40 ~ 75 °C
MGB-TLB10(V2)		1000	WDM(LC)	Single Mode	10km	1550nm	1310nm	-40 ~ 75 °C
MGB-TLA20	YES	1000	WDM(LC)	Single Mode	20km	1310nm	1550nm	-40 ~ 75 °C
MGB-TLB20		1000	WDM(LC)	Single Mode	20km	1550nm	1310nm	-40 ~ 75 °C
MGB-TLA40	YES	1000	WDM(LC)	Single Mode	40km	1310nm	1550nm	-40 ~ 75 °C
MGB-TLB40		1000	WDM(LC)	Single Mode	40km	1550nm	1310nm	-40 ~ 75 °C
MGB-TLA80	YES	1000	WDM(LC)	Single Mode	80km	1490nm	1550nm	-40 ~ 75 °C
MGB-TLB80		1000	WDM(LC)	Single Mode	80km	1550nm	1490nm	-40 ~ 75 °C

10Gbps SFP+ (10G Ethernet/10GBASE)

Model	DDM	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (nm)	Operating Temp.
MTB-RJ	-	10G	Copper	-	30m	-	0 ~ 70 °C
MTB-SR	YES	10G	LC	Multi Mode	Up to 300m	850nm	0 ~ 60 °C
MTB-LR	YES	10G	LC	Single Mode	10km	1310nm	0 ~ 60 °C
MTB-TSR	YES	10G	LC	Multi Mode	Up to 300m	850nm	-40 ~ 75 °C
MTB-TLR	YES	10G	LC	Single Mode	10km	1310nm	-40 ~ 75 °C

10Gbps SFP+ (10GBASE-BX, Single Fiber Bi-directional SFP)

Model	DDM	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (TX)	Wavelength (RX)	Operating Temp.
MTB-LA20	YES	10G	WDM(LC)	Single Mode	20km	1270nm	1330nm	0 ~ 60 °C
MTB-LB20		10G	WDM(LC)	Single Mode	20km	1330nm	1270nm	0 ~ 60 °C
MTB-LA40	YES	10G	WDM(LC)	Single Mode	40km	1270nm	1330nm	0 ~ 60 °C
MTB-LB40		10G	WDM(LC)	Single Mode	40km	1330nm	1270nm	0 ~ 60 °C
MTB-LA60	YES	10G	WDM(LC)	Single Mode	60km	1270nm	1330nm	0 ~ 60 °C
MTB-LB60		10G	WDM(LC)	Single Mode	60km	1330nm	1270nm	0 ~ 60 °C



It is recommended to use PLANET 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 PLANET SGS-5240 series to the other network device, we have to make sure both sides of the SFP transceivers are with the same media type, for example: 1000BASE-SX to 1000BASE-SX, 1000BASE-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.

■ Connecting 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 "10G Force", or "1000M Force".

■ Removing 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 MGB 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



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 XP/2003/Vista/7/8/2008/10, MAC OS X or later, Linux, UNIX, or other platforms are compatible with TCP/IP protocols.
- Workstations are installed with Ethernet NIC (Network Interface Card)
- Serial Port Connection (Terminal)
 - The above Workstations come with **COM Port (DB9)** or **USB-to-RS232** converter.
 - The above Workstations have been installed with **terminal emulator**, such as Tera Term or PuTTY.
 - Serial cable -- one end is attached to the RS232 serial port, while the other end to the console port of the Managed Switch.
- Ethernet **Port Connection**
 - Network cables -- Use standard network (UTP) cables with RJ45 connectors.
 - The above PC is installed with Web browser.



It is recommended to use Internet Explorer 8.0 or above to access the Managed Switch. If the Web interface of the Managed Switch is not accessible, please turn off the anti-virus software or firewall and then try it again.

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 • Workstations have been installed with terminal emulator, such as Tera Term or PuTTY • 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.

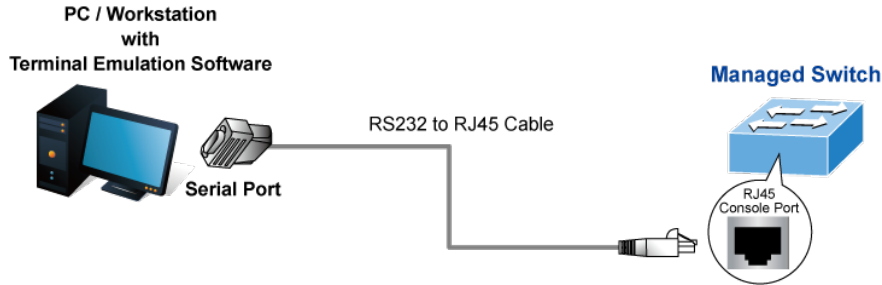


Figure 3-1: Console Management

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 Tera Term or Putty) 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

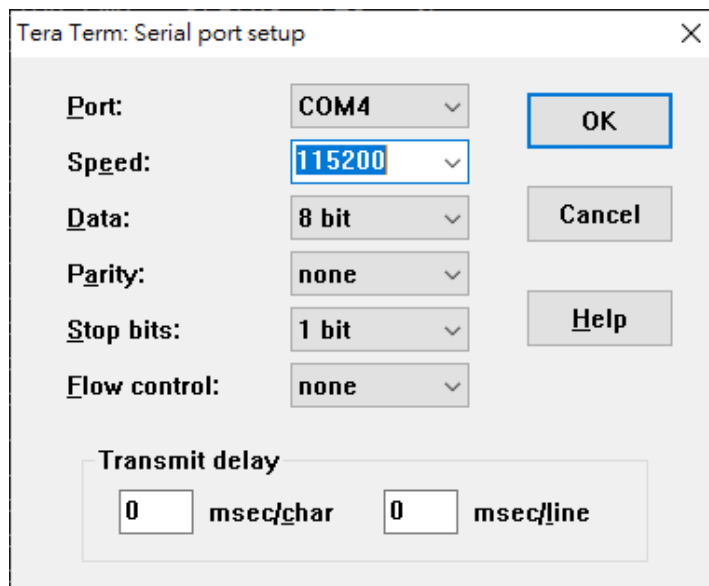


Figure 3-2: Terminal Parameter Settings

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.

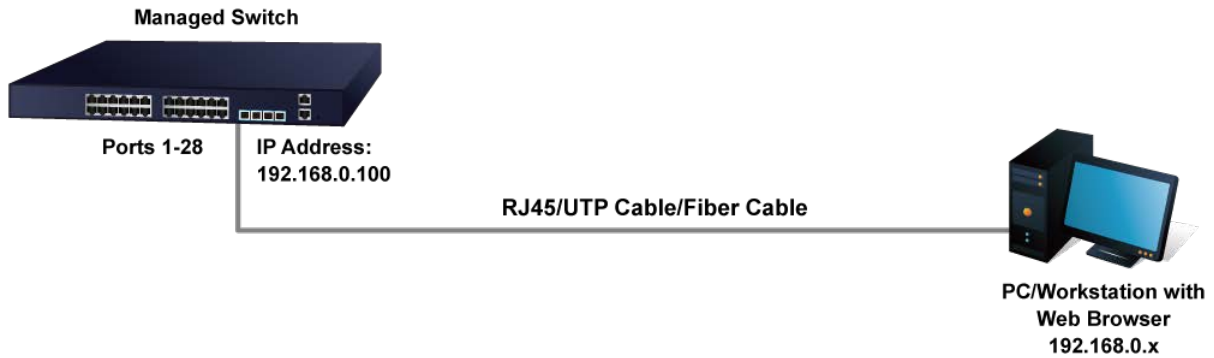


Figure 3-1-3: Web Management

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, **Google Chrome**, **Safari** or **Mozilla Firefox**.

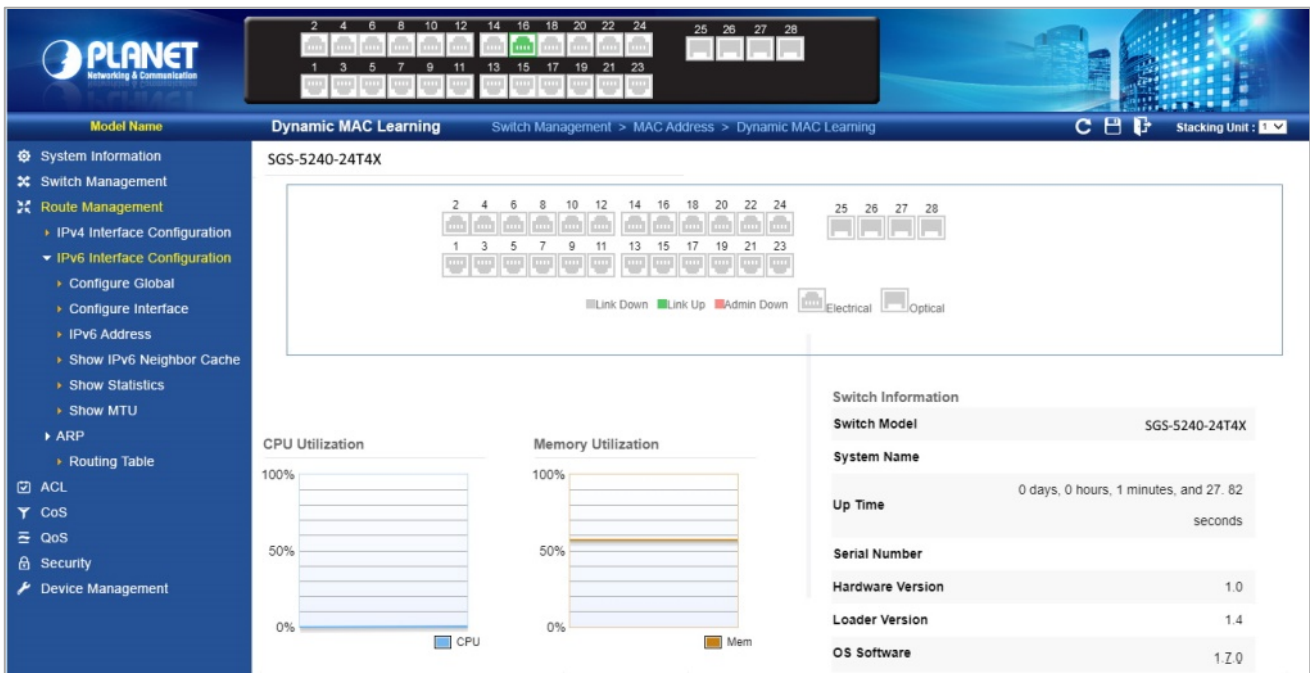


Figure 3-1-4: Web Main Screen of Managed Switch

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.

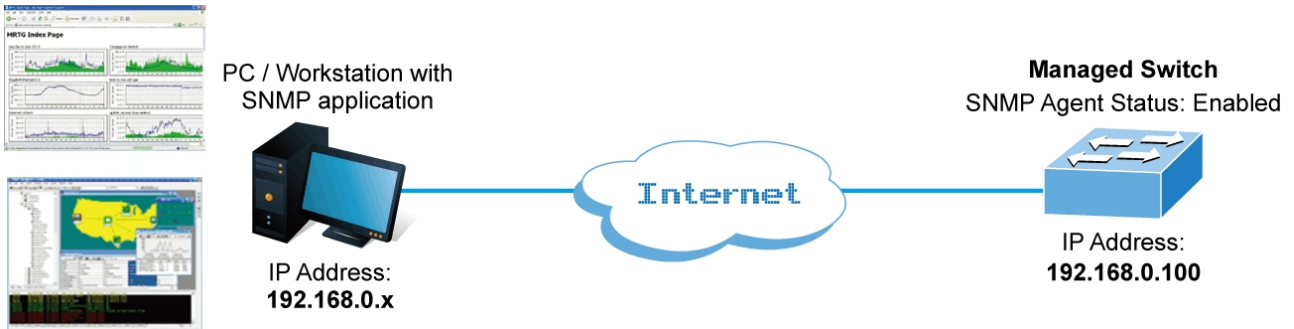


Figure 3-1-5: SNMP Management

3.6 PLANET Smart Discovery Utility

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

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

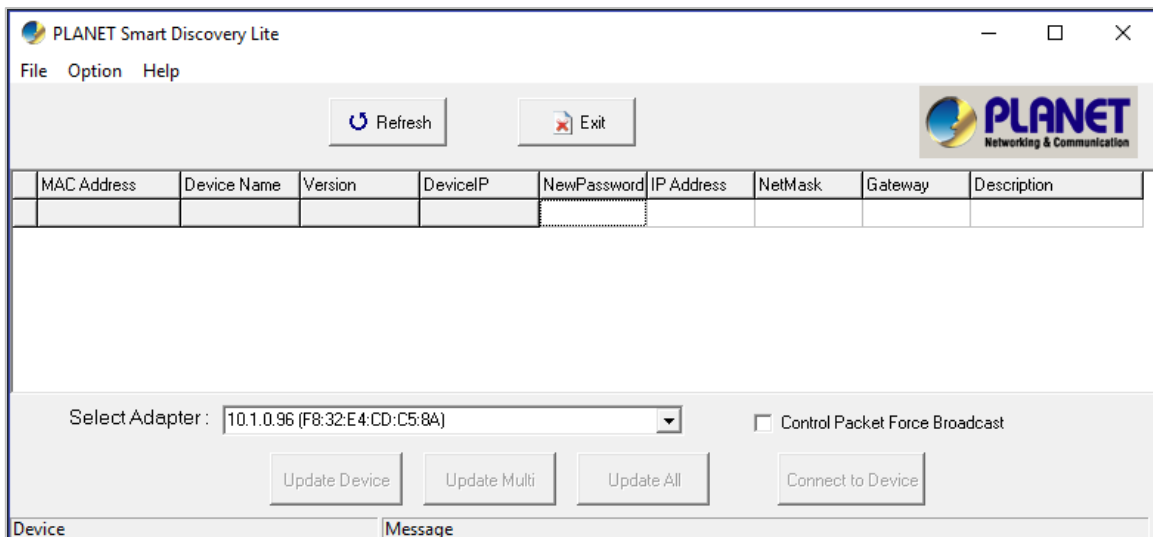


Figure 3-1-6: Planet Smart Discovery Utility Screen



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 the "Refresh" button for the currently connected devices in the discovery list as the screen shows below:

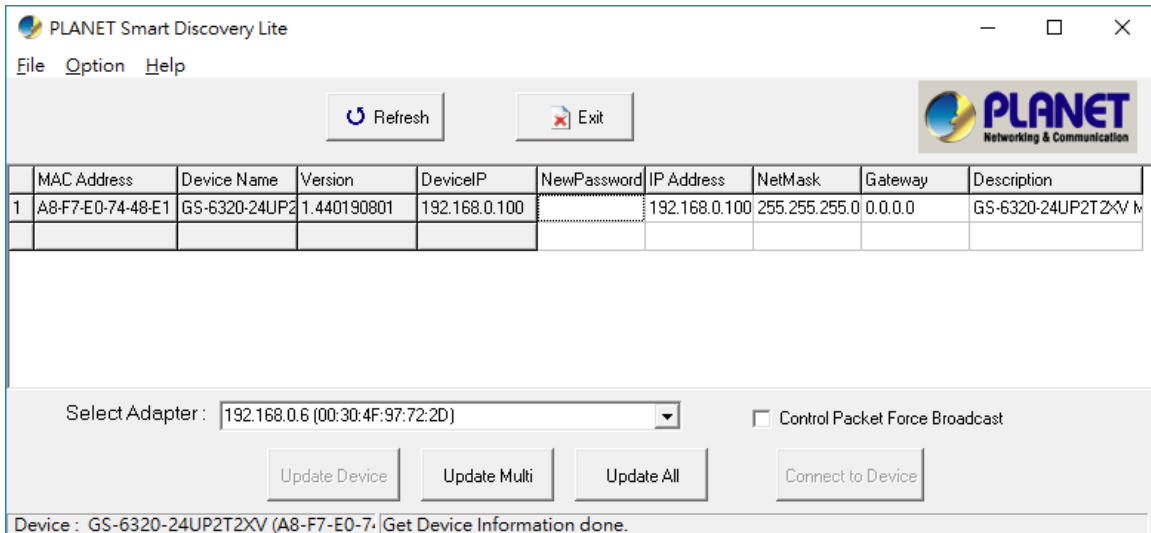


Figure 3-1-7: Planet Smart Discovery Utility Screen

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 to the devices.
2. After setup is completed, press the "Update Device", "Update Multi" or "Update All" button to take effect. The functions of the 3 buttons above are shown 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 allows you to assign a new setting value to the Web Smart Switch under a different IP subnet address.
4. Press the "Connect to Device" button and the Web login screen appears in [Figure 3-1-4](#).
5. Press the "Exit" button to shut down the Planet 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 provides a built-in browser interface. You can manage it remotely by having a remote host with Web browser, such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrome or Apple Safari.

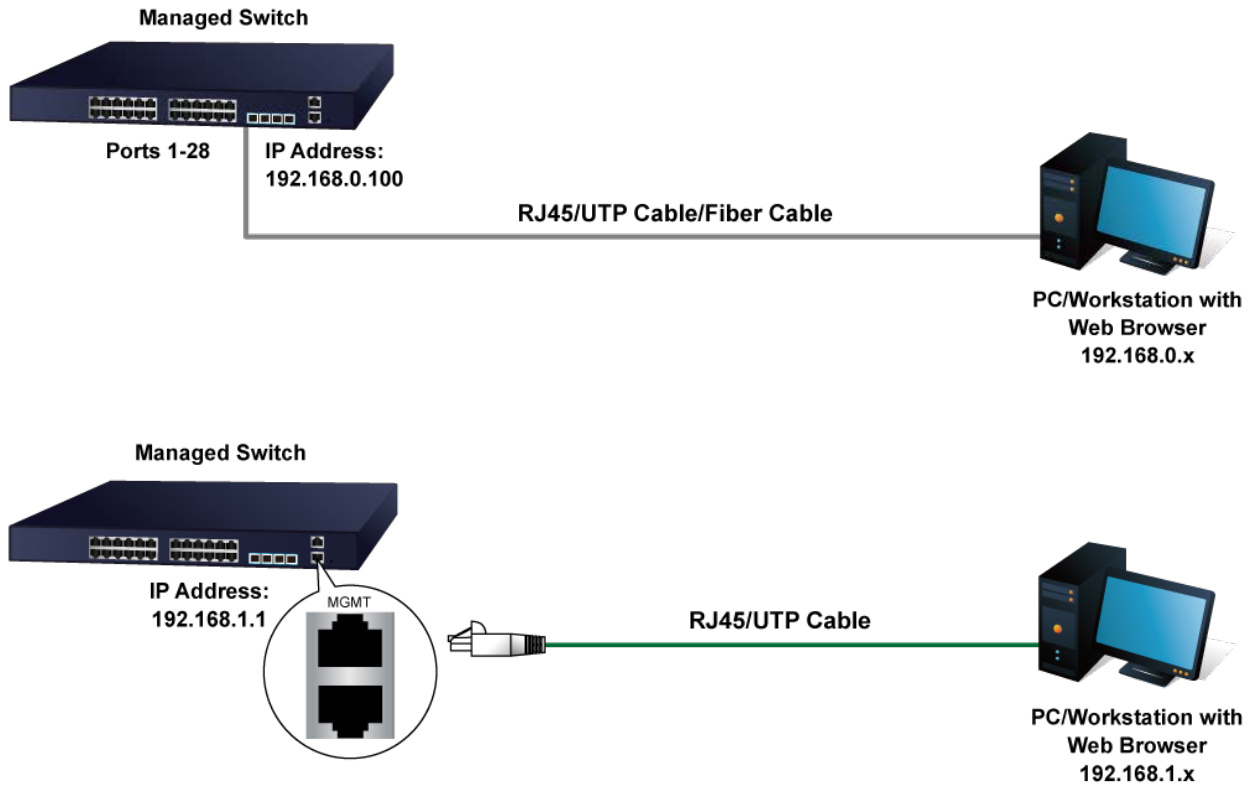


Figure 4-1 IP Management Diagram

The following shows how to start up the **Web Management** of the Managed Switch. Please note the Managed Switch is configured through an Ethernet connection. Please make sure the manager PC must be set to the same **IP subnet address**.

For example, the IP address of the Managed Switch is configured with **192.168.0.100** on **Interface VLAN 1** and **192.168.1.1** on **Management Port**, then the manager PC should be set to **192.168.0.x** or **192.168.1.x** (where x is a number between 1 and 254, except 1 or 100), and the default subnet mask is 255.255.255.0.

The factory default user name and password are as follows:

Default IP of Management Port: **192.168.1.1**
 Default IP of Interface VLAN 1: **192.168.0.100**
 Username: **admin**
 Password: **admin**

■ Logging in to the Managed Switch from Management Port

1. Use Internet Explorer 8.0 or above Web browser and enter IP address <http://192.168.1.1> to access the Web interface.
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 log in the main screen of Managed Switch. The login screen in [Figure 4-1-2](#) appears.

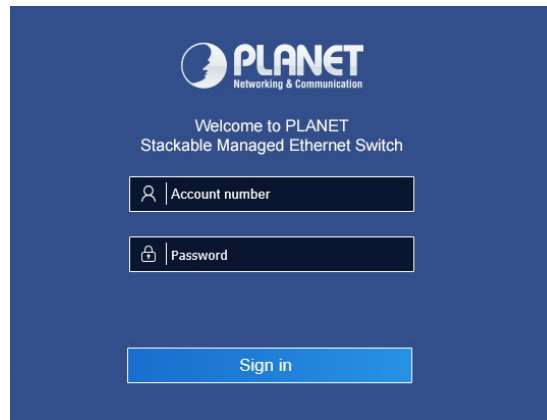


Figure 4-1-2: Login Screen

Default User name: **admin**

Default Password: **admin**

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

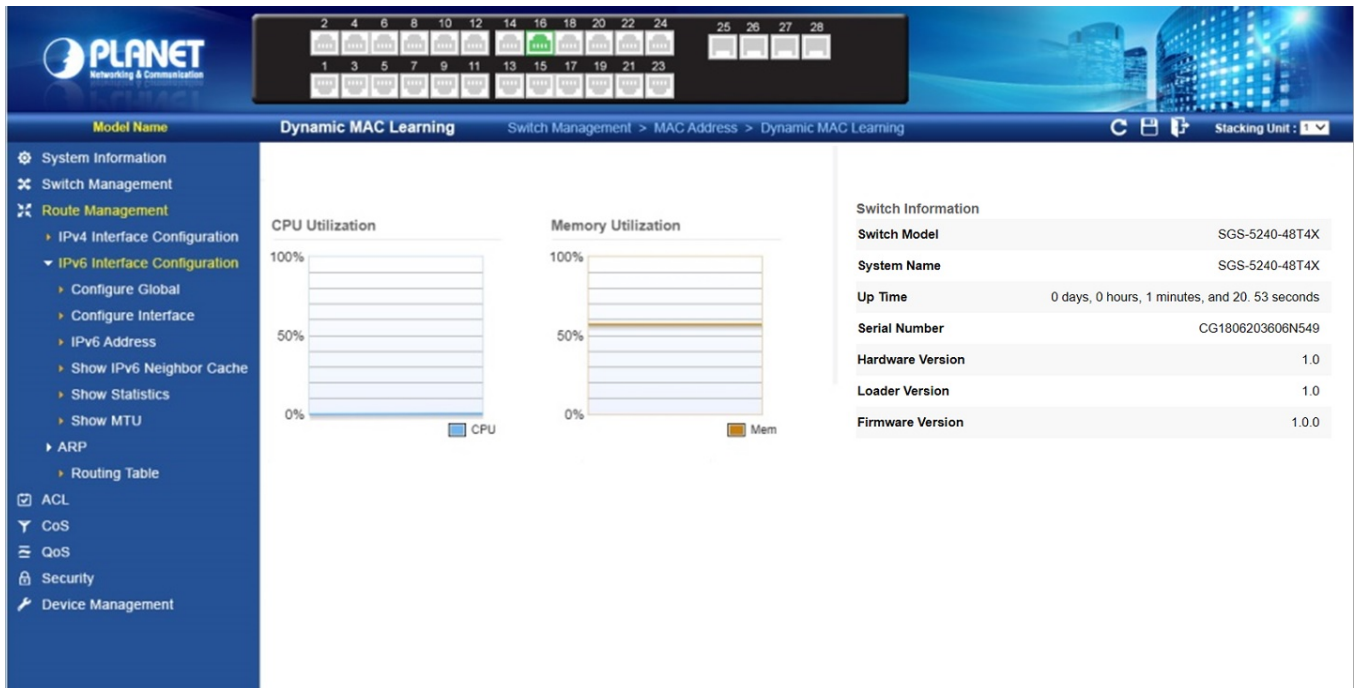


Figure 4-1-3: Web Main Page

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.

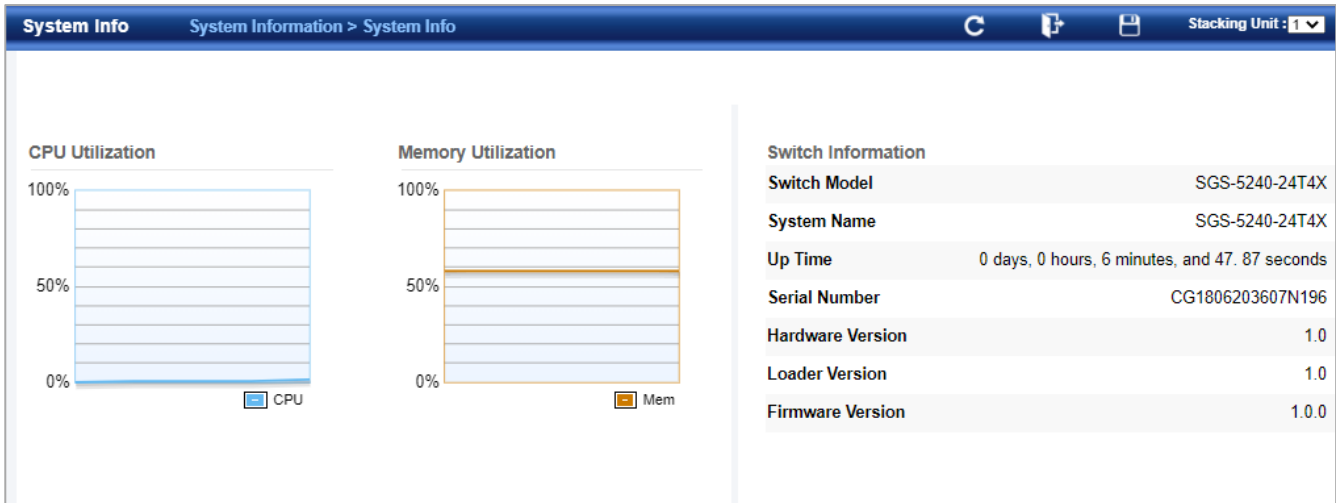


1. It is recommended to use Google Chrome to access Managed Switch.
2. The changed IP address takes effect immediately after clicking on the **Save** button. You need to use the new IP address to access the Web interface.
3. For security reason, please change and memorize the new password after this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

4.1 System Information

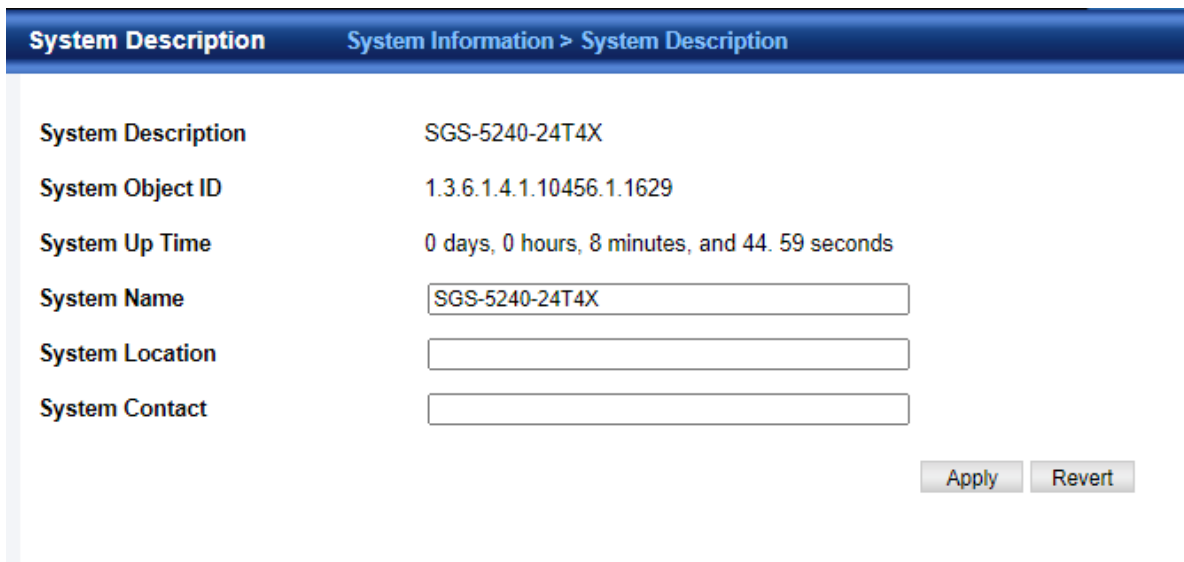
4.1.1 System Info

Use the System Information>System Info page to identify the system by displaying information



4.1.2 System Description

System Information > System Description display the information of the firmware and device.

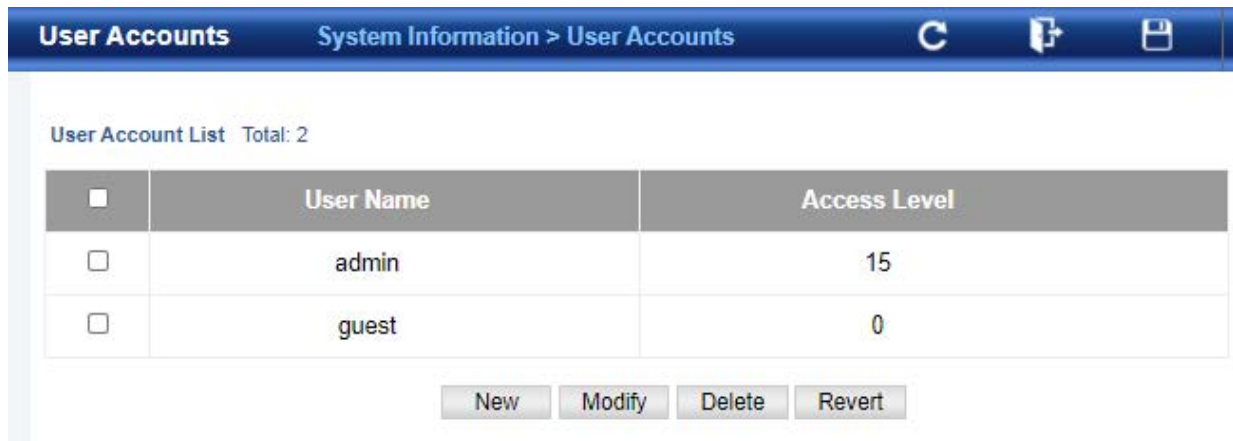


The screenshot shows the 'System Description' page with the following fields and values:

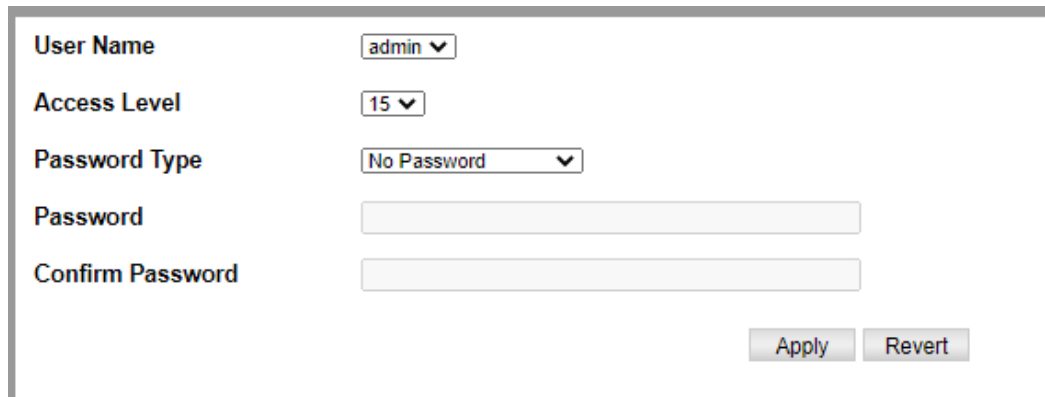
System Description	SGS-5240-24T4X
System Object ID	1.3.6.1.4.1.10456.1.1629
System Up Time	0 days, 0 hours, 8 minutes, and 44.59 seconds
System Name	<input type="text" value="SGS-5240-24T4X"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>

4.1.3 User Accounts

System Information> User Accounts page to control management access to the switch based on manually configured user names and passwords.



<input type="checkbox"/>	User Name	Access Level
<input type="checkbox"/>	admin	15
<input type="checkbox"/>	guest	0



User Name

Access Level

Password Type

Password

Confirm Password

- ◆ **User Name** – The name of the user.
(Maximum length: 32 characters; maximum number of users: 16)
- ◆ **Access Level** – Specifies the user level. (Options: 0 - Normal, 15 - Privileged)
Normal privilege level provides access to a limited number of the commands which display the current status of the switch, as well as several database clear and reset functions. Privileged level provides full access to all commands.
- ◆ **Password Type** – Specifies the following options:
 - **No Password** – No password is required for this user to log in.
 - **Plain Password** – Plain text unencrypted password.
 - **Encrypted Password** – Encrypted password.
The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP or FTP server. There is no need for you to manually configure encrypted passwords.
- ◆ **Password** – Specifies the user password.
(Range: 0-32 characters, case sensitive)
- ◆ **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the password if these two fields do not match.



1. The default guest name is "guest" with the password "guest."
2. The default administrator name is "admin" with the password "admin."

4.2 Switch Management

4.2.1 Jumbo Frame

Use the Switch Management > Jumbo Frame page to configure support for layer 2 jumbo frames. The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 10240 bytes for Gigabit Ethernet. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

Jumbo Frame
Switch Management > Jumbo Frame

General Capability

Jumbo Frame Enabled

Apply
Revert

- ◆ **Jumbo Frame** – Configures support for jumbo frames.
(Default: Disabled)

4.2.2 Interface

4.2.2.1 Port

■ Port Information

Use the Switch Management > Interface > Port > Port Information page to display the information of ports.

Port										
Switch Management > Interface > Port										Stacking Unit: 1
Port Information										Configure
Port	Type	Name	Admin	Status	Autonegotiation	Capability	Oper Speed Duplex	Oper Flow Control	MTU Size	Link Up Down Trap
1	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
2	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
3	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
4	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
5	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
6	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
7	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
8	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled

■ **Configure**

Switch Management >Interface > Port > Configure page is used to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

Port Switch Management > Interface > Port

Port Information

Configure

Mode	<input checked="" type="radio"/> by one port <input type="radio"/> by port range
Port	<input type="text" value="1"/>
Port Name	<input type="text"/>
Admin	<input checked="" type="checkbox"/> Enabled
Autonegotiation	<input checked="" type="checkbox"/> Enabled
	<input checked="" type="checkbox"/> 10half <input checked="" type="checkbox"/> 100half <input checked="" type="checkbox"/> 1000full <input type="checkbox"/> Sym
	<input checked="" type="checkbox"/> 10full <input checked="" type="checkbox"/> 100full <input type="checkbox"/> 10Gfull <input type="checkbox"/> FC
Speed Duplex	<input type="text" value="100full"/>
Flow Control	<input type="checkbox"/> Enabled
MTU Size (1500-9216)	<input type="text" value="1518"/>
Link Up Down Trap	<input checked="" type="checkbox"/> Enabled

Note: FC - flowcontrol; Sym - symmetric .

For more information on command usage and a description of the parameters.

4.2.2.2 sFlow

Switch Management >Interface > sflow page is used to configure sflow.

■ **sFlow Receiver Management**

Receiver Owner Name	<input type="text"/>
Receiver Timeout (30 - 10000000)	<input type="text"/> sec
Receiver Destination	<input type="text"/>
Receiver Socket Port (1 - 65535)	<input type="text"/>
Maximum Datagram Size (200 - 1500)	<input type="text"/> bytes
Datagram Version	<input type="checkbox"/> <input type="text" value="v4"/>

sFlow Switch Management > Interface > sFlow Stacking Unit: 1

sFlow Receiver Management sFlow Management

Receiver List Total: 1

<input type="checkbox"/>	Name	Destination	Socket Port	Version	Max Datagram Size	Timeout
<input type="checkbox"/>	Test	192.168.1.100	22500	5	500	298

Press **'New'** button to set the parameters:

- ◆ **Receiver Owner Name** – The name of the receiver. (Range: 1-256 characters; Default: None)
- ◆ **Type** – Specifies the polling type as an sFlow polling data source for a specified interface that polls periodically based on a specified time interval, or an sFlow data source instance for a specific interface that takes samples periodically based on the number of packets processed.

■ sFlow Management

sFlow Switch Management > Interface > sFlow Stacking Unit: 1

sFlow Receiver Management **sFlow Management**

Receiver Owner Name

Type Sampling Polling

Sampling List Total: 1

<input type="checkbox"/>	Data Source (Unit/Port)	Instance ID	Rate	Maximum Header Size (bytes)
<input type="checkbox"/>	1/1	1	256	256

Press **'New'** button to set the parameters:

- **Data Source** – The source from which the samples will be taken and sent to a collector.
- **Instance ID** – An instance ID used to identify the sampling source. (Range: 1)
- **Sampling Rate** – The number of packets out of which one sample will be taken. (Range: 256-16777215 packets; Default: Disabled)
- **Maximum Header Size** – Maximum size of the sFlow datagram header. (Range: 64-256 bytes)

4.2.2.3 Transceiver

Switch Management>Interface>Transceiver page is used to configure thresholds for alarm and warning messages for optical transceivers which support **Digital Diagnostic Monitoring (DDM)**. This page also displays identifying information for supported transceiver types, and operational parameters for transceivers which support DDM.



	Low Alarm	Low Warning	High Warning	High Alarm
Temperature(°C)	-123.00	0.00	70.00	75.00
Voltage(Volts)	3.10	3.15	3.45	3.50
Current(mA)	6.00	7.00	90.00	100.00
Tx Power(dBm)	-12.00	-11.50	-9.50	-9.00
Rx Power(dBm)	-21.50	-21.00	-3.50	-3.00

- ◆ **Port** – Port number.
- ◆ **General** – Information on connector type and vendor-related parameters.
- ◆ **DDM Information** – Information on temperature, supply voltage, laser bias current, laser power, and received optical power.
The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as **Digital Diagnostic Monitoring (DDM)** provides information on transceiver parameters.
- ◆ **Trap** – Sends a trap when any of the transceiver's operation values falls outside of specified thresholds. (Default: Disabled)
- ◆ **Auto Mode** – Uses default threshold settings obtained from the transceiver to determine when an alarm or trap message should be sent. (Default: Enabled)
- ◆ **DDM Thresholds** – Information on alarm and warning thresholds. The switch can be configured to send a trap when the measured parameter falls outside of the specified thresholds.

The following alarm and warning parameters are supported:

- **High Alarm** – Sends an alarm message when the high threshold is crossed.
- **High Warning** – Sends a warning message when the high threshold is crossed.
- **Low Warning** – Sends a warning message when the low threshold is crossed.
- **Low Alarm** – Sends an alarm message when the low threshold is crossed. The configurable ranges are:
 - **Temperature:** -128.00-128.00 °C
 - **Voltage:** 0.00-6.55 Volts
 - **Current:** 0.00-131.00 mA
 - **Power:** -40.00-8.20 dBm
- The threshold value for Rx and Tx power is calculated as the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW). Threshold values for alarm and warning messages can be configured as described below.

- A high-threshold alarm or warning message is sent if the current value is greater than or equal to the threshold, and the last sample value was less than the threshold. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the high threshold and reaches the low threshold.
- A low-threshold alarm or warning message is sent if the current value is less than or equal to the threshold, and the last sample value was greater than the threshold. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the low threshold and reaches the high threshold.
- Threshold events are triggered as described above to avoid a hysteresis effect which would continuously trigger event messages if the power level were to fluctuate just above and below either the high threshold or the low threshold.
- Trap messages configured by this command are sent to any management station configured as an SNMP trap manager using the Administration > SNMP (Configure Trap) page.

4.2.2.4 Cable Test

Switch Management>Interface>Cable Test page is used to test the cable attached to a port. The cable test will check for any cable faults (short, open, etc.). If a fault is found, the switch reports the length to the fault.

Otherwise, it reports the cable length. It can be used to determine the quality of the cable, connectors, and terminations.

Problems such as opens, shorts, and cable impedance mismatch can be diagnosed with this test.

Cable Test						
Switch Management > Interface > Cable Test						
Cable Test Port List Total: 26						
Port	Test	Test Time	Test Result			
			Pair A	Pair B	Pair C	Pair D
1	<input type="button" value="Test"/>		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
2	<input type="button" value="Test"/>		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
3	<input type="button" value="Test"/>		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
4	<input type="button" value="Test"/>		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
5	<input type="button" value="Test"/>		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
6	<input type="button" value="Test"/>		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
7	<input type="button" value="Test"/>		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
8	<input type="button" value="Test"/>		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet
9	<input type="button" value="Test"/>		Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet

- ◆ **Port** – Switch port identifier.
- ◆ **Type** – Displays media type. (GE – Gigabit Ethernet, Other – SFP+)
- ◆ **Link Status** – Shows if the port link is up or down.
- ◆ **Test Result** – The results include common cable failures, as well as the status and approximate distance to a fault, or the approximate cable length if no fault is found.

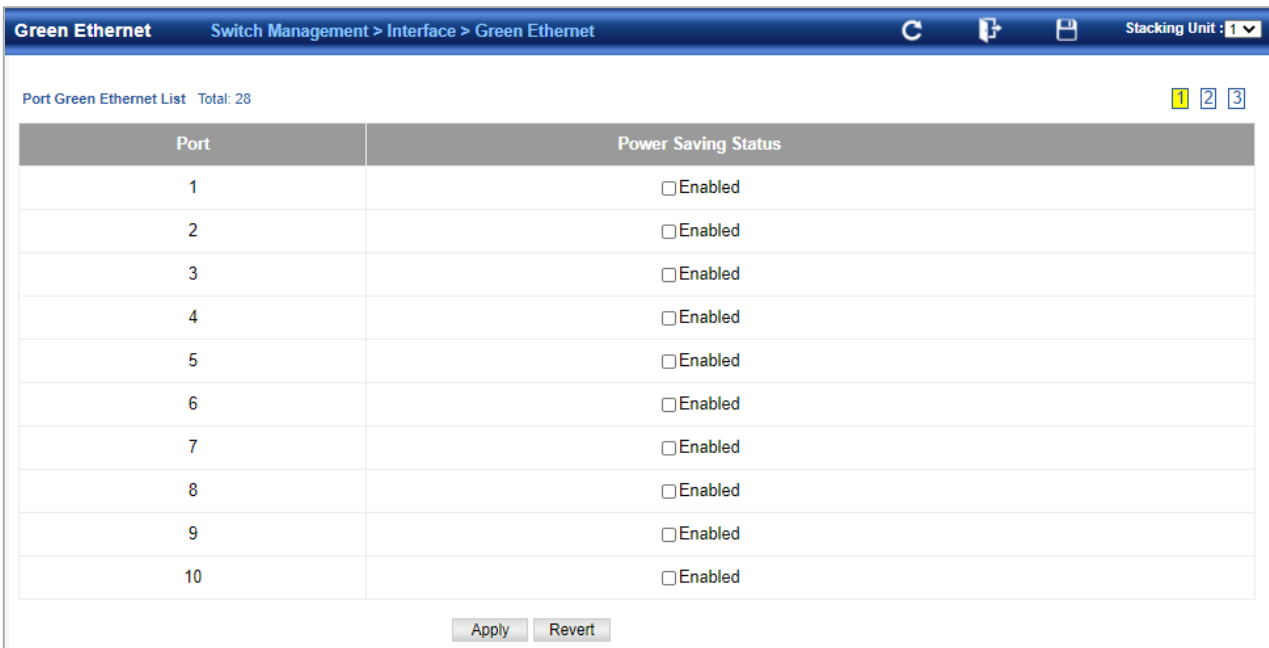
To ensure more accurate measurement of the length to a fault, first disable power-saving mode on the link partner before running cable diagnostics.

For link-down ports, the reported distance to a fault is accurate to within +/- 2 meters. For link-up ports, the accuracy is +/- 10 meters.

- ◆ **Last Updated** – Shows the last time this port was tested.

4.2.2.5 Green Ethernet

Switch Management>Interface>Green Ethernet page is used to enable power savings mode on the selected port.



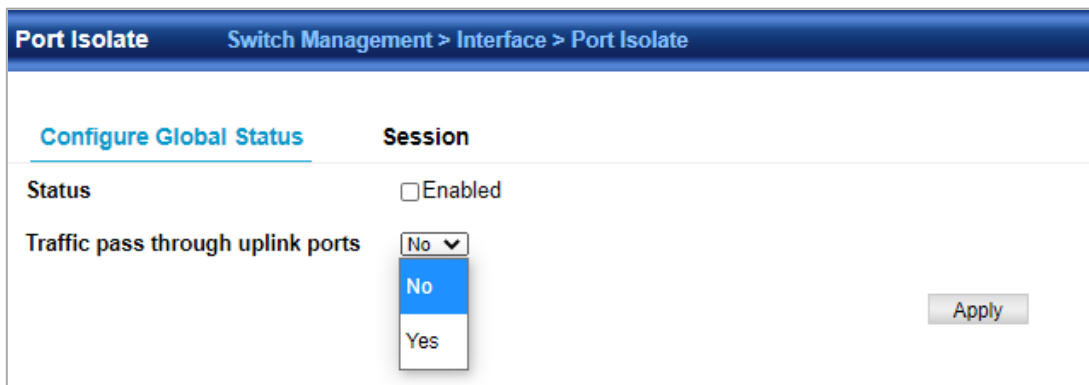
Port	Power Saving Status
1	<input type="checkbox"/> Enabled
2	<input type="checkbox"/> Enabled
3	<input type="checkbox"/> Enabled
4	<input type="checkbox"/> Enabled
5	<input type="checkbox"/> Enabled
6	<input type="checkbox"/> Enabled
7	<input type="checkbox"/> Enabled
8	<input type="checkbox"/> Enabled
9	<input type="checkbox"/> Enabled
10	<input type="checkbox"/> Enabled

These parameters are displayed:

- ◆ **Port** – Power saving mode only applies to the Gigabit Ethernet ports using copper media.
- ◆ **Power Saving Status** – Adjusts the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements. (Default: Enabled on Gigabit Ethernet RJ-45 ports)

4.2.2.6 Port Isolate

Switch Management>Interface> Port Isolate page is used to enable traffic segmentation.



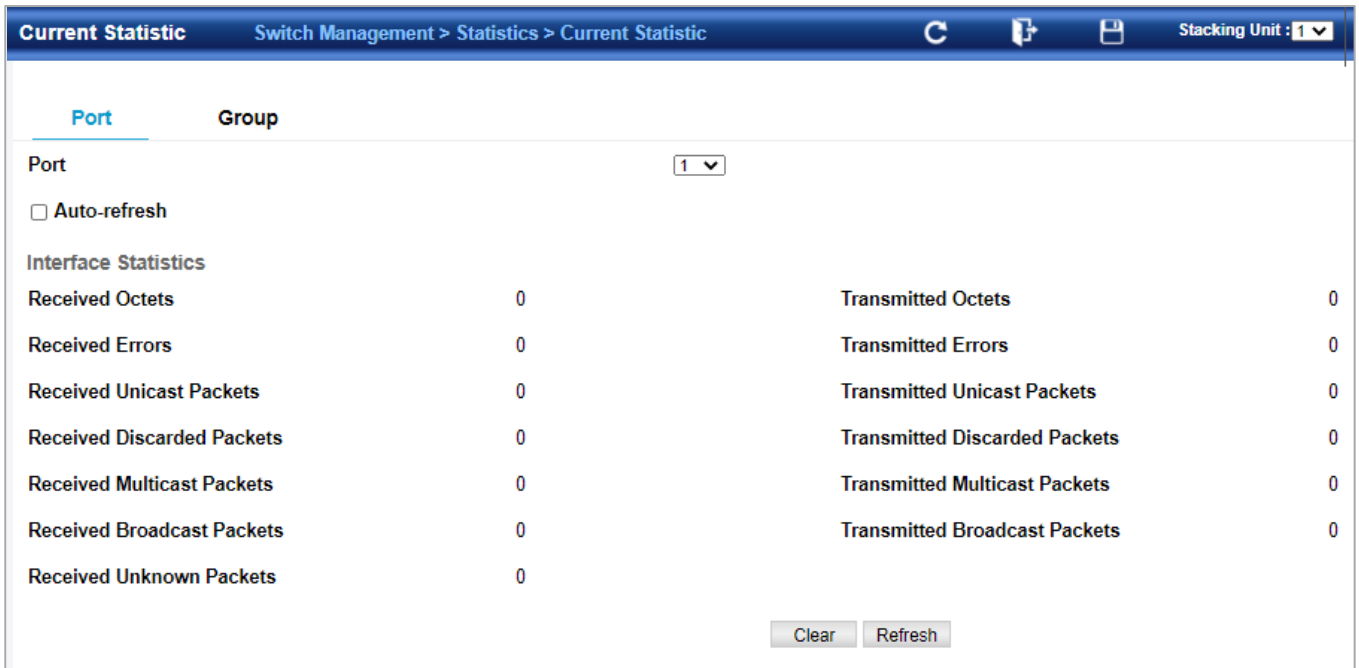
- ◆ **Status** – Enables port-based traffic segmentation. (Default: Disabled)
- ◆ **Traffic pass through uplink ports** – Specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions.
 - **No** – Blocks traffic between uplink ports assigned to different sessions.
 - **Yes** – Forwards traffic between uplink ports assigned to different sessions.

4.2.3 Statistics

4.2.3.1 Current Statistics

Switch management > Statistics > Current Statistic page is used to display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on thermion MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy traffic).

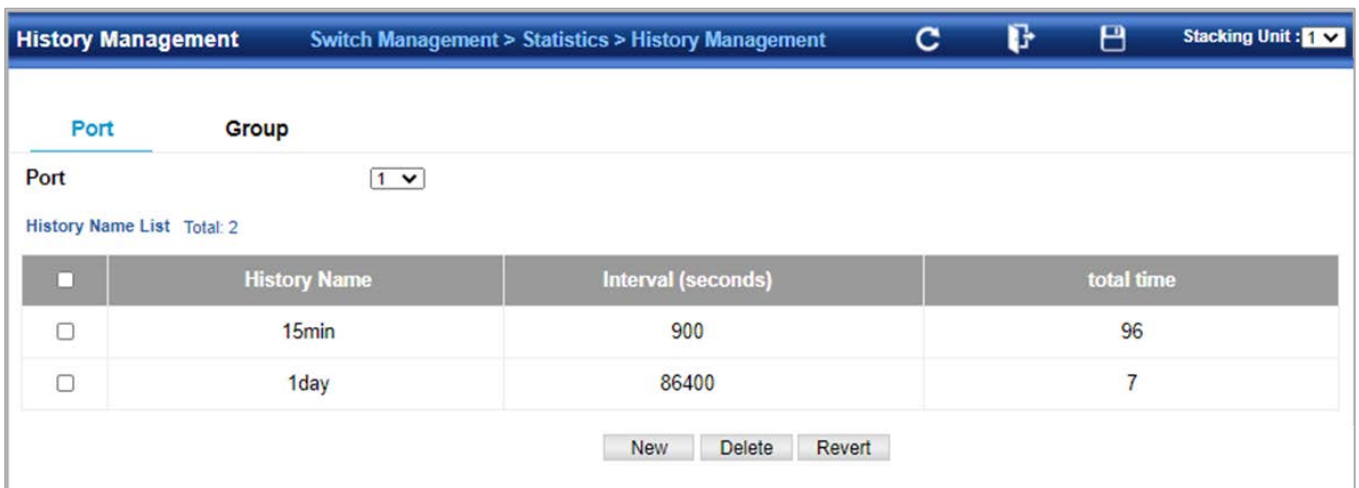
RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.



Current Statistic			
Switch Management > Statistics > Current Statistic			
Port	Group		
Port	1		
<input type="checkbox"/> Auto-refresh			
Interface Statistics			
Received Octets	0	Transmitted Octets	0
Received Errors	0	Transmitted Errors	0
Received Unicast Packets	0	Transmitted Unicast Packets	0
Received Discarded Packets	0	Transmitted Discarded Packets	0
Received Multicast Packets	0	Transmitted Multicast Packets	0
Received Broadcast Packets	0	Transmitted Broadcast Packets	0
Received Unknown Packets	0		
<input type="button" value="Clear"/> <input type="button" value="Refresh"/>			

4.2.3.2 History Management

Switch Management > Statistics > History Management page is used to display statistical history for the specified interfaces.



History Management			
Switch Management > Statistics > History Management			
Port	Group		
Port	1		
History Name List Total: 2			
<input type="checkbox"/>	History Name	Interval (seconds)	total time
<input type="checkbox"/>	15min	900	96
<input type="checkbox"/>	1day	86400	7
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>			

4.2.3.3 History Info

History Info
Stacking Unit: 1

Switch Management > Statistics > History Info

Port: 1 Group: Mode: Ingress history Egress history

Name: 15min

Input Previous Entry List Total: 2

Start Time	%	Octets	Unicast	Multicast	Broadcast	Discarded	Errors	Unknown Proto
00d 00:00:00	0.00	0	0	0	0	0	0	0
00d 00:15:00	0.00	0	0	0	0	0	0	0

4.2.4 VLAN

4.2.4.1 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 VLANs.
2. The Managed Switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.



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.

■ 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 4K VLANs based on the IEEE 802.1Q standard
 1. Port overlapping, allowing a port to participate in multiple VLANs
 2. End stations can belong to multiple VLANs
 3. Passing traffic between VLAN-aware and VLAN-unaware devices
 4. 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:

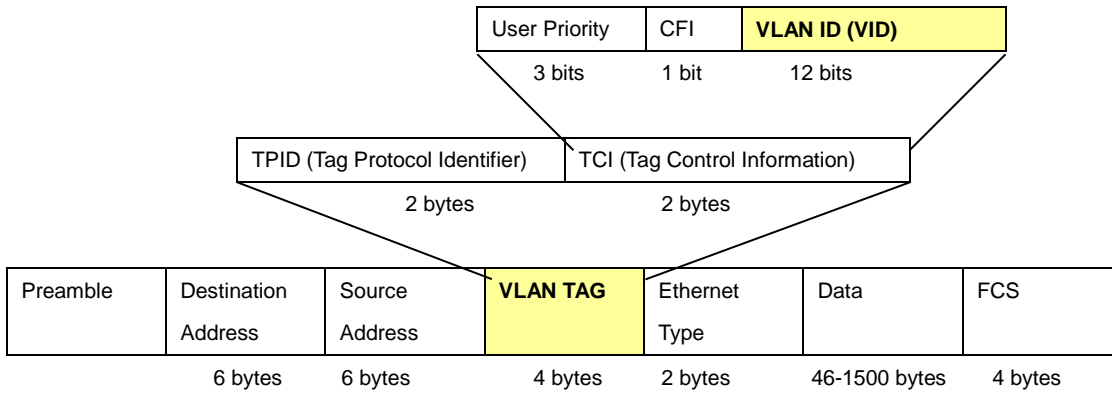
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

■ 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.

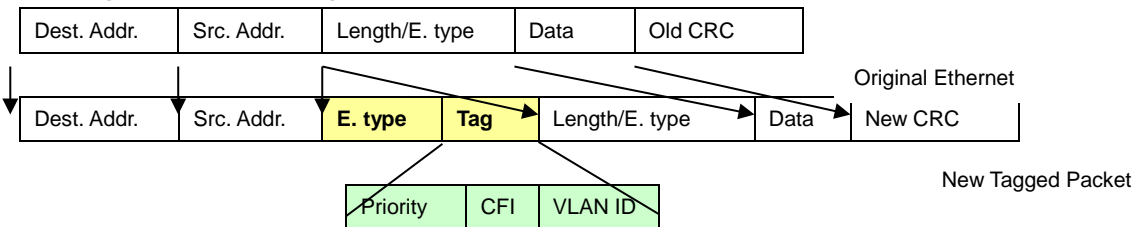
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

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.

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.

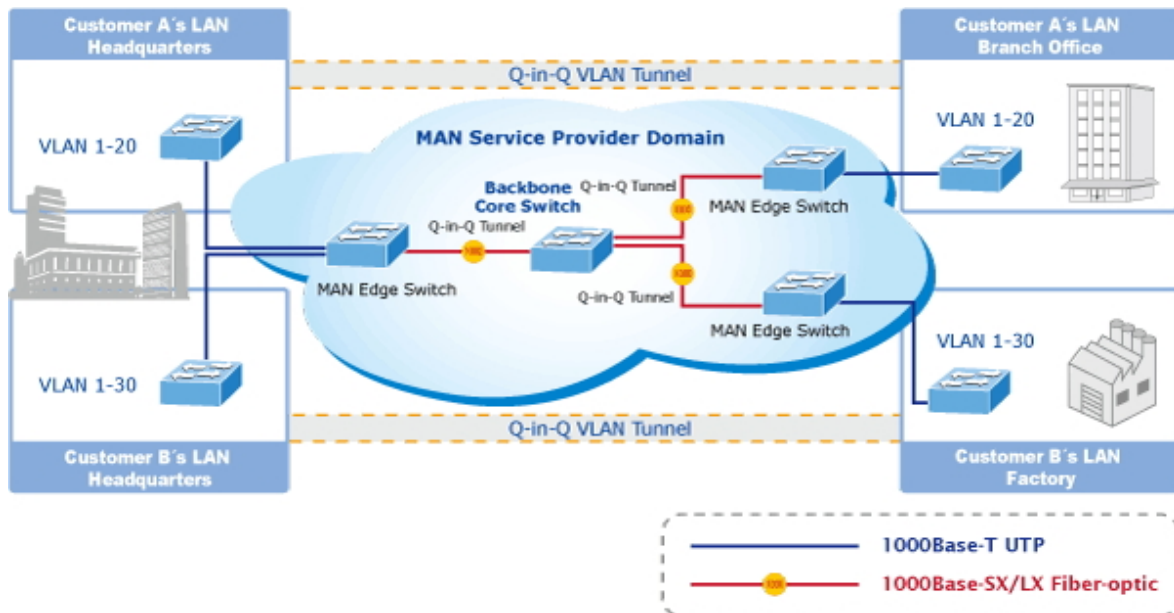
Frame Income / Frame Leave	Income Frame is tagged	Income Frame is untagged
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remains untagged

Table 4-3-3-1: 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.

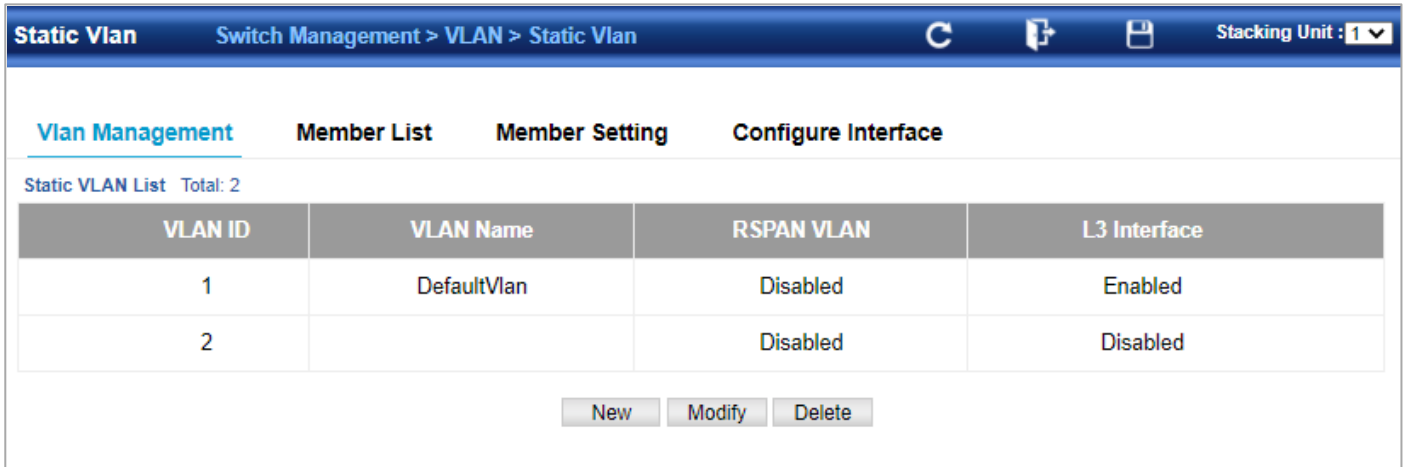
In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements is reduced.

4.2.4.2 Static VLAN

■ VLAN Management

Switch Management >VLAN > Static Vlan > Vlan Management page is used to add, modify or delete static VLAN groups, set administrative status, or specify Remote VLAN type.

To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.



VLAN ID	VLAN Name	RSPAN VLAN	L3 Interface
1	DefaultVlan	Disabled	Enabled
2		Disabled	Disabled

- ◆ **VLAN ID** – ID of VLAN or range of VLANs (1-4093).
Up to 4093 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.
- ◆ **VLAN Name** – Name of the VLAN (1 to 32 characters).
- ◆ **Status** – Enables or disables the specified VLAN.
- ◆ **Remote VLAN** – Reserves this VLAN for RSPAN.
- ◆ **L3 Interface** – Sets the interface to support Layer 3 configuration, and reserves memory space required to maintain additional information about this interface type. This parameter must be enabled before you can assign an IP address to a VLAN

Member List

Switch Management > VLAN > Static Vlan > Member List by vlan page is used to add/delete multiple port members to/from a special vlan.

Static Vlan
Stacking Unit : 1

Switch Management > VLAN > Static Vlan

[Refresh](#)
[Print](#)
[Save](#)

Vlan Management
Member List
Member Setting
Configure Interface

List Type Vlan Interface

VLAN 1

Interface Port Group

Static VLAN Port Member List Total: 16
1
2

Port	Mode	PVID (1-4094)	Acceptable Frame Type	Ingress Filtering	Membership Type
1	Access	1	All	Disabled	Untagged
2	Access	1	All	Disabled	Untagged
3	Access	1	All	Disabled	Untagged
4	Access	1	All	Disabled	Untagged
5	Access	1	All	Disabled	Untagged
6	Access	1	All	Disabled	Untagged

Member Setting

Switch Management > VLAN > Static Vlan > Member Setting by interface page is used to add/delete an interface member to/from multiple vlan

Static Vlan
Stacking Unit : 1

Switch Management > VLAN > Static Vlan

Vlan Management
Member List
Member Setting
Configure Interface

Interface Port Group

Port Range (1-28) -

Member Type Joined

Mode Hybrid

VLAN ID (1-4094) -

Packet Action Tagged Untagged Forbidden

PVID

Apply
Revert

4.2.4.3 GVRP

Switch Management > VLAN > GVRP page is used to enable GVRP globally on the switch, or to enable GVRP and adjust the protocol timers per interface.

◆ **GVRP Status** – GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch. (Default: Disabled)

◆ **Interface** – Displays a list of ports or group.

◆ **Port** – Port Identifier. (Range: 1-28)

◆ **Group** – Group Identifier. (Range: 1-12)

◆ **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect (using the Configure General page). When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)

GVRP cannot be enabled for ports set to Access mode

◆ **GVRP Timers** – Timer settings must follow this rule:

$2 \times (\text{join timer}) < \text{leave timer} < \text{leaveAll timer}$

- **Join** – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)
- **Leave** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group.
(Range: 60-3000 centiseconds; Default: 60)
- **LeaveAll** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000)

Show Dynamic VLAN – Show VLAN

VLAN ID – Identifier of a VLAN this switch has joined through GVRP.

VLAN Name – Name of a VLAN this switch has joined through GVRP.

Status – Indicates if this VLAN is currently operational.

(Display Values: Enabled, Disabled)

Show Dynamic VLAN – Show VLAN Member

◆ **VLAN** – Identifier of a VLAN this switch has joined through GVRP.

◆ **Interface** – Displays a list of ports or groups which have joined the selected VLAN through GVRP.

4.2.4.4 Protocol VLAN

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use. Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the Configure Protocol (Add) page.
3. Then map the protocol for each interface to the appropriate VLAN using the Configure Interface (Add) page.

When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

■ Protocol Mapping Table

Switch Management > VLAN > Protocol Vlan page is used to create and delete a protocol vlan entry.



■	Group ID	Frame Type	Protocol Type
<input type="checkbox"/>	100	Ethernet	08 06

Press **New** button to create a protocol vlan entry:

Group ID (1-2147483647)

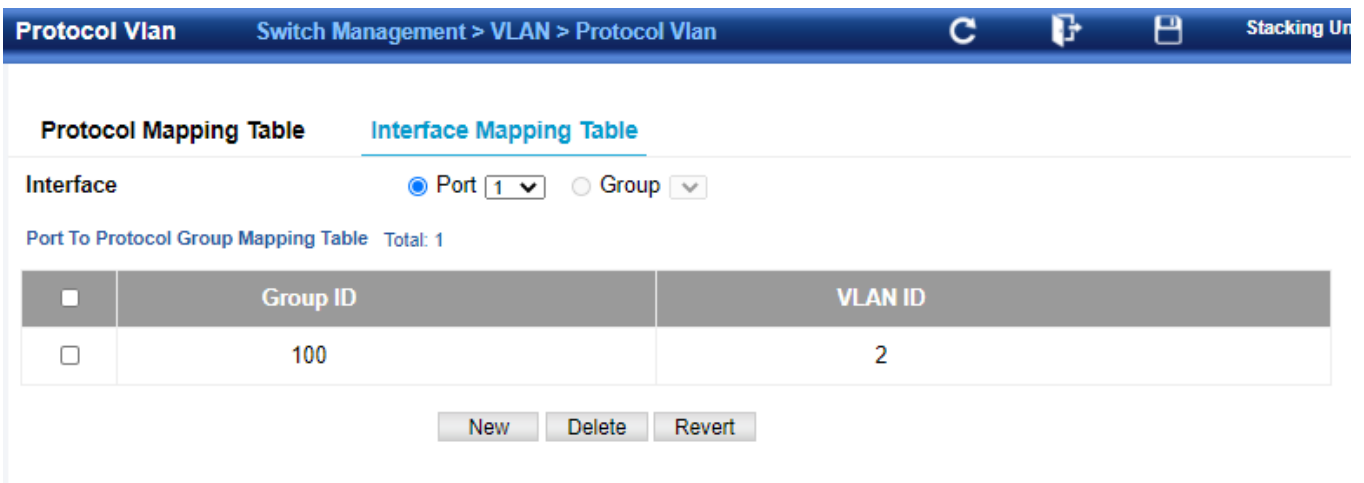
Frame Type

Protocol Type

- ◆ **Group ID** – Protocol Group ID assigned to the Protocol VLAN Group. (Range: 1-2147483647)
- ◆ **Frame Type** – Choose either Ethernet, RFC 1042, or LLC Other as the frame type used by this protocol.
- ◆ **Protocol Type** – Specifies the protocol type to match. The available options are IP, ARP, RARP and IPv6. If LLC Other is chosen for the Frame Type, the only available Protocol Type is IPX Raw.

■ Interface Mapping Table

Switch Management > VLAN > Interface Mapping Table page is used to add/delete an interface member to protocol vlan group.



■	Group ID	VLAN ID
<input type="checkbox"/>	100	2

4.2.4.5 IP Subnet VLAN

Switch Management > VLAN > IP Subnet Vlan page is used to configure IP subnet-based VLANs.

IP Subnet Vlan
Switch Management > VLAN > IP Subnet Vlan

IP Subnet to VLAN Mapping Table Total: 1

<input type="checkbox"/>	IP Address	Subnet Mask	VLAN	Priority
<input type="checkbox"/>	192.168.100.0	255.255.255.0	200	7

Press **New** button to create a IP subnet vlan entry.

IP Address	<input style="width: 95%;" type="text"/>
Subnet Mask	<input style="width: 95%;" type="text"/>
VLAN (1-4094)	<input style="width: 80%;" type="text"/>
Priority (0-7)	<input style="width: 80%;" type="text"/>

◆ **IP Address** – The IP address for a subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.

◆ **Subnet Mask** – This mask identifies the host address bits of the IP subnet.

◆ **VLAN** – VLAN to which matching IP subnet traffic is forwarded.

(Range: 1-4093)

◆ **Priority** – The priority assigned to untagged ingress traffic.

(Range: 0-7, where 7 is the highest priority; Default: 0)

To delete a IP subnet vlan entry, select the entry and press **Delete** button.

4.2.4.6 MAC-Based VLAN

Switch Management > VLAN > Mac-Based Vlan page is used to configure VLAN based on MAC addresses.

MAC-Based Vlan
Switch Management > VLAN > MAC-Based Vlan

MAC-Based VLAN List Total: 1

<input type="checkbox"/>	MAC Address	Mask	VLAN	Priority
<input type="checkbox"/>	A8-F7-E0-11-22-33	FF-FF-FF-FF-FF-FF	20	7

To create a Mac based vlan, press **New** button:

MAC Address (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)
VLAN (1-4094)
Priority (0-7)

- ◆ **MAC Address** – A source MAC address which is to be mapped to a specific VLAN. The MAC address must be specified in the format xx-xxxx-xx-xx-xx.
- ◆ **VLAN** – VLAN to which ingress traffic matching the specified source MAC address is forwarded. (Range: 1-4093)
- ◆ **Priority** – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority; Default: 0)

To delete a Mac based vlan entry, select the entry and press delete button.

4.2.4.7 VLAN Translation

Switch Management > VLAN > Vlan Translation page is used to map VLAN IDs between the customer and service provider for networks that do not support IEEE802.1Q tunneling.

Vlan Translation
Switch Management > VLAN > Vlan Translation

Interface Port Group

Port 2

VLAN Translation Table Total: 1

	Incoming VLAN	Outgoing Vlan
<input type="checkbox"/>	2	100

New
Delete
Revert

Press **New** button to create a vlan translation.

Interface Port Group

Port 2

Incoming VLAN (1-4094)

Outgoing Vlan (1-4094)

Apply
Revert

These parameters are displayed:

- ◆ **Incoming VLAN** – The original VLAN ID. (Range: 1-4093)
- ◆ **Outgoing VLAN** – The new VLAN ID. (Range: 1-4093)

To delete an entry, select the entry and press delete button.

4.2.4.8 QinQ

Switch Management > VLAN > QinQ > QinQ Global Setting page is used to configure the switch to operate in IEEE 802.1Q (QinQ) tunneling mode, which is used for passing Layer 2 traffic across a service provider's metropolitan area network. You can also globally set the **Tag Protocol Identifier (TPID)** value of the tunnel port if the attached client is using a nonstandard 2-byte ether type to identify 802.1Q tagged frames.

■ QinQ Global Setting



- ◆ **Tunnel Status** – Sets the switch to QinQ mode. (Default: Disabled)
- ◆ **Ethernet Type** – The Tag Protocol Identifier (TPID) specifies the ethertype of incoming packets on a tunnel port. (Range: hexadecimal 0800-FFFF; Default: 8100)

■ QinQ VLAN

Switch Management > VLAN > QinQ > QinQ VLAN page is used to configure the QinQ entry.



	Customer VLAN ID	Service VLAN ID
<input checked="" type="checkbox"/>	10	100

Press **New** button to create new QinQ entry.

Port ▼

Customer VLAN ID (1-4094)

Service VLAN ID (1-4094)

To delete an entry, select the entry and press delete button.

■ **QinQ Interface**

Switch Management > VLAN > QinQ > QinQ Interface page is used to set the tunnel mode for any participating interface.

QinQ
Switch Management > VLAN > QinQ

QinQ Global Setting QinQ VLAN QinQ Interface

Interface Port Group

802.1Q Tunnel Port List Total: 28 1 2 3

Port	Mode
1	None ▼
2	None ▼
3	None ▼
4	None ▼
5	None ▼
6	None ▼
7	None ▼
8	None ▼
9	None ▼
10	None ▼

- ◆ **Interface** – Displays a list of ports or groups.
- ◆ **Port** – Port Identifier. (Range: 1-28)
- ◆ **Group** – Group Identifier. (Range: 1-12)
- ◆ **Mode** – Sets the VLAN membership mode of the port.
 - **None** – The port operates in its normal VLAN mode. (This is the default.)
 - **Access** – Configures QinQ tunneling for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
 - **Uplink** – Configures QinQ tunneling for an uplink port to another device within the service provider network.

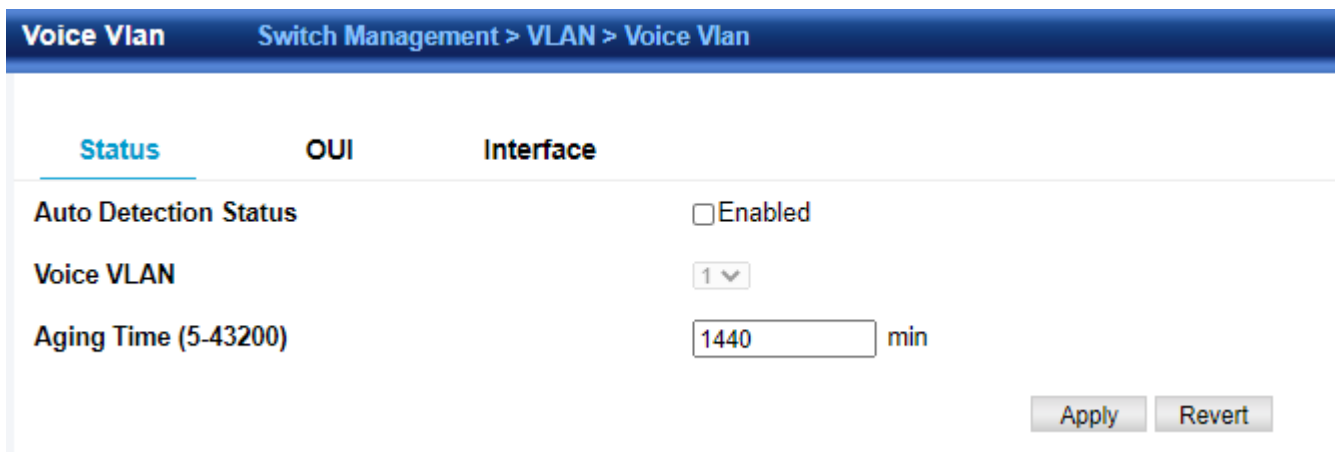
Use the Configure Global page to set the switch to QinQ mode before configuring a QinQ access port or tunnel uplink port.

4.2.4.9 Voice VLAN

Switch Management > VLAN > Voice Vlan > Status page is used to configure the voice vlan.

VLAN membership cannot be set to access mode.

■ Status



- ◆ **Auto Detection Status** – Enables the automatic detection of VoIP traffic on switch ports. (Default: Disabled)
- ◆ **Voice VLAN** – Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported and it must already be created on the switch. (Range: 1-4094)
- ◆ **Aging Time** – The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. (Range: 5-43200 minutes; Default: 1440 minutes)

Note: The Voice VLAN ID cannot be modified when the global Auto Detection Status is enabled.

■ OUI

Switch Management > VLAN > Voice Vlan > OUI page is used to configure the Organizational Unique Identifier (OUI) in the source MAC address of received packets.

Voice Vlan Switch Management > VLAN > Voice Vlan C ↗ 📄 Stacking Unit : 1 ▼

Status OUI **Interface**

Telephony OUI List Total: 1

<input type="checkbox"/>	Telephony OUI	Mask	Description
<input type="checkbox"/>	00-30-4F-00-00-00	FF-FF-FF-00-00-00	PLANET IP Phones

To create a OUI, press **New** button.

Telephony OUI (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)
Mask (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)
Description

- ◆ **Telephony OUI** – Specifies a MAC address range to add to the list. Enter the MAC address in format 01-23-45-67-89-AB.
- ◆ **Mask** – Identifies a range of MAC addresses. Setting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Setting a mask of FF-FF-FF-FF-FF-FF specifies a single MAC address. (Default: FF-FF-FF-00-00-00)
- ◆ **Description** – User-defined text that identifies the VoIP devices

To delete a OUI, select the OUI and press delete button.

■ **Interface**

Switch Management > VLAN > Voice Vlan > Interface Management page is used to configure ports for voice vlan, you need to set the mode (Auto or Manual), specify the discovery method to use, and set the traffic priority. You can also enable security filtering to ensure that only voice vlan traffic is forwarded on the Voice VLAN.

Voice Vlan Switch Management > VLAN > Voice Vlan Stacking Unit: 1

Status OUI Interface

VoIP Port List Total: 28 1 2 3

Port	Mode	Security	Discovery Protocol	Priority (0-6)	Remaining Age (minutes)
1	None	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA
2	None	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA
3	None	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA
4	None	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA
5	None	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA
6	None	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA
7	None	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA
8	None	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA
9	None	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA
10	None	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> OUI <input type="checkbox"/> LLDP	6	NA

Apply Revert

All ports are set to VLAN hybrid mode by default. Prior to enabling VoIP for a port (by setting the VoIP mode to Auto or Manual as described below), first ensure that VLAN membership is not set to access mode.

- ◆ **Mode** – Specifies if the port will be added to the Voice VLAN when VoIP traffic is detected. (Default: None)
 - **None** – The Voice VLAN feature is disabled on the port. The port will not detect VoIP traffic or be added to the Voice VLAN.
 - **Auto** – The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port. You must select a method for detecting VoIP traffic, either OUI or 802.1AB (LLDP). When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list.
 - **Manual** – The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.
- ◆ **Security** – Enables security filtering that discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped. (Default: Disabled)
- ◆ **Discovery Protocol** – Selects a method to use for detecting VoIP traffic on the port. (Default: OUI)
 - **OUI** – Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to vendors and form the first three octets of a device MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.
 - **LLDP** – Uses LLDP (IEEE 802.1AB) to discover voice vlan devices attached to the port. LLDP checks that the “telephone bit” in the system capability TLV is turned on.
- ◆ **Priority** – Defines a CoS priority for port traffic on the Voice VLAN. The priority of any received voice vlan packet is overwritten with the new priority when the Voice VLAN feature is active for the port. (Range: 0-6; Default: 6)
- ◆ **Remaining Age** – Number of minutes before this entry is aged out.

The Remaining Age starts to count down when the OUI's MAC address expires from the MAC address table. Therefore, the MAC address aging time should be added to the overall aging time.

For example, if you configure the MAC address table aging time to 30 seconds, and the voice VLAN aging time to 5 minutes, then after 5.5 minutes, a port will be removed from voice VLAN when voice vlan traffic is no longer received on the port.

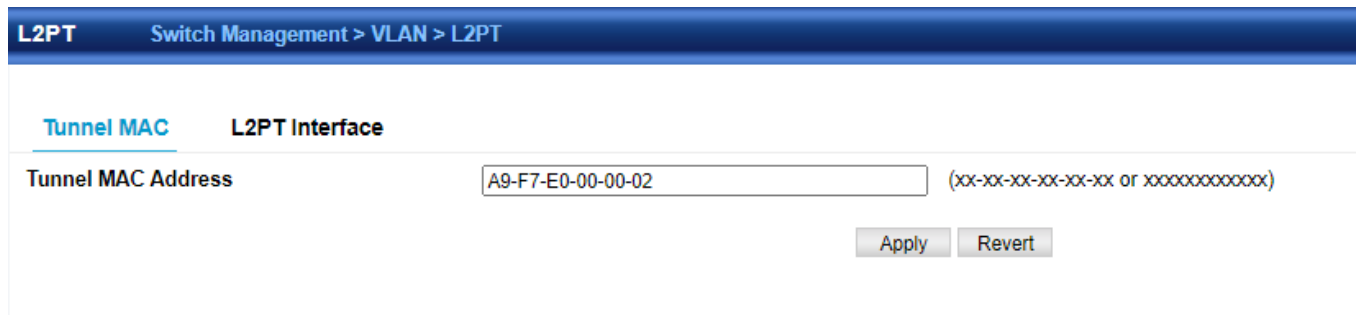
Alternatively, if you clear the MAC address table manually, then the switch will also start counting down the Remaining Age.

4.2.4.10 L2PT

Switch Management > VLAN > L2PT is used to configure the I2 protocol tunnel.

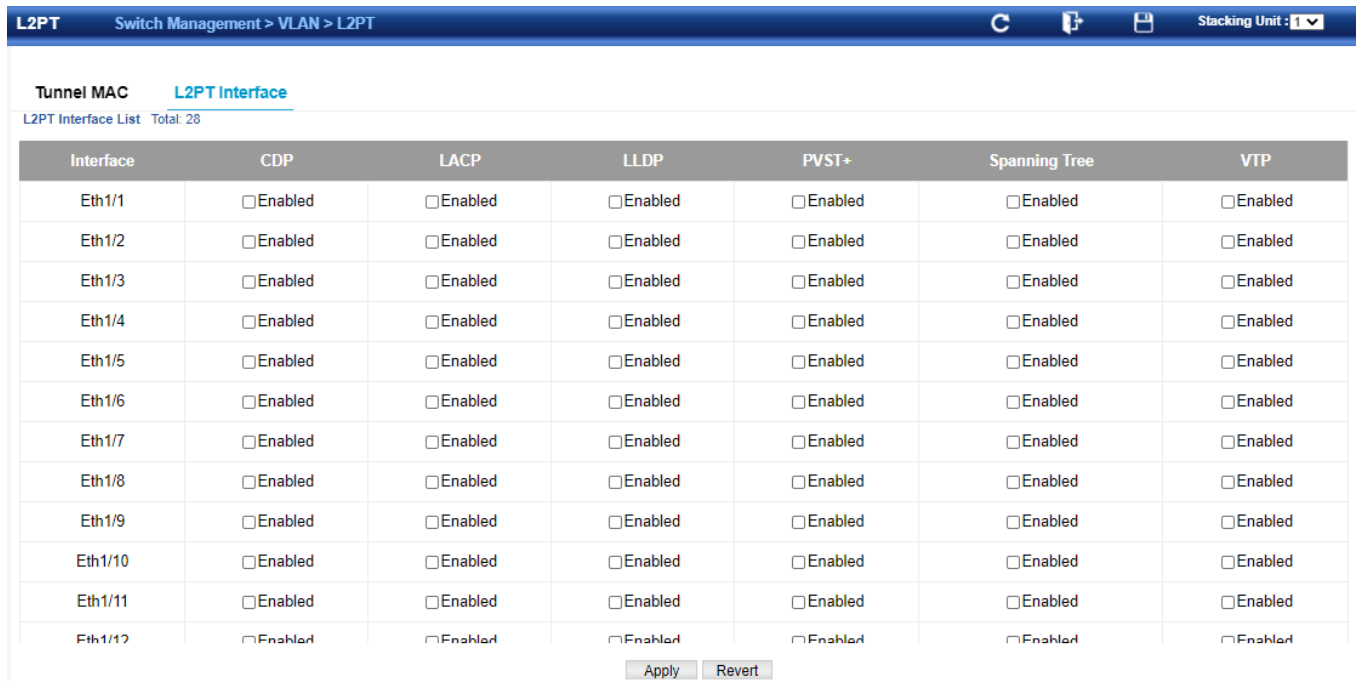
■ Tunnel MAC page:

Used to configure the destination of the tunnel.



■ L2PT Interface page:

Used to configure which protocol will pass through in the tunnel.



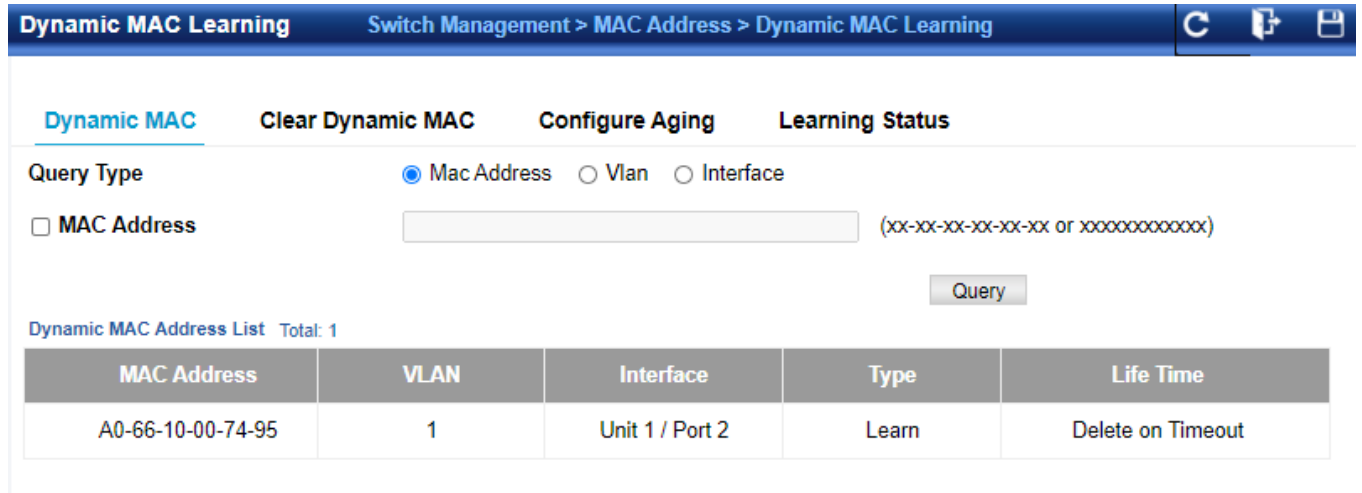
Interface	CDP	LACP	LLDP	PVST+	Spanning Tree	VTP
Eth1/1	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
Eth1/2	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
Eth1/3	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
Eth1/4	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
Eth1/5	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
Eth1/6	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
Eth1/7	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
Eth1/8	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
Eth1/9	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
Eth1/10	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
Eth1/11	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
Eth1/12	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled

4.2.5 MAC Address

4.2.5.1 Dynamic MAC Learning

■ Dynamic MAC

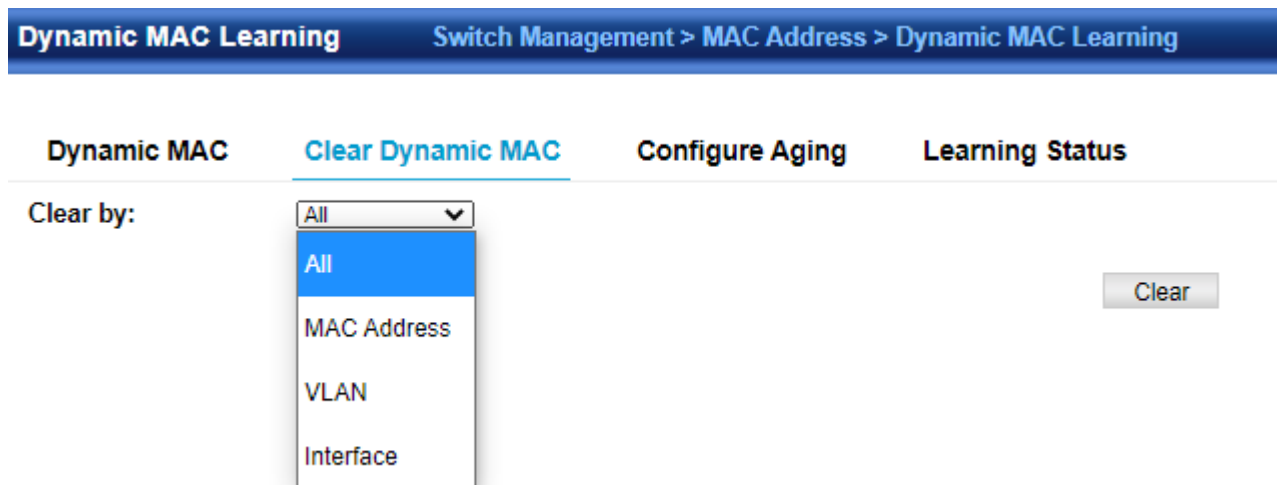
Switch Management >MAC Address > Dynamic MAC Learning> Dynamic Mac page is used to display the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.



MAC Address	VLAN	Interface	Type	Life Time
A0-66-10-00-74-95	1	Unit 1 / Port 2	Learn	Delete on Timeout

■ Clear Dynamic MAC

Switch Management >MAC Address > Dynamic MAC Learning> Clear Dynamic MAC page is used to remove any learned entries from the forwarding database.



◆**Clear by** – All entries can be cleared; or you can clear the entries for a specific MAC address, all the entries in a VLAN, or all the entries associated with a port or group.

■ Configure Aging

Switch Management >MAC Address > Dynamic MAC Learning> Configure Aging page is used to set the aging time for entries in the dynamic address table. The aging time is used to age out dynamically learned forwarding information.

Dynamic MAC Clear Dynamic MAC Configure Aging Learning Status

Aging Status Enabled

Aging Time (10-1000000) sec

Apply Revert

■ Learning Status

Switch Management >MAC Address > Dynamic MAC Learning> Learning status page is used to set learning status on port.

Dynamic MAC Clear Dynamic MAC Configure Aging Learning Status

Interface Port Group

Port Learning Status List Total: 28

Port	Status
1	<input checked="" type="checkbox"/> Enabled
2	<input checked="" type="checkbox"/> Enabled
3	<input checked="" type="checkbox"/> Enabled
4	<input checked="" type="checkbox"/> Enabled
5	<input checked="" type="checkbox"/> Enabled
6	<input checked="" type="checkbox"/> Enabled
7	<input checked="" type="checkbox"/> Enabled
8	<input checked="" type="checkbox"/> Enabled
9	<input checked="" type="checkbox"/> Enabled
10	<input checked="" type="checkbox"/> Enabled

Apply Revert

4.2.5.2 Static Mac Setting

Switch Management > MAC Address > Static Mac Setting page is used to configure static MAC addresses.

Static Mac Setting					
Switch Management > MAC Address > Static Mac Setting					
Static MAC Address to Interface Mapping Table Total: 1					
<input type="checkbox"/>	MAC Address	VLAN	Interface	Type	Life Time
<input type="checkbox"/>	EC-D6-8A-33-A2-3A	1	CPU	CPU	Power On
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>					

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

To configure a static MAC address:

1. Click Switch Management, MAC Address, Static Mac Setting, New button.
2. Specify the VLAN, the port or group to which the address will be assigned, the MAC address, and the time to retain this entry.
3. Click Apply.

VLAN

Interface Port Group

MAC Address (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)

Static Status

- ◆ **VLAN** – ID of configured VLAN. (Range: 1-4093)
- ◆ **Interface** – Port or group associated with the device assigned a static address.
- ◆ **MAC Address** – Physical address of a device mapped to this interface.
Enter an address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
- ◆ **Static Status** – Sets the time to retain the specified address.
 - Delete-on-reset - Assignment lasts until the switch is reset.
 - Permanent - Assignment is permanent. (This is the default.)

◆ Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

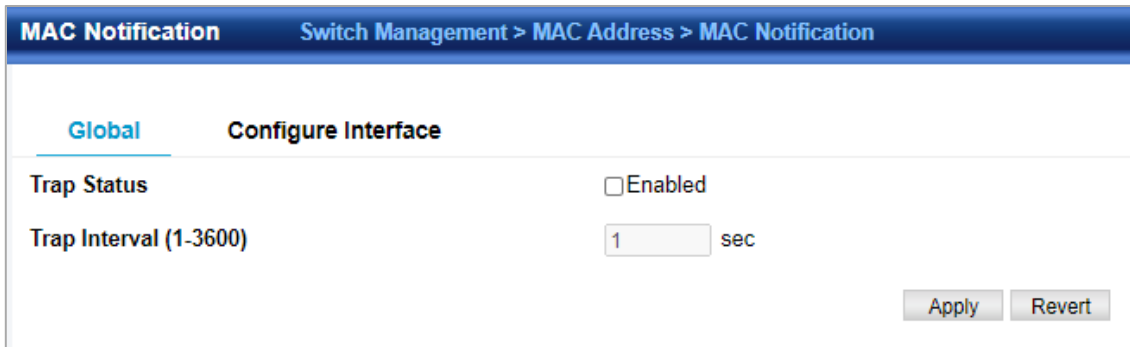
◆ Static addresses will not be removed from the address table when given interface link is down.

◆ A static address cannot be learned on another port until the address is removed from the table.

4.2.5.3 MAC Notification

Switch Management > MAC Address > MAC Notification page is used to send SNMP traps (i.e., SNMP notifications) when a dynamic MAC address is added or removed.

■ Configure Global



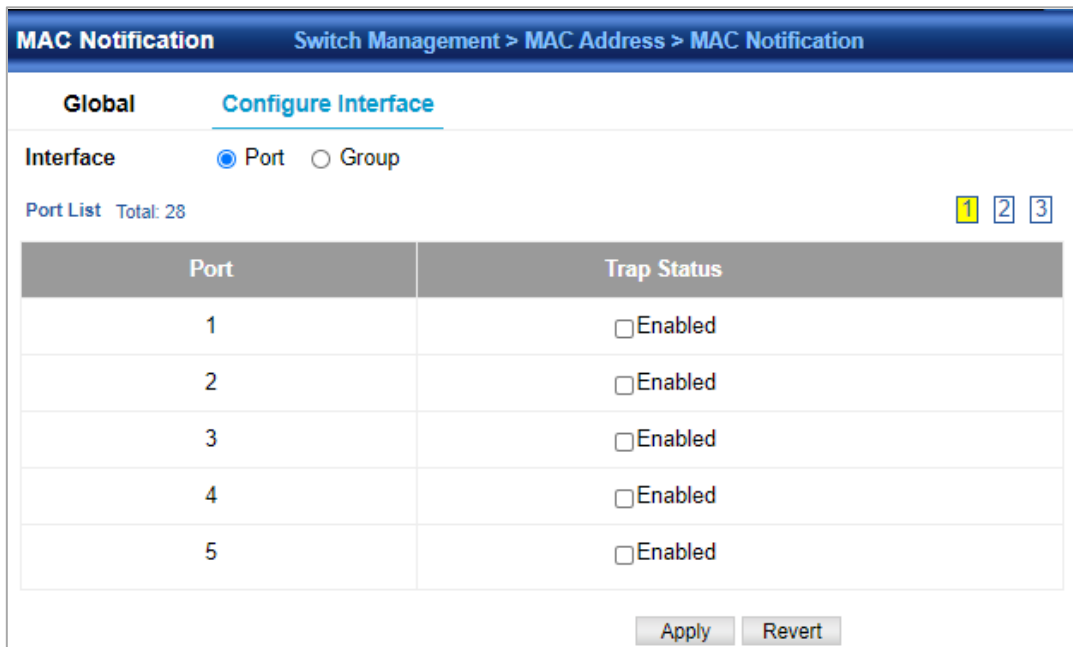
- ◆ Trap Status – Issues a trap when a dynamic MAC address is added or removed. (Default: Disabled)
- ◆ Trap Interval – Specifies the interval between issuing two consecutive traps. (Range: 1-3600 seconds; Default: 1 second)

Configure Interface

- ◆ Port – Port Identifier. (Range: 1-28/52)
 - ◆ Trap Status – Enables MAC authentication traps on the current interface. (Default: Disabled)
- MAC authentication traps must be enabled at the global level for this attribute to take effect.

■ Configure Interface

To enable MAC address traps at the global level:



Port	Trap Status
1	<input type="checkbox"/> Enabled
2	<input type="checkbox"/> Enabled
3	<input type="checkbox"/> Enabled
4	<input type="checkbox"/> Enabled
5	<input type="checkbox"/> Enabled

1. Click Switch Management, MAC Address, MAC Notification.
2. Select Global from the Step list.
3. Configure MAC notification traps and the transmission interval.
4. Click Apply.

4.2.6 Port Mirror

4.2.6.1 Local Port Mirror

Switch Management > Port Mirror > Local Port Mirror page is used to mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

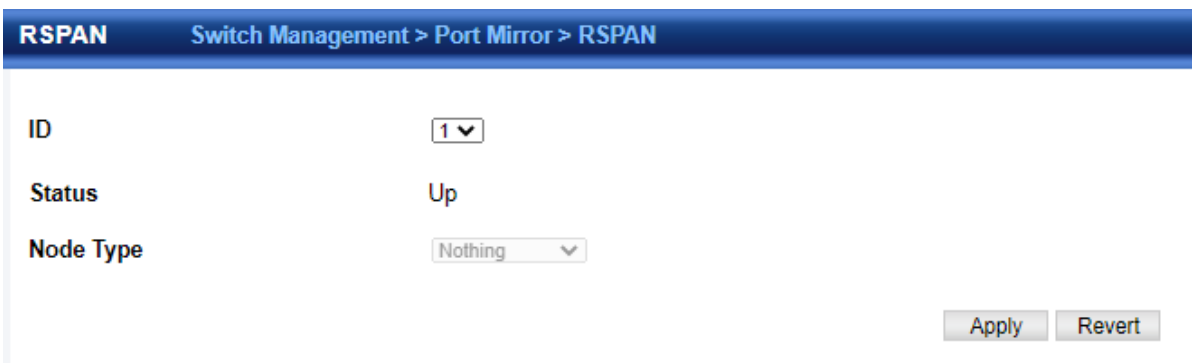


ID	Source Port (Unit/Port)	Destination Port (Unit/Port)
1	1 / 1 (Both)	1 / 24

- ◆ **Source Port** – The port whose traffic will be monitored.
- ◆ **Target Port** – The port that will mirror the traffic on the source port.
- ◆ **Type** – Allows you to select which traffic to mirror to the target port, Rx(receive), Tx (transmit), or Both. (Default: Rx)

4.2.6.2 RSPAN

Switch Management > Port Mirror > RSPAN page is used to mirror traffic from remote switches for analysis at a destination port on the local switch.



Take the following step to configure an RSPAN session:

1. Use the VLAN Static List to reserve a VLAN for use by RSPAN (marking the “Remote VLAN” field on this page. (Default VLAN 1 is prohibited.)
2. Set up the source switch on the RSPAN configuration page by specifying the mirror session, the switch’s role (Source), the RSPANVLAN, and the uplink port1. Then specify the source port(s), and the traffic type to monitor (Rx, Tx or Both).
3. Set up all intermediate switches on the RSPAN configuration page, entering the mirror session, the switch’s role (Intermediate), the RSPAN VLAN, and the uplink port(s).
4. Set up the destination switch on the RSPAN configuration page by specifying the mirror session, the switch’s role (Destination), the destination port, whether or not the traffic exiting this port will be tagged or untagged, and the RSPAN VLAN. Then specify each uplink port where the mirrored traffic is being received.

◆ RSPAN Limitations

The following limitations apply to the use of RSPAN on this switch:

- *RSPAN Ports* – Only ports can be configured as an RSPAN source, destination, or uplink; static and dynamic trunks are not allowed. A port can only be configured as one type of RSPAN interface –source, destination, or uplink. Also, note that the source port and destination port cannot be configured on the same switch.
- *Local/Remote Mirror* – The destination of a local mirror session (created on the Interface > Port > Mirror page) cannot be used as the destination for RSPAN traffic.
- *Spanning Tree* – If the spanning tree is disabled, BPDUs will not be flooded onto the RSPAN VLAN.
- MAC address learning is not supported on RSPAN uplink ports when RSPAN is enabled on the switch. Therefore, even if spanning tree is enabled after RSPAN has been configured, MAC address learning will still not be re-started on the RSPAN uplink ports.
- *IEEE 802.1X* – RSPAN and 802.1X are mutually exclusive functions.
- When 802.1X is enabled globally, RSPAN uplink ports cannot be configured, even though RSPAN source and destination ports can still be configured. When RSPAN uplink ports are enabled on the switch, 802.1X cannot be enabled globally.
- *Port Security* – If port security is enabled on any port, that port cannot be set as an RSPAN uplink port, even though it can still be configured as an RSPAN source or destination port. Also, when a port is configured as an RSPAN uplink port, port security cannot be enabled on that port.

◆ Session – A number identifying this RSPAN session. (Range: 1)

Only one mirror session is allowed, including both local and remote mirroring. If local mirroring is enabled, then no session can be configured for RSPAN.

- ◆ **Operation Status** – Indicates whether or not RSPAN is currently functioning.
- ◆ **Switch Role** – Specifies the role this switch performs in mirroring traffic.
 - **None** – This switch will not participate in RSPAN.
 - **Source** - Specifies this device as the source of remotely mirrored traffic.
 - **Intermediate** - Specifies this device as an intermediate switch, transparently passing mirrored traffic from one or more sources to one or more destinations.
 - **Destination** - Specifies this device as a switch configured with a destination port which is to receive mirrored traffic for this session.
- ◆ **Remote VLAN** – The VLAN to which traffic mirrored from the source port will be flooded. The VLAN specified in this field must first be reserved for the RSPAN application using the Switch Management >VLAN > Static Vlan page.
- ◆ **Uplink Port** – A port on any switch participating in RSPAN through which mirrored traffic is passed on to or received from the RSPANVLAN.

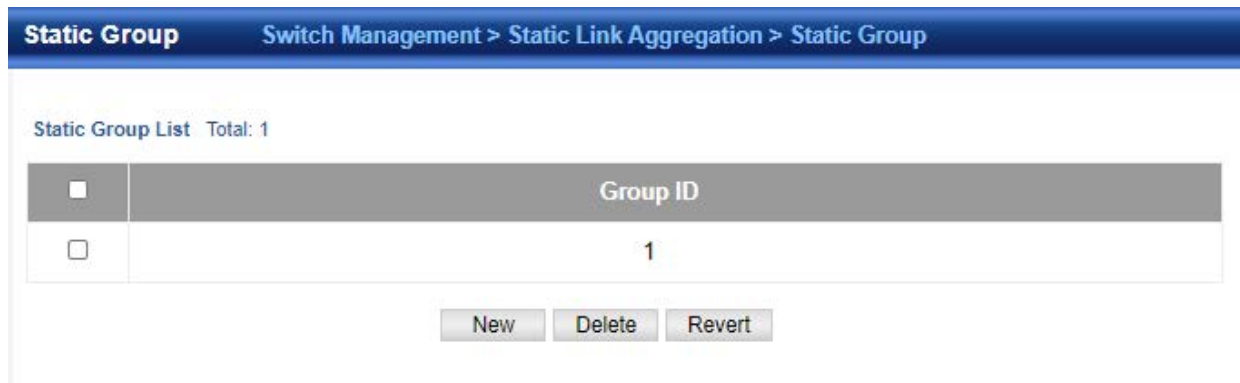
Only one uplink port can be configured on a source switch, but there is no limitation on the number of uplink ports configured on an intermediate or destination switch.

Only destination and uplink ports will be assigned by the switch as members of the RSPAN VLAN. Ports cannot be manually assigned to an RSPAN VLAN through the Switch Management >VLAN > Static Vlan page. Nor can GVRP dynamically add port members to an RSPAN VLAN. Also, note that the Switch Management >VLAN > Static Vlan page will not display any members for an RSPANVLAN, but will only show configured RSPAN VLAN identifiers.
- ◆ **Type** – Specifies the traffic type to be mirrored remotely. (Options: Rx,Tx, Both)
- ◆ **Destination Port** – Specifies the destination port to monitor the traffic mirrored from the source ports. Only one destination port can be configured on the same switch per session, but a destination port can be configured on more than one switch for the same session. Also note that a destination port can still send and receive switched traffic, and participate in any Layer 2 protocols to which it has been assigned.
- ◆ **Tag** – Specifies whether or not the traffic exiting the destination port through the monitoring device carries the RSPAN VLAN tag.

4.2.7 Static Link Aggregation

4.2.7.1 Static Group

Switch Management > Static Link Aggregation > Static Group page is used to create and delete static trunk group.



<input type="checkbox"/>	Group ID
<input type="checkbox"/>	1

To create a static trunk group, press New button. You can create a new group.

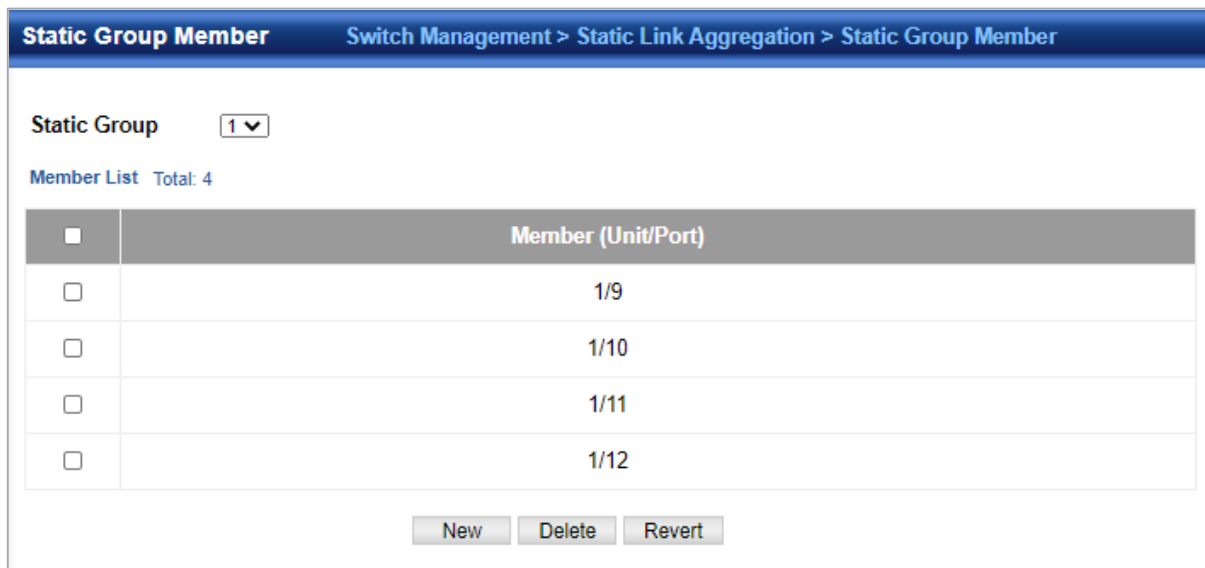
Group ID (1-26)

The static Group configuration will override the LACP configuration.

◆ **Group ID** – Trunk identifier. (Range: 1-12)

4.2.7.2 Static Group Member

Switch Management > Static Link Aggregation > Static Group member page is used to add and delete static group member.



Static Group 1 ▼

Member List Total: 4

<input type="checkbox"/>	Member (Unit/Port)
<input type="checkbox"/>	1/9
<input type="checkbox"/>	1/10
<input type="checkbox"/>	1/11
<input type="checkbox"/>	1/12

Member – The initial group member.

Unit – Unit identifier. (Range: 1)

Port – Port identifier. (Range: 1-28)

4.2.7.3 Static Trunk Management

Switch Management > Static Link Aggregation > Static Group Parameters page is used to configure the parameters of trunk group.

Static Group Parameters										
Switch Management > Static Link Aggregation > Static Group Parameters										Stacking Unit : 1
Static Group List Total: 1										
Group	Type	Name	Admin	Status	Autonegotiation	Capability	Speed Duplex	Flow Control	MTU Size	Link Up Down Trap
1	1000BASE-T		Enabled	Down	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled
Configure										
Note: FC - flowcontrol.										

To configure the parameters, button configure button.

Mode by one Group by Group range

Group

Group Name

Admin Enabled

Autonegotiation Enabled

10half 100half 1000full FC

10full 100full Sym

Speed Duplex

Flow Control Enabled

MTU Size (1500-9216)

Link Up Down Trap Enabled

[Apply](#) [Revert](#)

Note: FC - flowcontrol; Sym - symmetric .

4.2.8 LACP

4.2.8.1 Group Member

Switch Management > LACP > Group Member page is used to configure parameters of Group.

Group Member Switch Management > LACP > Group Member

Join Group Member Port Priority

Port List Total: 28 1 2 3

Port	Group(0-26)
1	<input type="text" value="0"/>
2	<input type="text" value="0"/>
3	<input type="text" value="0"/>
4	<input type="text" value="0"/>
5	<input type="text" value="0"/>
6	<input type="text" value="0"/>
7	<input type="text" value="0"/>
8	<input type="text" value="0"/>
9	<input type="text" value="0"/>
10	<input type="text" value="0"/>

Group Member Switch Management > LACP > Group Member

Join Group Member Port Priority

Port List Total: 28 1 2 3

Port	Port Priority (0-65535)
1	<input type="text" value="32768"/>
2	<input type="text" value="32768"/>
3	<input type="text" value="32768"/>
4	<input type="text" value="32768"/>
5	<input type="text" value="32768"/>
6	<input type="text" value="32768"/>
7	<input type="text" value="32768"/>
8	<input type="text" value="32768"/>
9	<input type="text" value="32768"/>
10	<input type="text" value="32768"/>

4.2.8.2 Group Link Configuration

Switch Management > LACP > Group Link Configuration page is used to display and configure parameters of LCAP trunk group.

Group Link Configuration											
Switch Management > LACP > Group Link Configuration											
Dynamic Group List Total: 1											
Group	Type	Name	Admin	Status	Autonegotiation	Capability	Speed Duplex	Flow Control	MTU Size	Link Up Down Trap	
1	1000BASE-T		Enabled	Up	Enabled	10half,10full,100half,100full,1000full	1000full	None	1518	Enabled	

[Configure](#)

Note: FC - flowcontrol.

X Close

Mode by one Group by Group range

Group

Group Name

Admin Enabled

Autonegotiation Enabled

10half 100half 1000full FC

10full 100full Sym

Speed Duplex

Flow Control Enabled

MTU Size (1500-9216)

Link Up Down Trap Enabled

[Apply](#) [Revert](#)

Note: FC - flowcontrol; Sym - symmetric .

4.2.8.3 Group LACP Configuration

Switch Management > LACP > Group LACP Configuration page is used to display and configure System Priority and Timeout Mode of LCAP trunk group.

Group LACP Configuration		
Switch Management > LACP > Group LACP Configuration		
Group List Total: 1		
Group	System Priority (0-65535)	Timeout Mode
1	<input type="text" value="32768"/>	<input type="text" value="Long Timeout"/>

[Apply](#) [Revert](#)

4.2.8.4 Counter

Switch Management > LACP > Counter page is used to display counters, information of local and remote port in LCAP group.

◆ Counters:

Counter
Switch Management > LACP > Counter

Counters

Port 13 ▼

Group ID 1

Port Counters Information

LACPDU Sent	3	LACPDUs Received	4
Marker Sent	0	Marker Received	0
Marker Unknown Pkts	0	Marker Illegal Pkts	0

Refresh

4.2.8.5 Show Dynamic Group Member

Switch Management > LACP > Show Dynamic Group Member page is used to display the current members of a LACP group.

Show Dynamic Group Member
Switch Management > LACP > Show Dynamic Group Member

Group 1 ▼

Member List Total: 2

Member (Unit/Port)
1/13
1/14

4.2.9 Trunk Group Load Balance

Switch Management > Trunk Group Load Balance page is used to configure the load balance mode of trunk group.



Load Balance Mode

Source and destination IP address ▼

Destination IP address

Destination MAC address

Source and destination IP address

Source and destination MAC address

Source IP address

Source MAC address

Apply Revert

This page applies to all static and dynamic trunks on the switch.

To ensure that the switch traffic load is distributed evenly across all links in a trunk, select the source and destination addresses used in the load-balance calculation to provide the best result for trunk connections:

- **Destination IP Address:** All traffic with the same destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic.
- **Destination MAC Address:** All traffic with the same destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-router trunk links where the destination MAC address is the same for all traffic.
- **Source and Destination IP Address:** All traffic with the same source and destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is received from and destined for many different hosts.
- **Source and Destination MAC Address:** All traffic with the same source and destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from and destined for many different hosts.
- **Source IP Address:** All traffic with the same source IP address is output on the same link in a trunk. This mode works best for switch-to-router or switch-to-server trunk links where traffic through the switch is received from many different hosts.
- **Source MAC Address:** All traffic with the same source MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from many different hosts.

4.2.10 Spanning Tree Protocol

4.3.10.1 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

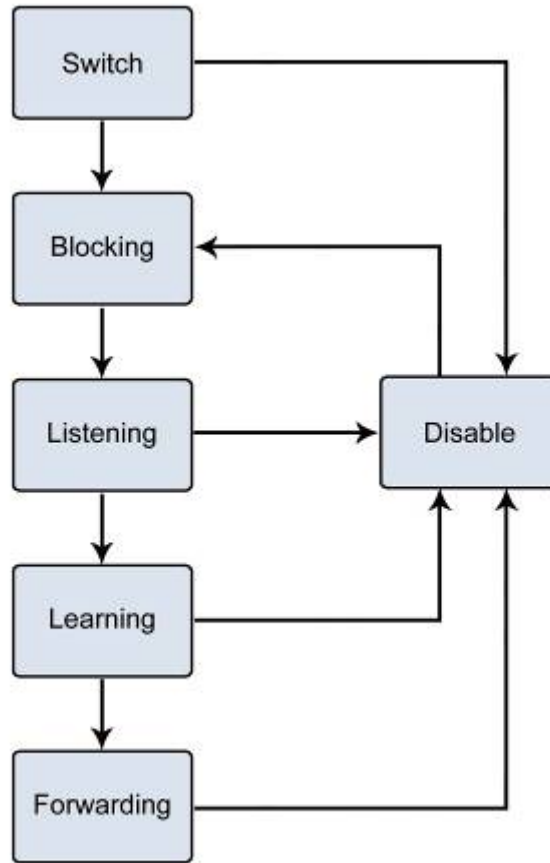



Figure 4-2-10-1: STP Port State Transitions

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.

 Note	<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 20,000-100Mbps 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.

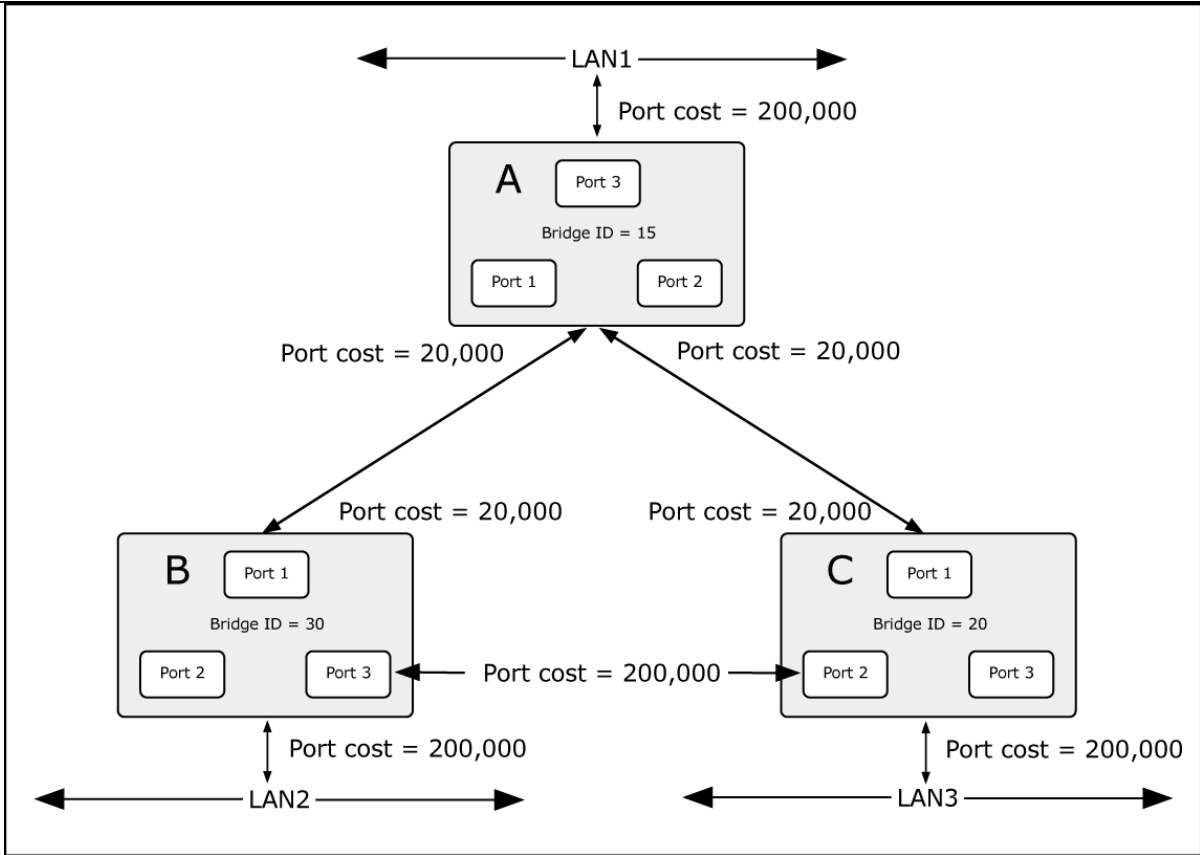


Figure 4-2-10-2: Before Applying the STA Rules

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

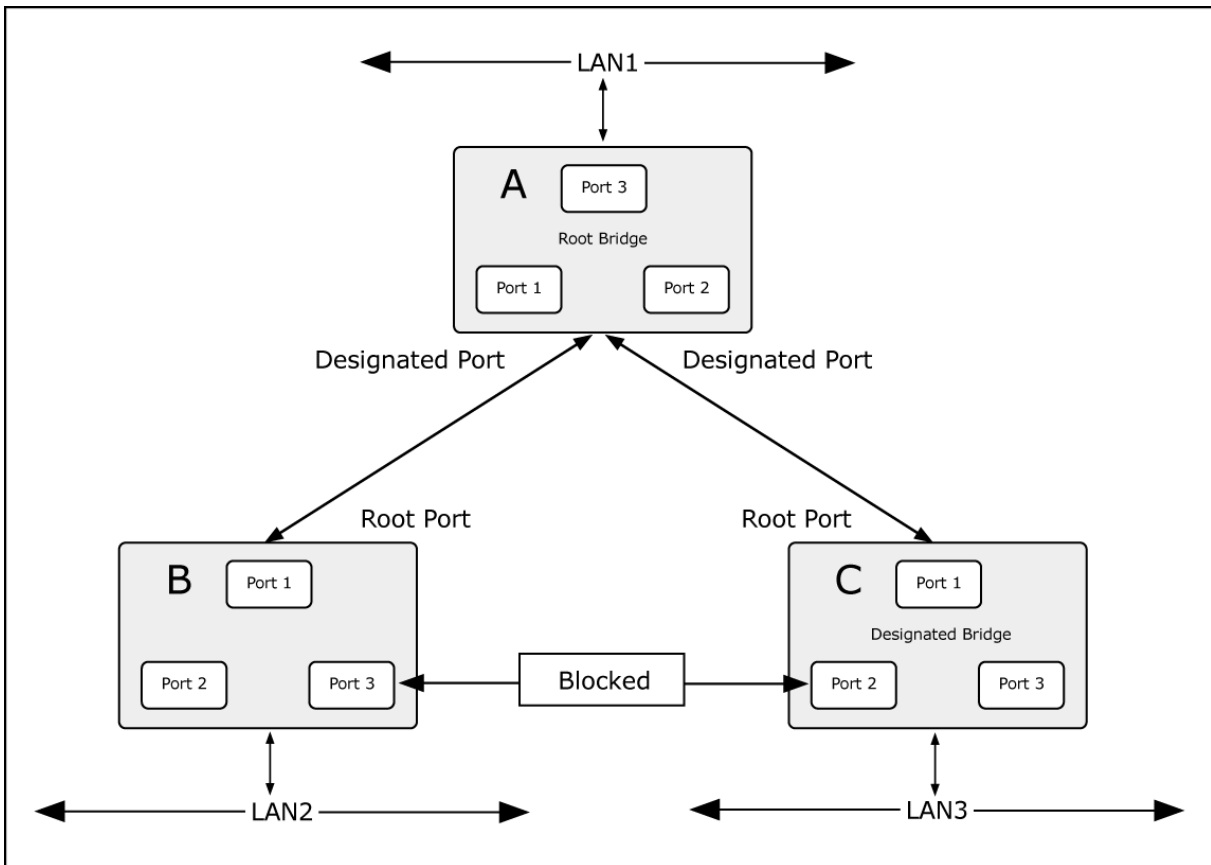
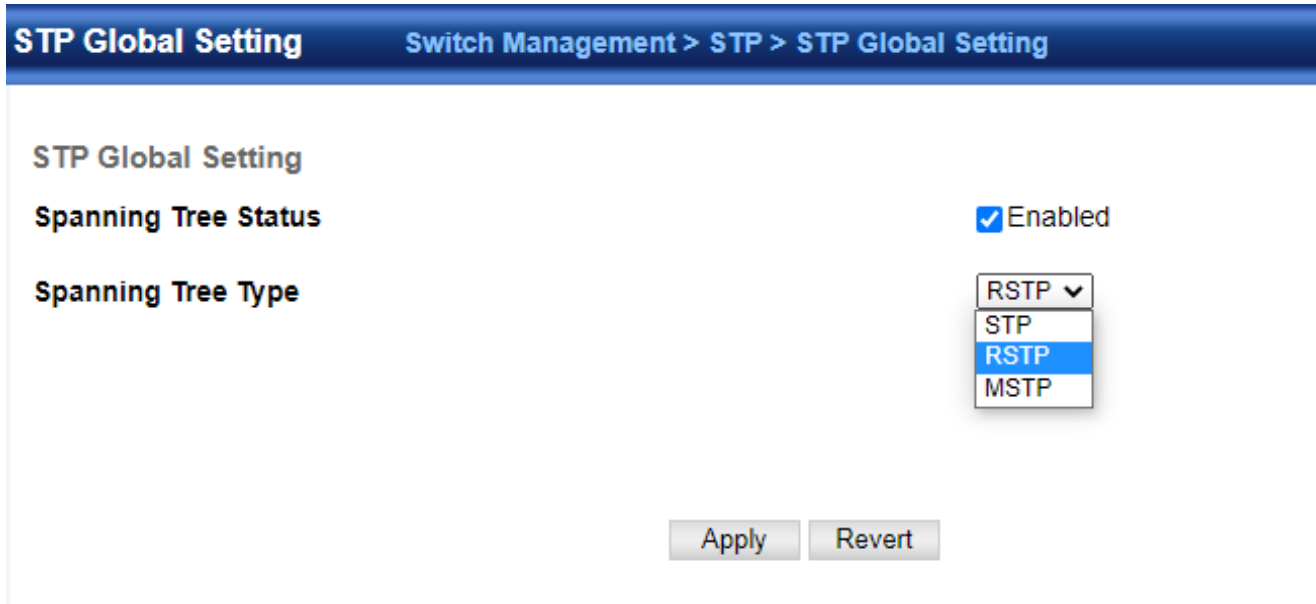


Figure 4-2-10-3: After Applying the STA Rules

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.

4.2.10.2 STP Global Setting

Switch Management > STP > STP Global Setting page is used to configure STA status and the type of spanning tree.



◆ **Spanning Tree Status** – Enables/disables STA on this switch.

(Default: Enabled)

◆ **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:

- **STP:** Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
- **RSTP:** Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
- **MSTP:** Multiple Spanning Tree (IEEE 802.1s)

4.2.10.3 STP-RSTP

Switch Management > STP > STP-RSTP > **Global Management** page is used to configure global settings for the spanning tree that apply to the entire switch.

■ Global Management

STP-RSTP
Switch Management > STP > STP-RSTP

Global Management
Interface Status

Spanning Tree Information

Spanning Tree Status	Enabled	Spanning Tree Type	RSTP
Designated Root	32768.A8F7E033A23A	Bridge ID	32768.A8F7E033A23A
Root Port	0	Max Age	20 sec
Root Path Cost	0	Hello Time	2 sec
Topology Changes	0	Forward Delay	15 sec
Last Topology Change	0 days, 0 hours, 8 minutes, 58 seconds		

Priority (0-61440, in steps of 4096)

BPDU Flooding ▼

Root parameters:

Hello Time (1-10) sec

Maximum Age (6-40) sec

Forward Delay (4-30) sec

Path Cost Method ▼

Transmission Limit (1-10)

Note: 2 * (Hello Time + 1) <= Max Age <= 2 * (Forward Delay - 1)

◆ **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

(Note that lower numeric values indicate higher priority.)

- Default: 32768
- Range: 0-61440, in steps of 4096
- Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

◆ **BPDU Flooding** – Configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port.

- **To VLAN:** Floods BPDUs to all other ports within the receiving port's native VLAN (i.e., as determined by port's PVID). This is the default.
- **To All:** Floods BPDUs to all other ports on the switch.
The setting has no effect if BPDU flooding is disabled on a port.

The following attributes are based on **RSTP**, but also apply to STP since the switch uses a backwards-compatible subset of RSTP to implement STP, and also apply to MSTP which is based on RSTP according to the standard:

◆ **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

- **Long:** Specifies 32-bit based values that range from 1-200,000,000.
(This is the default.)
- **Short:** Specifies 16-bit based values that range from 1-65535.

◆ **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

When the Switch Becomes Root

◆ **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.

- **Default:** 2
- **Minimum:** 1
- **Maximum:** The lower of 10 or $[(\text{Max. Message Age} / 2) - 1]$

◆ **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconverge. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

(References to "ports" in this section mean "interfaces," which includes both ports and groups.)

- **Default:** 20
- **Minimum:** The higher of 6 or $[2 \times (\text{Hello Time} + 1)]$
- **Maximum:** The lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$

◆ **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

- **Default:** 15
- **Minimum:** The higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$
- **Maximum:** 30

RSTP does not depend on the forward delay timer in most cases. It is able to confirm that a port can transition to the forwarding state without having to rely on any timer configuration. To achieve fast convergence, RSTP relies on the use of edge ports, and automatic detection of point-to-point link types, both of which allow a port to directly transition to the forwarding state.

Configuration Settings for MSTP

MSTP Configuration	
Max Instance Numbers	65
Configuration Digest	0xAC36177F50283CD4B83821D8AB26DE62
Region Revision (0-65535)	<input type="text" value="0"/>
Region Name	<input type="text" value="A8 F7 E0 33 A2 3A"/>
Max Hop Count (1-40)	<input type="text" value="20"/>
<input type="button" value="Apply"/> <input type="button" value="Revert"/>	

- ◆ **Max Instance Numbers** – The maximum number of MSTP instances to which this switch can be assigned.
- ◆ **Configuration Digest** – An MD5 signature key that contains the VLAN ID to MST ID mapping table. In other words, this key is a mapping of all VLANs to the CIST.
- ◆ **Region Revision⁴** – The revision for this MSTI. (Range: 0-65535; Default: 0)
- ◆ **Region Name⁴** – The name for this MSTI. (Maximum length: 32 characters; switch's MAC address)
- ◆ **Max Hop Count** – The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)
- ◆ **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority, the MST Instance ID 0 for the Common Spanning Tree when spanning tree type is set to MSTP, and MAC address (where the address is taken from the switch system).
- ◆ **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- ◆ **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
- ◆ **Root Path Cost** – The path cost from the root port on this switch to the root device.
- ◆ **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- ◆ **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

■ **Interface Status**

Switch Management > STP > STP-RSTP > **Interface Status** page is used to configure RSTP and MSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared media connection, and edge port to indicate if the attached device can support fast forwarding. (References to "ports" in this section means "interfaces," which includes both ports and groups.)

STP-RSTP Switch Management > STP > STP-RSTP Stacking Unit: 1

Global Management Interface Status

Interface Port Group

Spanning Tree Port List Total: 28 1 2 3

Port	Spanning Tree	BPDU Flooding	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Path Cost	Link Type	Edge Port	Port Role
1	Enabled	Enabled	Discarding	0	0	32768.0.ECD68A33A23A	128.1	20000	Point-to-Point	Disabled	Disabled
2	Enabled	Enabled	Discarding	0	0	32768.0.ECD68A33A23A	128.2	20000	Point-to-Point	Disabled	Disabled
3	Enabled	Enabled	Discarding	0	0	32768.0.ECD68A33A23A	128.3	20000	Point-to-Point	Disabled	Disabled
4	Enabled	Enabled	Discarding	0	0	32768.0.ECD68A33A23A	128.4	20000	Point-to-Point	Disabled	Disabled
5	Enabled	Enabled	Discarding	0	0	32768.0.ECD68A33A23A	128.5	20000	Point-to-Point	Disabled	Disabled
6	Enabled	Enabled	Discarding	0	0	32768.0.ECD68A33A23A	128.6	20000	Point-to-Point	Disabled	Disabled
7	Enabled	Enabled	Discarding	0	0	32768.0.ECD68A33A23A	128.7	20000	Point-to-Point	Disabled	Disabled
8	Enabled	Enabled	Discarding	0	0	32768.0.ECD68A33A23A	128.8	20000	Point-to-Point	Disabled	Disabled
9	Enabled	Enabled	Discarding	0	0	32768.0.ECD68A33A23A	128.9	20000	Point-to-Point	Disabled	Disabled
10	Enabled	Enabled	Discarding	0	0	32768.0.ECD68A33A23A	128.10	20000	Point-to-Point	Disabled	Disabled

[Configure](#)

- ◆ **Interface** – Displays a list of ports or groups.
- ◆ **Spanning Tree** – Enables/disables STA on this interface.
(Default: Enabled)
- ◆ **BPDU Flooding** - Enables/disables the flooding of BPDUs to other ports when global spanning tree is disabled or when spanning tree is disabled on a specific port. When flooding is enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port's native VLAN as specified by the Spanning Tree BPDU Flooding attribute .
(Default: Enabled)
- ◆ **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
 - Default: 128
 - Range: 0-240, in steps of 16
- ◆ **Admin Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost takes precedence over port priority. (Range: 0 for auto-configuration, 1-65535 for the short path cost methods, 1-200,000,000 for the long path cost method)

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 8021w standard exceeds 65,535, the default is set to 65,535.

Table 12: Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	1-5	200-20,000

Table 13: Default STA Path Costs

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

◆ **Admin Link Type** – The link type attached to this interface.

- Point-to-Point – A connection to exactly one other bridge.
- Shared – A connection to two or more bridges.
- Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)

◆ **Root Guard** – STA allows a bridge with a lower bridge identifier (or same identifier and lower MAC address) to take over as the root bridge at any time. Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It could also be used to form a border around part of the network where the root bridge is allowed.

(Default: Disabled)

◆ **Admin Edge Port** – Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end node device. (Default: Auto)

- **Enabled** – Manually configures a port as an Edge Port.
- **Disabled** – Disables the Edge Port setting.
- **Auto** – The port will be automatically configured as an edge port if the edge delay time expires without receiving any RSTP or MSTP BPDUs. Note that edge delay time (802.1D-2004 17.20.4) equals the protocol migration time if a port's link type is point-to-point (which is 3 seconds as defined in IEEE 802.3D-2004 17.20.4); otherwise it equals the spanning tree's maximum age for configuration messages.

An interface cannot function as an edge port under the following conditions:

- If spanning tree mode is set to STP , edge-port mode cannot automatically transition to operational edge-port state using the automatic setting.
 - If loopback detection is enabled and a loopback BPDU is detected, the interface cannot function as an edge port until the loopback state is released.
 - If an interface is in forwarding state and its role changes, the interface cannot continue to function as an edge port even if the edge delay time has expired.
 - If the port does not receive any BPDUs after the edge delay timer expires, its role changes to designated port and it immediately enters forwarding state.
- ◆ **BPDU Guard** – This feature protects edge ports from receiving BPDUs. It prevents loops by shutting down an edge port when a BPDU is received instead of putting it into the spanning tree discarding state. In a valid configuration, configured edge ports should not receive BPDUs. If an edge port receives a BPDU an invalid configuration exists, such as a connection to an unauthorized device. The BPDU guard feature provides a secure response to invalid configurations because an administrator must manually enable the port.
(Default: Disabled)
- ◆ **BPDU Filter** – BPDU filtering allows you to avoid transmitting BPDUs on configured edge ports that are connected to end nodes. By default, STA sends BPDUs to all ports regardless of whether administrative edge is enabled on a port. BPDU filtering is configured on a per-port basis.
(Default: Disabled)
- ◆ **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP compatible) to send on the selected interfaces. (Default: Disabled)

Switch Management > STP > STP-RSTP> **Interface Status** page is used to display the current status of ports or groups in the Spanning Tree.

- ◆ **Spanning Tree** – Shows if STA has been enabled on this interface.
- ◆ **BPDU Flooding** – Shows if BPDUs will be flooded to other ports when spanning tree is disabled globally on the switch or disabled on a specific port.
- ◆ **STA Status** – Displays current state of this port within the Spanning Tree:
 - **Discarding** - Port receives STA configuration messages, but does not forward packets.
 - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
 - **Forwarding** - Port forwards packets, and continues learning addresses.
 - The rules defining port status are:
 - A port on a network segment with no other STA compliant bridging device is always forwarding.
 - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
 - All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.
- ◆ **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- ◆ **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- ◆ **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.

- ◆ **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
- ◆ **Oper Path Cost** – The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
- ◆ **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration .
- ◆ **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- ◆ **Port Role** – Roles are assigned according to whether the port is part of the active topology, that is the best port connecting a non-root bridge to the root bridge (i.e., **root** port), connecting a LAN through the bridge to the root bridge (i.e., **designated** port), is the MSTI regional root (i.e., **master** port), or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.

4.2.10.4 MSTP

Switch Management > STP > MSTP> MST List page is used to create an MSTP instance, or to add VLAN groups to an MSTP instance.

To use multiple spanning trees:

1. [Set the spanning tree type to MSTP .](#)
2. [Enter the spanning tree priority for the selected MST instance on the Spanning Tree > MSTP \(MST List - New\) page.](#)
3. [Add the VLANs that will share this MSTI on the Spanning Tree > MSTP > \(MST List - New\) page.](#)

To ensure that the MSTI maintains connectivity across the network, you must configure a related set of bridges with the same MSTI settings.

- ◆ **MST ID** – Instance identifier to configure. (Range: 0-4094)
- ◆ **VLAN ID** – VLAN to assign to this MST instance. (Range: 1-4093)
- ◆ **Priority** – The priority of a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)

■ Global Management

MSTP Switch Management > STP > MSTP

Global Management MST List MST Information MST Member MST Interface

Priority (0-61440, in steps of 4096)

BPDU Flooding

Root parameters:

Hello Time (1-10) sec

Maximum Age (6-40) sec

Forward Delay (4-30) sec

Path Cost Method

Transmission Limit (1-10)

Note: $2 * (\text{Hello Time} + 1) \leq \text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$

MSTP Configuration

Max Instance Numbers 65

Configuration Digest 0xAC36177F50283CD4B83821D8AB26DE62

Region Revision (0-65535)

Region Name

Max Hop Count (1-40)

MSTP Switch Management > STP > MSTP Stacking Unit :

Global Management MST List MST Information MST Member MST Interface

MST List Total: 1

	MST ID
<input type="checkbox"/>	0

MSTP Switch Management > STP > MSTP

Global Management MST List MST Information MST Member MST Interface

MST ID (0-4094)

VLAN ID (1-4094) -

Priority (0-61440, in steps of 4096)

MSTP Switch Management > STP > MSTP

Global Management MST List MST Information MST Member MST Interface

MST ID	<input type="text" value="0"/>		
Priority	32768	Designated Root	32768.0.A8F7E033A23A
Bridge ID	32768.0.ECD68A33A23A	Root Port	0
Max Age	20 sec	Root Path Cost	0
Hello Time	2 sec	Configuration Changes	0
Forward Delay	15 sec	Last Topology Change	2 hrs 19 mins 55 seconds

MSTP Switch Management > STP > MSTP Stacking Unit : 1

Global Management MST List MST Information **MST Member** MST Interface

MST ID

Member List Total: 409 1 2 3 4 5 6 7 8 9 10

	VLAN
<input type="checkbox"/>	1
<input type="checkbox"/>	2
<input type="checkbox"/>	3
<input type="checkbox"/>	4
<input type="checkbox"/>	5
<input type="checkbox"/>	6
<input type="checkbox"/>	7
<input type="checkbox"/>	8
<input type="checkbox"/>	9
<input type="checkbox"/>	10
<input type="checkbox"/>	11

■ **MST Interface**

Switch Management > STP > MSTP > **MST Interface** page is used to configure the STA interface settings for an MST instance.

MSTP Switch Management > STP > MSTP Stacking Unit : 1

Global Management MST List MST Information MST Member **MST Interface**

MST ID 0

Interface Port Group

Spanning Tree Port List Total: 28 1 2 3

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Path Cost	Link Type	Edge Port	Port Role
1	Discarding	0	0	32768.0.A8F7E033A23A	128.1	20000	Point-to-Point	Disabled	Disabled
2	Discarding	0	0	32768.0.A8F7E033A23A	128.2	20000	Point-to-Point	Disabled	Disabled
3	Discarding	0	0	32768.0.A8F7E033A23A	128.3	20000	Point-to-Point	Disabled	Disabled
4	Discarding	0	0	32768.0.A8F7E033A23A	128.4	20000	Point-to-Point	Disabled	Disabled
5	Discarding	0	0	32768.0.A8F7E033A23A	128.5	20000	Point-to-Point	Disabled	Disabled
6	Discarding	0	0	32768.0.A8F7E033A23A	128.6	20000	Point-to-Point	Disabled	Disabled
7	Discarding	0	0	32768.0.A8F7E033A23A	128.7	20000	Point-to-Point	Disabled	Disabled
8	Discarding	0	0	32768.0.A8F7E033A23A	128.8	20000	Point-to-Point	Disabled	Disabled
9	Discarding	0	0	32768.0.A8F7E033A23A	128.9	20000	Point-to-Point	Disabled	Disabled
10	Discarding	0	0	32768.0.A8F7E033A23A	128.10	20000	Point-to-Point	Disabled	Disabled

◆ **MST ID** – Instance identifier to configure. (Default: 0)

◆ **Interface** – Displays a list of ports or groups.

◆ **STA Status** – Displays the current state of this interface within the Spanning Tree.

- **Discarding** – Port receives STA configuration messages, but does not forward packets.
- **Learning** – Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.

- **Forwarding** – Port forwards packets, and continues learning addresses.

- ◆ **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. (Default: 128; Range: 0-240, in steps of 16)

- ◆ **Admin MST Path Cost** – This parameter is used by the MSTP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535.

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 8021w standard exceeds 65,535, the default is set to 65,535.

The recommended range is listed in [Table 12](#) .

The default path costs are listed in [Table 13](#) .

MST ID

Interface Port Group

Spanning Tree Port List Total: 28 1 2 3

Port	STA Status	Priority (0-240, in steps of 16)	Admin MST Path Cost (0-200000000, 0: Auto)
1	Discarding	<input type="text" value="128"/>	<input type="text" value="0"/>
2	Discarding	<input type="text" value="128"/>	<input type="text" value="0"/>
3	Discarding	<input type="text" value="128"/>	<input type="text" value="0"/>
4	Discarding	<input type="text" value="128"/>	<input type="text" value="0"/>
5	Discarding	<input type="text" value="128"/>	<input type="text" value="0"/>
6	Discarding	<input type="text" value="128"/>	<input type="text" value="0"/>
7	Discarding	<input type="text" value="128"/>	<input type="text" value="0"/>
8	Discarding	<input type="text" value="128"/>	<input type="text" value="0"/>

To display MSTP parameters for a port or group:

Global Management MST List MST Information MST Member MST Interface

MST ID:

Interface: Port Group

Spanning Tree Group List Total: 0

Group	STA Status	Priority (0-240, in steps of 16)	Admin MST Path Cost (0-200000000, 0: Auto)
-------	------------	----------------------------------	--

4.2.10.5 Loopback Detection

Switch Management > STP > Loopback Detection page is used to configure loopback detection on an interface. When loopback detection is enabled and a port or group receives its own BPDU, the detection agent drops the loopback BPDU, sends an SNMP trap, and places the interface in discarding mode. This loopback state can be released manually or automatically. If the interface is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:

Loopback Detection Switch Management > STP > Loopback Detection Stacking Unit: 1

Interface: Port Group

Loopback Detection Port List Total: 26 1 2 3

Port	Status	Trap	Release Mode	Release	Action	Shutdown Interval (60-86400 sec)
1	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Shutdown	60
2	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Shutdown	60
3	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Shutdown	60
4	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Shutdown	60
5	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Shutdown	60
6	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Shutdown	60
7	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Shutdown	60
8	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Shutdown	60
9	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Shutdown	60
10	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Auto	Release	Shutdown	60

- ◆ The interface receives any other BPDU except for its own, or;
 - ◆ The interfaces' link status changes to link down and then link up again,
- or;
- ◆ The interface ceases to receive its own BPDUs in a forward delay interval.
- ◆ **Interface** – Displays a list of ports or groups.
 - ◆ **Status** – Enables loopback detection on this interface.
(Default: Enabled)
 - ◆ **Trap** – Enables SNMP trap notification for loopback events on this interface. (Default: Disabled)

- ◆ **Release Mode** – Configures the interface for automatic or manual loopback release. (Default: Auto)
- ◆ **Release** – Allows an interface to be manually released from discard mode. This is only available if the interface is configured for manual release mode.
- ◆ **Action** – Sets the response for loopback detection to block user traffic or shut down the interface. (Default: Block)
- ◆ **Shutdown Interval** – The duration to shut down the interface. (Range: 60-86400 seconds; Default: 60 seconds)

If an interface is shut down due to a detected loopback, and the release mode is set to “Auto,” the selected interface will be automatically enabled when the shutdown interval has expired. If an interface is shut down due to a detected loopback, and the release mode is set to “Manual,” the interface can be re-enabled using the Release button.

4.2.11 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.

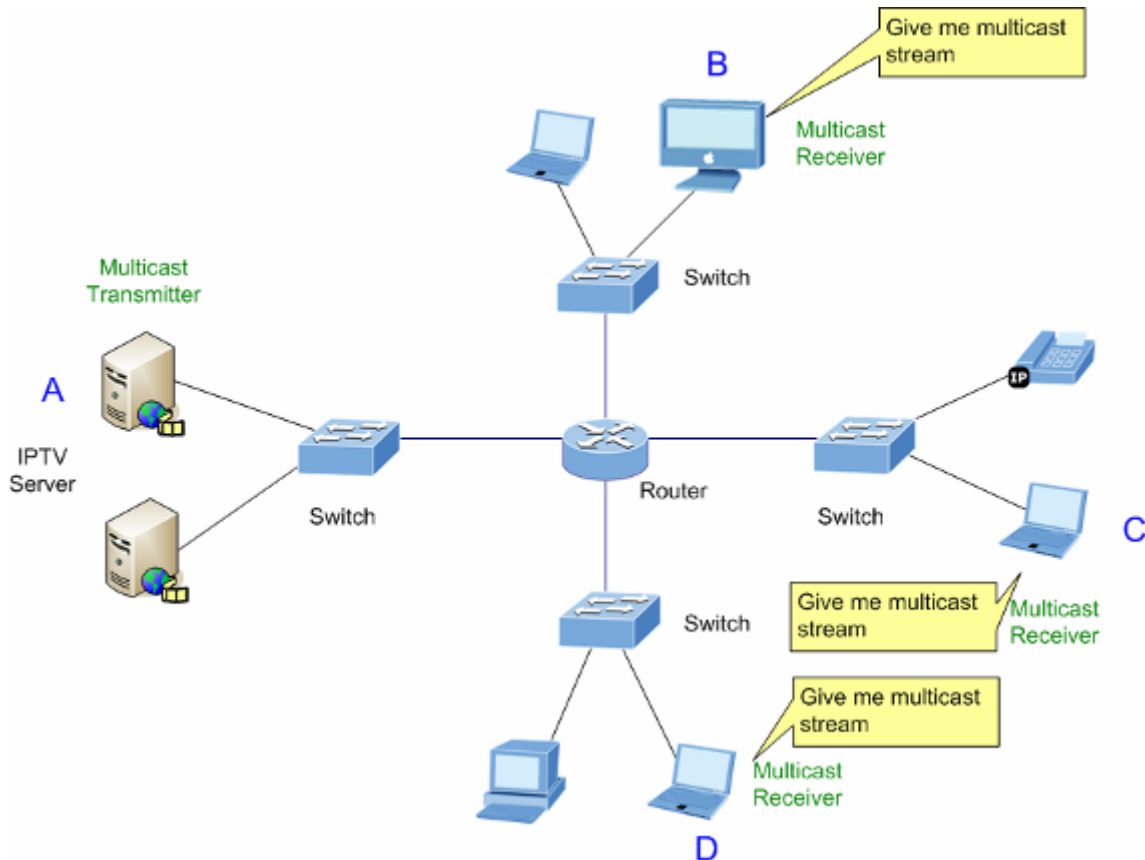


Figure 4-3-5-1: Multicast Service

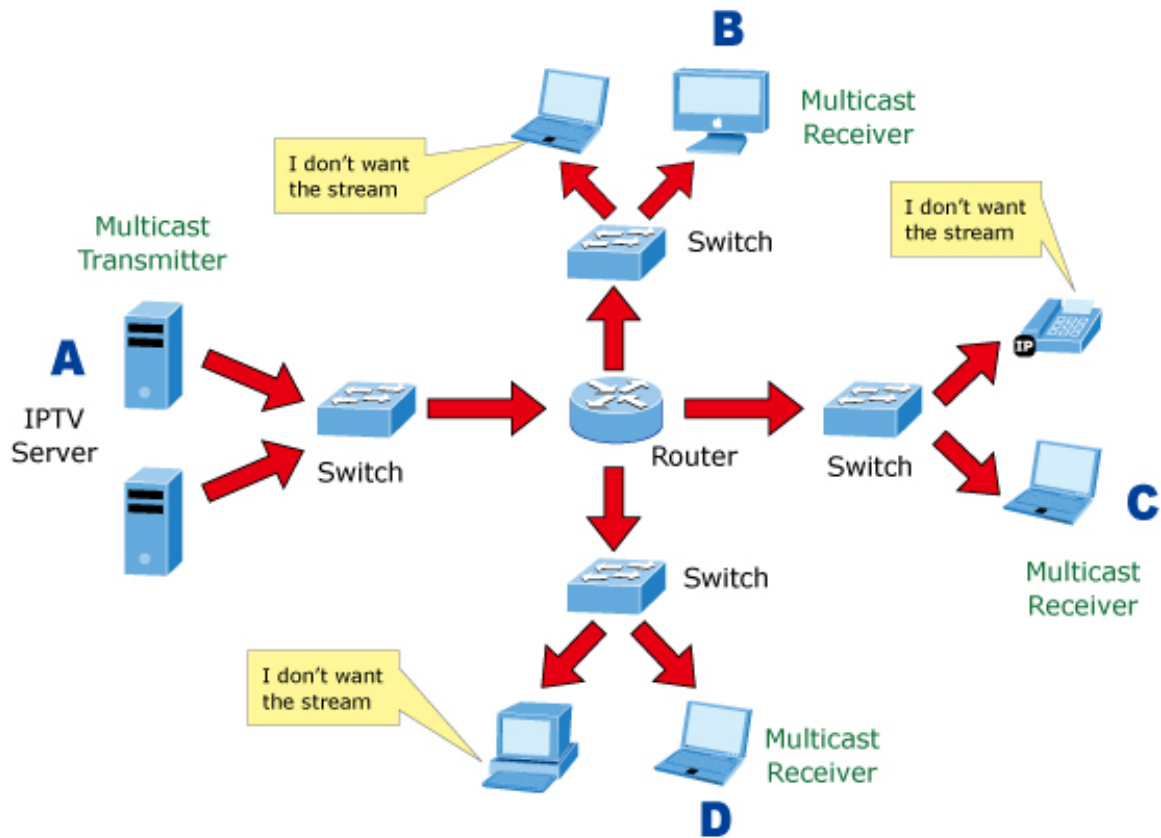


Figure 4-3-5-2: Multicast Flooding

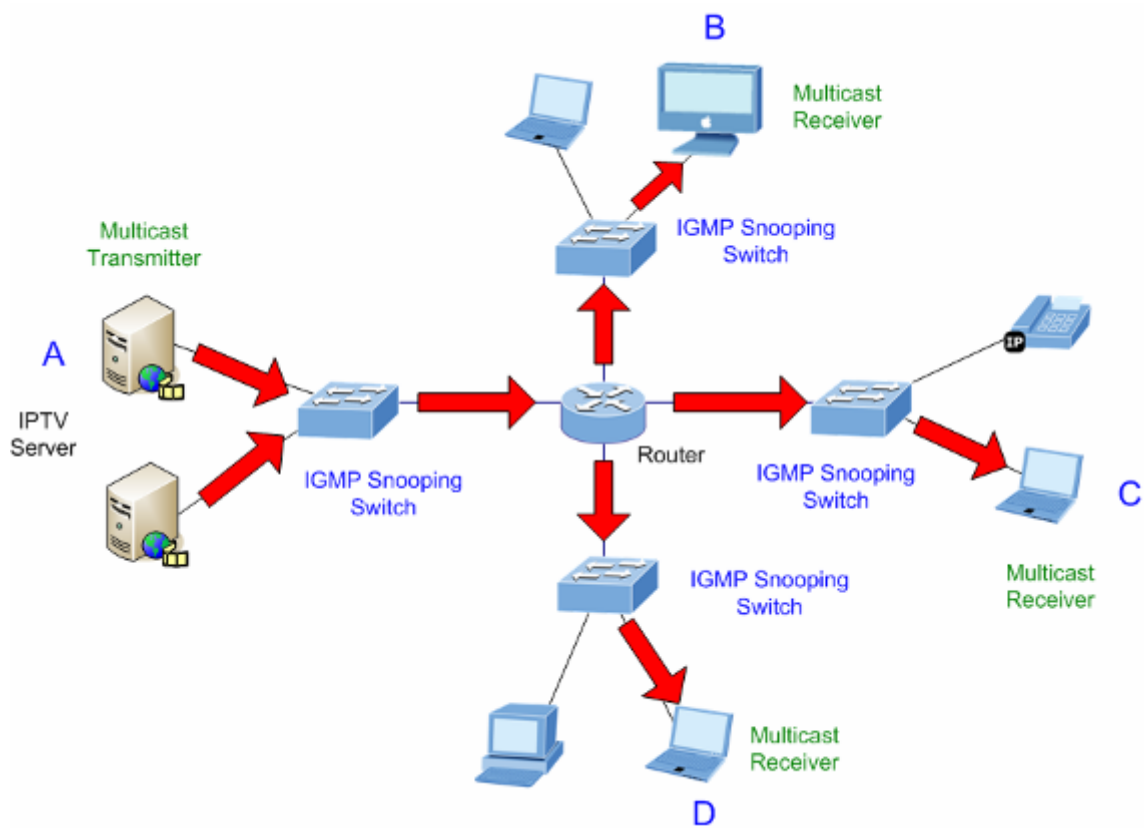


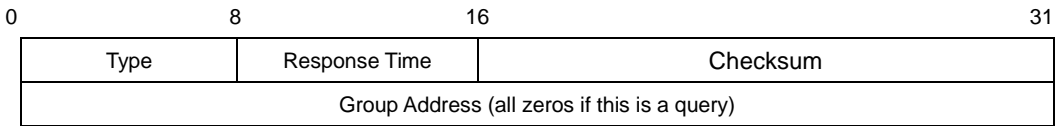
Figure 4-3-5-3: IGMP Snooping Multicast Stream Control

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:

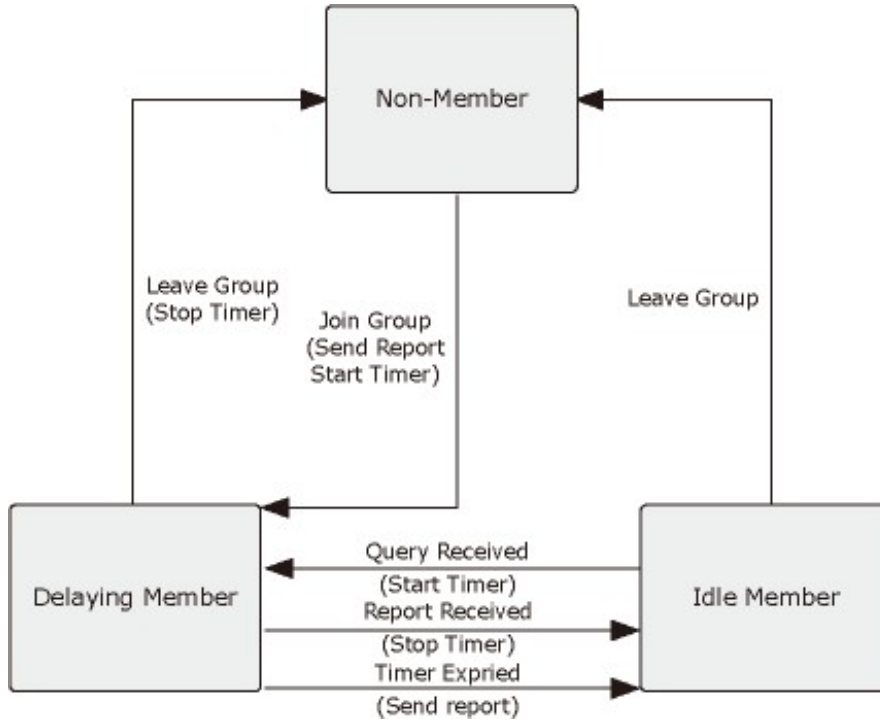
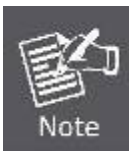


Figure 4-3-5-4: IGMP State Transitions

■ **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 “**queried**” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.



Note

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

4.2.11.1 Global Setting

Switch Management> IGMP Snooping>Global Setting page is used to configure the switch to forward multicast traffic.

Global Setting		Switch Management > IGMP Snooping > Global Setting	
IGMP Snooping Status	<input type="checkbox"/>	Enabled	
Proxy Reporting Status	<input type="checkbox"/>	Enabled	
TCN Flood	<input type="checkbox"/>	Enabled	
TCN Query Solicit	<input type="checkbox"/>	Enabled	
Router Alert Option	<input type="checkbox"/>	Enabled	
Unregistered Data Flooding	<input type="checkbox"/>	Enabled	
Forwarding Priority (0-7)	<input type="checkbox"/>	<input type="text" value=""/>	
Version Exclusive	<input type="checkbox"/>	Enabled	
IGMP Unsolicited Report Interval (1-65535)	<input type="text" value="400"/>	seconds	
Router Port Expire Time (1-65535)	<input type="text" value="300"/>	seconds	
IGMP Snooping Version (1-3)	<input type="text" value="2"/>		
Querier Status	<input checked="" type="checkbox"/>	Enabled	

- ◆ **IGMP Snooping Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Disabled)
 When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence.
 When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.
- ◆ **Proxy Reporting Status** – Enables IGMP Snooping with Proxy Reporting. (Default: Disabled)
 When proxy reporting is enabled with this command, the switch performs “IGMP Snooping with Proxy Reporting” (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression. Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device. When proxy reporting is disabled, all IGMP reports received by the switch are forwarded natively to the upstream multicast routers.
- ◆ **TCN Flood** – Enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. (Default: Disabled)
 - **TCN Query Solicit** – Sends out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. (Default: Disabled)
 - **Router Alert Option** – Discards any IGMPv2/v3 packets that do not include the Router Alert option. (Default: Disabled)
 - **Unregistered Data Flooding** – Floods unregistered multicast traffic into the attached VLAN. (Default: Disabled)

- ◆ **Forwarding Priority** – Assigns a CoS priority to all multicast traffic.
(Range: 0-6, where 6 is the highest priority)
- ◆ **Version Exclusive** – Discards any received IGMP messages which use a version different to that currently configured by the IGMP Version attribute.
(Default: Disabled)
- ◆ **IGMP Unsolicited Report Interval** – Specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled.
(Range: 1-65535 seconds, Default: 400 seconds)
- ◆ **Router Port Expire Time** – The time the switch waits after the previous queried stops before it considers it to have expired.
(Range: 1-65535, Recommended Range: 300-500 seconds, Default: 300)
- ◆ **IGMP Snooping Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports.
(Range: 1-3; Default: 2)
- ◆ **Querier Status** – When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. This feature is not supported for IGMPv3 snooping.
(Default: Disabled)

4.2.11.2 Current Multicast Router

Switch Management> IGMP Snooping> Current Multicast Router page is used to statically show an interface to a multicast router/switch.

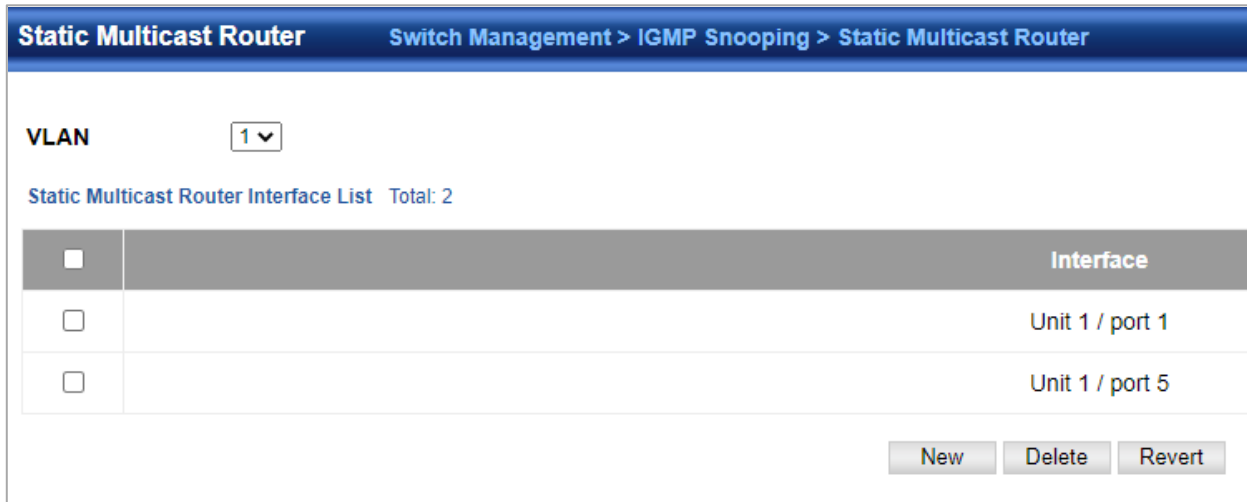
Current Multicast Router		Switch Management > IGMP Snooping > Current Multicast Router	
VLAN	1 ▼		
Multicast Router Interface Information Total: 2			
Interface	Type	Expire	
Unit 1 / port 1	Static		
Unit 1 / port 5	Static		

- ◆ **VLAN** – Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router.
(Range: 1-4093)
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port or Group** – Specifies the interface attached to a multicast router.

4.2.11.3 Static Multicast Router

Switch Management> IGMP Snooping> Static Multicast Router page is used to statically attach an interface to a multicast router/switch.

To show the static interfaces attached to a multicast router:



Static Multicast Router Switch Management > IGMP Snooping > Static Multicast Router

VLAN 1 ▾

Static Multicast Router Interface List Total: 2

<input type="checkbox"/>	Interface
<input type="checkbox"/>	Unit 1 / port 1
<input type="checkbox"/>	Unit 1 / port 5

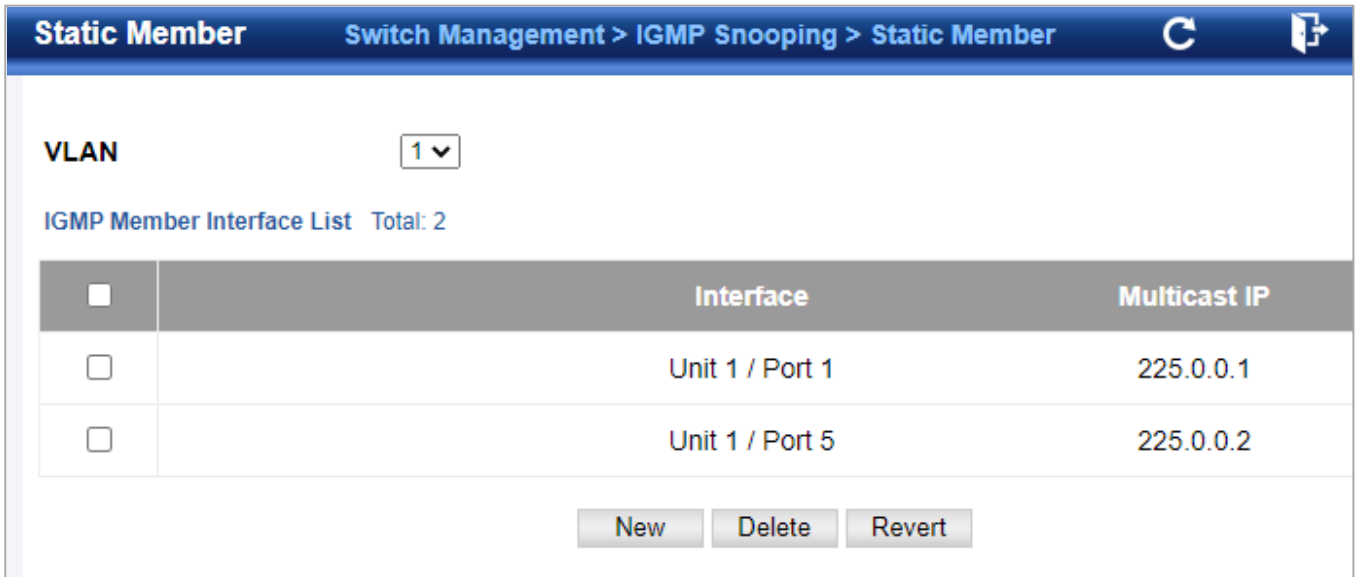
New Delete Revert

- ◆ **VLAN** – Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router.
(Range: 1-4093)
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port or Group** – Specifies the interface attached to a multicast router.

4.2.11.4 Static Member

Switch Management > IGMP Snooping>Static Member page is used to statically assign a multicast service to an interface. Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages.

To show the static interfaces assigned to a multicast service:

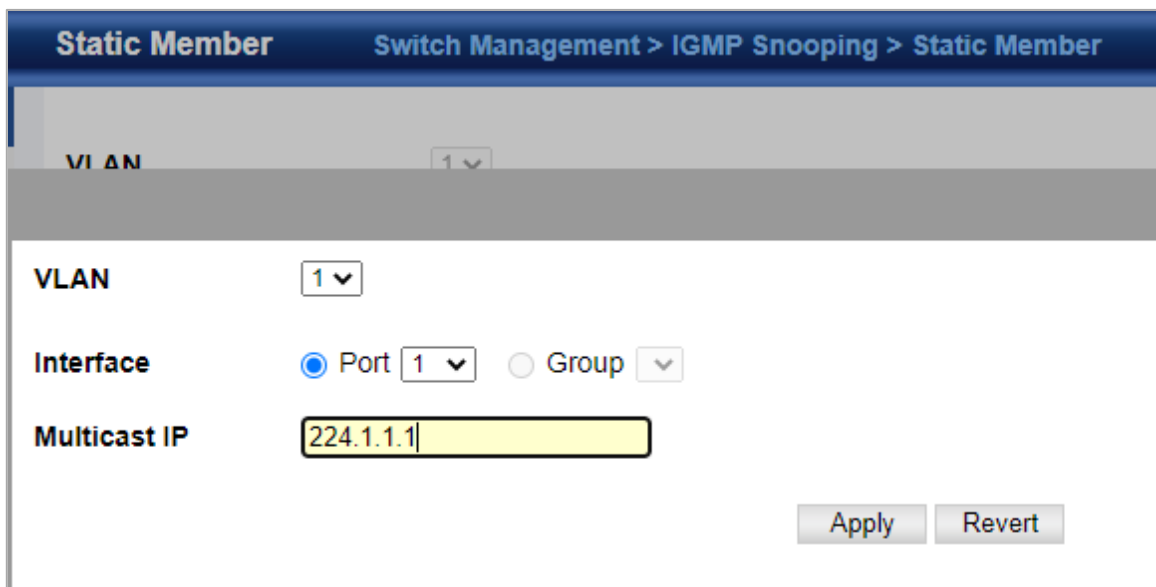


Static Member Switch Management > IGMP Snooping > Static Member

VLAN

IGMP Member Interface List Total: 2

<input type="checkbox"/>	Interface	Multicast IP
<input type="checkbox"/>	Unit 1 / Port 1	225.0.0.1
<input type="checkbox"/>	Unit 1 / Port 5	225.0.0.2



Static Member Switch Management > IGMP Snooping > Static Member

VLAN

VLAN

Interface Port Group

Multicast IP

- ◆ **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4093)
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port** or **Group** – Specifies the interface assigned to a multicast group.
- ◆ **Multicast IP** – The IP address for a specific multicast service.

4.2.11.5 VLAN Information

Switch Management > IGMP Snooping>VLAN Information page is used to configure IGMP snooping attributes for a VLAN.

VLAN Information												
Switch Management > IGMP Snooping > VLAN Information												
IGMP Snooping VLAN List Total: 1												
VLAN	IGMP Snooping Status	Immediate Leave Status	Query Interval	Query Response Interval	Last Member Query Interval	Last Member Query Count	Proxy (Query) Address	Proxy Reporting	Multicast Router Discovery	General Query Suppression	Version Exclusive	Interface Version
1	Disabled	Disabled	125	100	10	2	0.0.0.0	Disabled	Disabled	Disabled	Disabled	2

[Configure](#)

VLAN	1 ▼
IGMP Snooping Status	<input type="checkbox"/> Enabled
Version Exclusive	Using Global Status ▼
Immediate Leave Status	<input type="checkbox"/> Enabled By-Group ▼
Multicast Router Discovery	<input type="checkbox"/> Enabled
General Query Suppression	<input type="checkbox"/> Enabled
Proxy Reporting	Using Global Status ▼
Interface Version	Using Global Version ▼
Query Interval (2-31744)	<input type="text" value="125"/> seconds
Query Response Interval (10-31740)	<input type="text" value="100"/> (1/10 seconds, multiple of 10)
Last Member Query Interval (1-31744)	<input type="text" value="10"/> (1/10 seconds, multiple of 10)
Last Member Query Count (1-255)	<input type="text" value="2"/>
Proxy (Query) Address	<input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/> <input type="button" value="Revert"/>	

◆ **VLAN** – ID of configured VLANs.

(Range: 1-4093)

◆ **IGMP Snooping Status** – When enabled, the switch will monitor network traffic on the indicated VLAN interface to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping.

(Default: Disabled)

When IGMP snooping is enabled globally , the per VLAN interface settings for IGMP snooping take precedence. When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

◆ **Version Exclusive** – Discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled)

If version exclusive is disabled on a VLAN, then this setting is based on the global setting configured on the **Multicast > IGMP Snooping > General** page. If it is enabled on a VLAN, then this setting takes precedence over the global setting.

◆ **Immediate Leave Status** – Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate leave is enabled for the parent VLAN.

(Default: Disabled)

If immediate leave is not used, a multicast router (or querier) will send a group-specific query message when an IGMPv2 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified time out period.

Note that this time out is set to Last Member Query Interval * Robustness Variable (fixed at 2) as defined in RFC 2236.

If immediate leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping. This attribute is only effective if IGMP snooping is enabled, and IGMPv2 snooping is used.

◆ **Multicast Router Discovery** – MRD is used to discover which interfaces are attached to multicast routers.

(Default: Enabled)

◆ **General Query Suppression** – Suppresses general queries except for ports attached to downstream multicast hosts.

(Default: Disabled)

By default, general query messages are flooded to all ports, except for the multicast router through which they are received. If general query suppression is enabled, then these messages are forwarded only to downstream ports which have joined a multicast service.

◆ **Proxy Reporting** – Enables IGMP Snooping with Proxy Reporting.

(Default: Based on global setting)

When proxy reporting is enabled with this command, the switch performs "IGMP Snooping with Proxy Reporting" (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression. Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device.

◆ **Interface Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports.

(Range: 1-3; Default: 2)

This attribute configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.

◆ **Query Interval** – The interval between sending IGMP proxy general queries.

(Range: 2-31744 seconds; Default: 125 seconds)

An IGMP general query message is sent by the switch at the interval specified by this attribute. When this message is received by downstream hosts, all receivers build an IGMP report for the multicast groups they have joined. This command applies when the switch is serving as the querier, or as a proxy host when IGMP snooping proxy reporting is enabled.

◆ **Query Response Interval** – The maximum time the system waits for a response to proxy general queries.

(Range: 10-31744 tenths of a second; Default: 10 seconds)

This command applies when the switch is serving as the querier, or as a proxy host when IGMP snooping proxy reporting is enabled.

◆ **Last Member Query Interval** – The interval to wait for a response to a group-specific or group-and-source-specific query message.

(Range: 1-31740 tenths of a second in multiples of 10; Default: 1 second)

When a multicast host leaves a group, it sends an IGMP leave message. When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP group specific or group-and-source-specific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report

is sent to the upstream multicast router. A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more burst traffic. This attribute will take effect only if IGMP snooping proxy reporting is enabled or IGMP querier is enabled .

◆**Last Member Query Count** – The number of IGMP proxy group specific or group-and-source-specific query messages that are sent out before the system assumes there are no more local members.

(Range: 1-255; Default: 2)

This attribute will take effect only if IGMP snooping proxy reporting or IGMP querier is enabled.

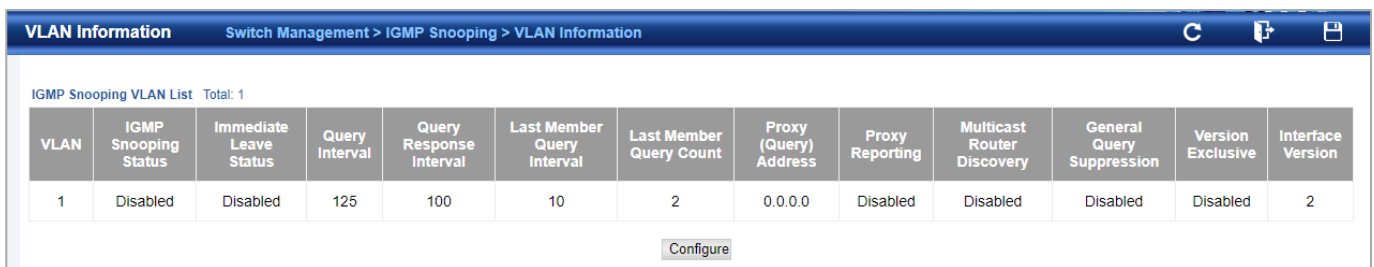
◆**Proxy Query Address** – A static source address for locally generated query and report messages used by IGMP Proxy Reporting.

(Range: Any valid IP unicast address; Default: 0.0.0.0)

IGMP Snooping uses a null IP address of 0.0.0.0 for the source of IGMP query messages which are proxied to downstream hosts to indicate that it is not the elected querier, but is only proxying these messages as defined in RFC 4541. The switch also uses a null address in IGMP reports sent to upstream ports. Many hosts do not implement RFC 4541, and therefore do not understand query messages with the source address of 0.0.0.0. These hosts will therefore not reply to the queries, causing the multicast router to stop sending traffic to them. To resolve this problem, the source address in proxies IGMP query messages can be replaced with any valid unicast address (other than the router's own address). Rules Used for Proxy Reporting When IGMP Proxy Reporting is disabled, the switch will use a null IP address for the source of IGMP query and report messages unless a proxy query address has been set. When IGMP Proxy Reporting is enabled, the source address is based on the following criteria:

- If a proxy query address is configured, the switch will use that address as the source IP address in general and group-specific query messages sent to downstream hosts, and in report and leave messages sent upstream from the multicast router port.
- If a proxy query address is not configured, the switch will use the VLAN's IP address as the IP source address in general and group specific query messages sent downstream, and use the source address of the last IGMP message received from a downstream host in report and leave messages sent upstream from the multicast router port.

To show the interface settings for IGMP snooping:



The screenshot shows a web-based management interface for a switch. The breadcrumb navigation is "Switch Management > IGMP Snooping > VLAN Information". Below the navigation, there is a title "IGMP Snooping VLAN List Total: 1". A table displays the configuration for VLAN 1. The table has 13 columns: VLAN, IGMP Snooping Status, Immediate Leave Status, Query Interval, Query Response Interval, Last Member Query Interval, Last Member Query Count, Proxy (Query) Address, Proxy Reporting, Multicast Router Discovery, General Query Suppression, Version Exclusive, and Interface Version. The values for each column are: 1, Disabled, Disabled, 125, 100, 10, 2, 0.0.0.0, Disabled, Disabled, Disabled, Disabled, and 2. Below the table is a "Configure" button.

VLAN	IGMP Snooping Status	Immediate Leave Status	Query Interval	Query Response Interval	Last Member Query Interval	Last Member Query Count	Proxy (Query) Address	Proxy Reporting	Multicast Router Discovery	General Query Suppression	Version Exclusive	Interface Version
1	Disabled	Disabled	125	100	10	2	0.0.0.0	Disabled	Disabled	Disabled	Disabled	2

4.2.11.6 Configure Interface

Switch Management > IGMP Snooping>Configure Interface page is used to configure an interface to drop IGMP query packets.

Configure Interface
Switch Management > IGMP Snooping > Configure Interface

Interface Port Group

Port List Total: 26

Port	IGMP Query Drop	Multicast Data Drop	IGMP Authentication
1	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
2	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
3	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
4	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
5	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
6	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
7	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
8	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
9	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
10	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled

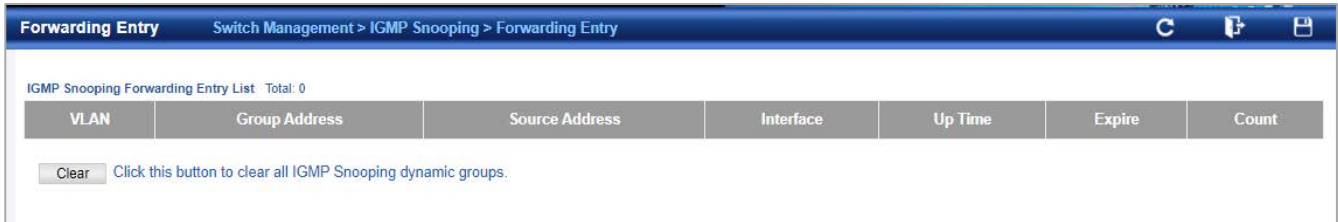
◆**IGMP Query Drop** – Configures an interface to drop any IGMP query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

4.2.11.7 Forwarding Entry

Switch Management > IGMP Snooping>Forwarding Entry page is used to display the forwarding entries learned through IGMP Snooping.

COMMAND USAGE

To display information about multicast groups, IGMP Snooping must first be enabled on the switch .



- ◆ **VLAN** – An interface on the switch that is forwarding traffic to downstream ports for the specified multicast group address.
- ◆ **Group Address** – IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.
- ◆ **Interface** – A downstream port or trunk that is receiving traffic for the specified multicast group. This field may include both dynamically and statically configured multicast router ports.
- ◆ **Up Time** – Time that this multicast group has been known.
- ◆ **Expire** – Time until this entry expires.
- ◆ **Count** – The number of times this address has been learned by IGMP snooping.

4.2.11.8 Query Statistics

Switch Management > IGMP Snooping> Query Statistics page is used to display IGMP snooping protocol-related statistics for the specified interface.

Query Statistics
Switch Management > IGMP Snooping > Query Statistics

VLAN 1 ▼

Query Statistics

Other Querier	None	Other Querier Expire	00(m):00(s)
Other Querier Uptime	00(h):00(m):00(s)	Self Querier	192.168.0.100
Self Querier Expire	00(m):00(s)	Self Querier Uptime	00(h):00(m):00(s)
General Query Received	0	General Query Sent	0
Specific Query Received	0	Specific Query Sent	0
Warn Rate Limit	0 sec.	V1 Warning Count	0
V2 Warning Count	0	V3 Warning Count	0

Clear All [Click this button to clear all IGMP Snooping statistics.](#)

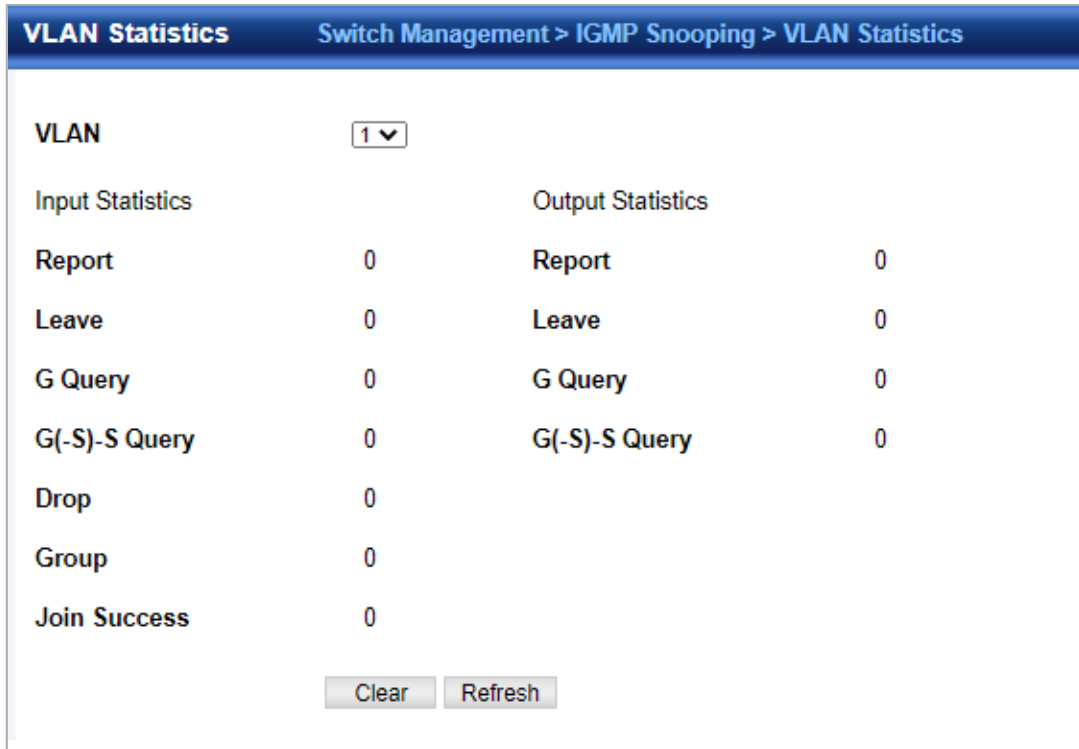
Refresh

- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
 - ◆ **Port** – Port identifier. (Range: 1-28)
 - ◆ **Group** – Group identifier. (Range: 1-12) Query Statistics
 - ◆ **Querier IP Address** – The IP address of the querier on this interface.
 - ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
 - ◆ **General Query Received** – The number of general queries received on this interface.
 - ◆ **General Query Sent** – The number of general queries sent from this interface.
 - ◆ **Specific Query Received** – The number of specific queries received on this interface.
 - ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
 - ◆ **Number of Reports Sent** – The number of reports sent from this interface.
 - ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.
- VLAN, Port, and Group Statistics Input Statistics
- ◆ **Report** – The number of IGMP membership reports received on this interface.
 - ◆ **Leave** – The number of leave messages received on this interface.
 - ◆ **G Query** – The number of general query messages received on this interface.
 - ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
 - ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or IGMP group report received.
 - ◆ **Join Success** – The number of times a multicast group was successfully joined.
- Output Statistics
- ◆ **Group** – The number of IGMP groups active on this interface.
 - ◆ **Report** – The number of IGMP membership reports sent from this interface.
 - ◆ **Leave** – The number of leave messages sent from this interface.
 - ◆ **G Query** – The number of general query messages sent from this interface.

◆**G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

4.2.11.9 VLAN Statistics

Switch Management > IGMP Snooping>Vlan Statistics page is used to display IGMP snooping protocol-related statistics for the specified interface.



VLAN Statistics		Switch Management > IGMP Snooping > VLAN Statistics	
VLAN	1		
Input Statistics		Output Statistics	
Report	0	Report	0
Leave	0	Leave	0
G Query	0	G Query	0
G(-S)-S Query	0	G(-S)-S Query	0
Drop	0		
Group	0		
Join Success	0		
<input type="button" value="Clear"/> <input type="button" value="Refresh"/>			

◆**VLAN** – VLAN identifier. (Range: 1-4093) Query Statistics

◆**Querier IP Address** – The IP address of the querier on this interface.

◆**Querier Expire Time** – The time after which this querier is assumed to have expired.

◆**General Query Received** – The number of general queries received on this interface.

◆**General Query Sent** – The number of general queries sent from this interface.

◆**Specific Query Received** – The number of specific queries received on this interface.

◆**Specific Query Sent** – The number of specific queries sent from this interface.

◆**Number of Reports Sent** – The number of reports sent from this interface.

◆**Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Group Statistics Input Statistics

◆**Report** – The number of IGMP membership reports received on this interface.

◆**Leave** – The number of leave messages received on this interface.

◆**G Query** – The number of general query messages received on this interface.

◆**G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.

◆**Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or IGMP group report received.

◆**Join Success** – The number of times a multicast group was successfully joined.

◆**Group** – The number of IGMP groups active on this interface. Output Statistics

◆**Report** – The number of IGMP membership reports sent from this interface.

◆**Leave** – The number of leave messages sent from this interface.

◆**G Query** – The number of general query messages sent from this interface.

◆**G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

4.2.11.10 Port Statistics

Switch Management > IGMP Snooping > Port Statistics page is used to display IGMP snooping protocol-related statistics for the specified interface.

Port Statistics
Switch Management > IGMP Snooping > Port Statistics

Port 1 ▾

Input Statistics	Output Statistics		
Report	0	Report	0
Leave	0	Leave	0
G Query	0	G Query	0
G(-S)-S Query	0	G(-S)-S Query	0
Drop	0		
Group	0		
Join Success	0		

Clear
Refresh

- ◆ **Port** – Port identifier. (Range: 1-28) Query Statistics
- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or IGMP group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of IGMP groups active on this interface. Output Statistics
- ◆ **Report** – The number of IGMP membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

4.2.11.11 Group Statistics

Switch Management > IGMP Snooping > Group Statistics page is used to display IGMP snooping protocol-related statistics for the specified interface.

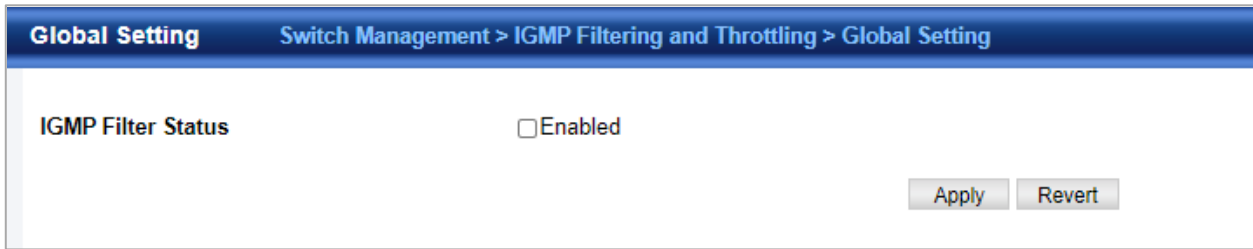
Group Statistics		Switch Management > IGMP Snooping > Group Statistics	
Group	1		
Input Statistics		Output Statistics	
Report	0	Report	0
Leave	0	Leave	0
G Query	0	G Query	0
G(-S)-S Query	0	G(-S)-S Query	0
Drop	0	Drop	0
Group	0	Group	0
Join Success	0		
<input type="button" value="Clear"/> <input type="button" value="Refresh"/>			

- ◆ **Group** – Group identifier. (Range: 1-12) Query Statistics
 - ◆ **Querier IP Address** – The IP address of the querier on this interface.
 - ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
 - ◆ **General Query Received** – The number of general queries received on this interface.
 - ◆ **General Query Sent** – The number of general queries sent from this interface.
 - ◆ **Specific Query Received** – The number of specific queries received on this interface.
 - ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
 - ◆ **Number of Reports Sent** – The number of reports sent from this interface.
 - ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.
- VLAN, Port, and Group Statistics Input Statistics
- ◆ **Report** – The number of IGMP membership reports received on this interface.
 - ◆ **Leave** – The number of leave messages received on this interface.
 - ◆ **G Query** – The number of general query messages received on this interface.
 - ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
 - ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or IGMP group report received.
 - ◆ **Join Success** – The number of times a multicast group was successfully joined.
- Output Statistics
- ◆ **Group** – The number of IGMP groups active on this interface.
 - ◆ **Report** – The number of IGMP membership reports sent from this interface.
 - ◆ **Leave** – The number of leave messages sent from this interface.
 - ◆ **G Query** – The number of general query messages sent from this interface.
 - ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

4.2.12 IGMP Filtering and Throttling

4.2.12.1 Global Setting

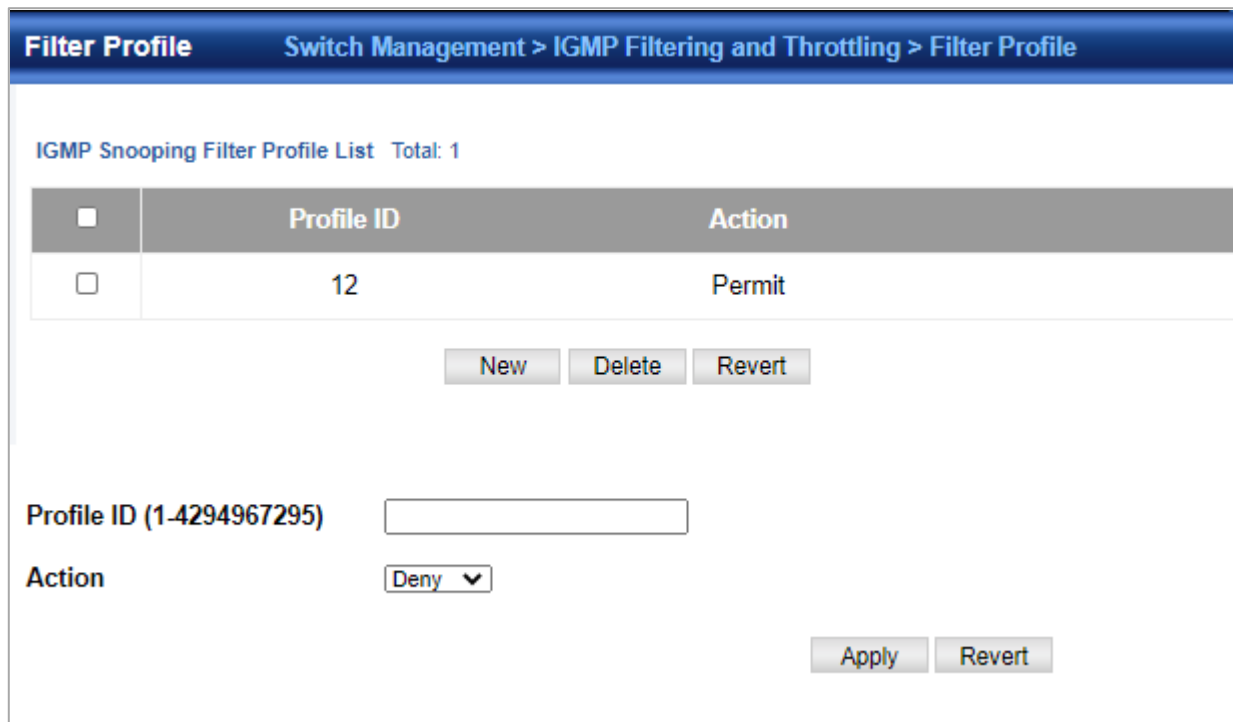
Switch Management > IGMP Filtering and Throttling>Global Setting page is used to enable IGMP filtering and throttling globally on the switch.



◆**IGMP Filter Status** – Enables IGMP filtering and throttling globally for the switch. (Default: Disabled)

4.2.12.2 Filter Profile

Switch Management > IGMP Filtering and Throttling>Filter Profile page is used to create an IGMP profile and set its access mode. Then use the (Add Multicast Group Range) page to configure the multicast groups to filter.



Profile ID	Action
12	Permit

◆**Profile ID** – Creates an IGMP profile. (Range: 1-4294967295)

◆**Access Mode** – Sets the access mode of the profile; either permit or deny. (Default: Deny) When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when the multicast group is not in the controlled range. Add Multicast Group Range

◆**Profile ID** – Selects an IGMP profile to configure.

◆**Start Multicast IP Address** – Specifies the starting address of a range of multicast groups.

◆**End Multicast IP Address** – Specifies the ending address of a range of multicast groups.

Filter Profile Switch Management > IGMP Filtering and Throttling > Filter Profile

IGMP Snooping Filter Profile List Total: 1

<input type="checkbox"/>	Profile ID	Action
<input type="checkbox"/>	12	Permit

To show the IGMP filter profiles:

1. Click Switch Management > IGMP Filtering and Throttling>Filter Profile.

4.2.12.3 Filter Range

Switch Management > IGMP Filtering and Throttling>Filter Range page is used to create an IGMP range and set its access mode. Then use the (new Multicast Group Range) page to configure the multicast groups to filter.

Filter Range Switch Management > IGMP Filtering and Throttling > Filter Range

Profile ID

Multicast IP Address Range List Total: 1

<input type="checkbox"/>	Start Multicast IP Address	End Multicast IP Address
<input type="checkbox"/>	224.1.1.1	224.1.1.10

Profile ID

Start Multicast IP Address

End Multicast IP Address

- ◆ **Start Multicast IP Address** – Specifies the starting address of a range of multicast groups.
- ◆ **End Multicast IP Address** – Specifies the ending address of a range of multicast groups.

Filter Range Switch Management > IGMP Filtering and Throttling > Filter Range

Profile ID

Multicast IP Address Range List Total: 1

<input type="checkbox"/>	Start Multicast IP Address	End Multicast IP Address
<input type="checkbox"/>	224.1.1.1	224.1.1.10

To show the multicast groups configured for an IGMP filter Range:

4.2.11.4 Configure Filter Interface

Switch Management > IGMP Filtering and Throttling>Configure Filter Interface page is used to assign and IGMP filter profile to interfaces on the switch, or to throttle multicast traffic by limiting the maximum number of multicast groups an interface can join at the same time.

Configure Filter Interface Switch Management > IGMP Filtering and Throttling > Configure Filter Interface

Interface Port Group

IGMP Filter and Throttling Port List Total: 26

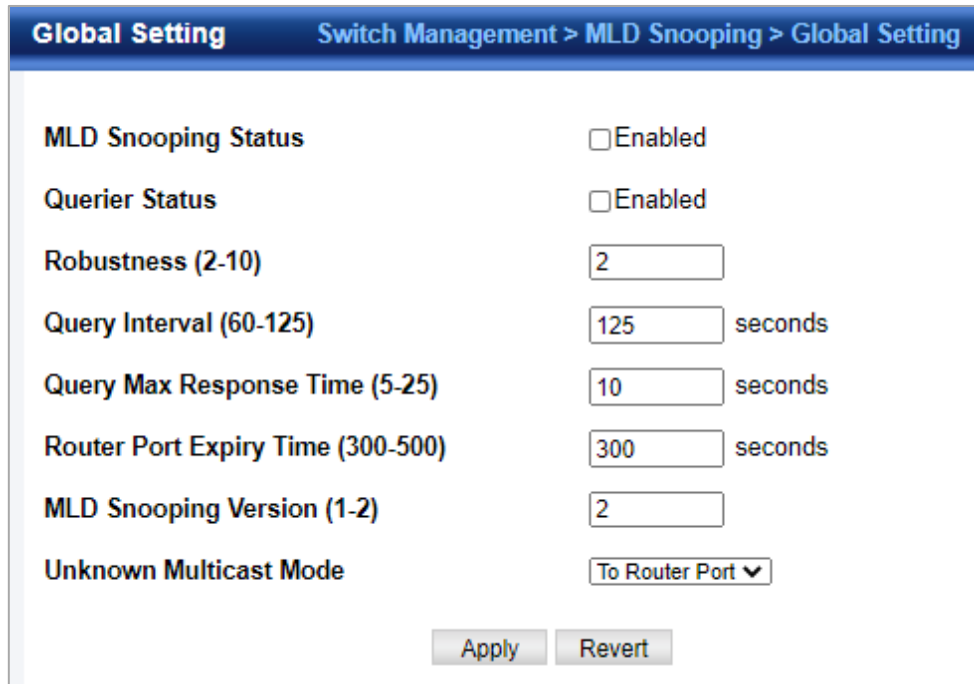
Port	Profile ID	Max Multicast Groups (1-255)	Current Multicast Groups	Throttling Action Mode	Throttling Status
1	(none)	255	0	Deny	False
2	(none)	255	0	Deny	False
3	(none)	255	0	Deny	False
4	(none)	255	0	Deny	False
5	(none)	255	0	Deny	False
6	(none)	255	0	Deny	False
7	(none)	255	0	Deny	False
8	(none)	255	0	Deny	False
9	(none)	255	0	Deny	False

- ◆ **Interface** – Port or group identifier. An IGMP profile or throttling setting can be applied to a port or trunk. When ports are configured as trunk members, the trunk uses the settings applied to the first port member in the trunk.
- ◆ **Profile ID** – Selects an existing profile to assign to an interface.
- ◆ **Max Multicast Groups** – Sets the maximum number of multicast groups an interface can join at the same time. (Range: 1-255; Default: 255)
- ◆ **Current Multicast Groups** – Displays the current multicast groups the interface has joined.
- ◆ **Throttling Action Mode** – Sets the action to take when the maximum number of multicast groups for the interface has been exceeded. (Default: Deny)
- **Deny** - The new multicast group join report is dropped.
- **Replace** - The new multicast group replaces an existing group.
- ◆ **Throttling Status** – Indicates if the throttling action has been implemented on the interface. (Options: True or False)

4.2.13 MLD Snooping

4.2.13.1 Global Setting

Switch Management > MLD Snooping > Global Setting page is used to configure the switch to forward multicast traffic intelligently.



Global Setting		Switch Management > MLD Snooping > Global Setting	
MLD Snooping Status	<input type="checkbox"/>	Enabled	
Querier Status	<input type="checkbox"/>	Enabled	
Robustness (2-10)	<input type="text"/>	2	
Query Interval (60-125)	<input type="text"/>	125	seconds
Query Max Response Time (5-25)	<input type="text"/>	10	seconds
Router Port Expiry Time (300-500)	<input type="text"/>	300	seconds
MLD Snooping Version (1-2)	<input type="text"/>	2	
Unknown Multicast Mode	<input type="text"/>	To Router Port	▼
		<input type="button" value="Apply"/>	<input type="button" value="Revert"/>

◆ **MLD Snooping Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.

(Default: Disabled)

◆ **Querier Status** – When enabled, the switch can serve as the querier for MLDv2 snooping if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

(Default: Disabled)

An IPv6 address must be configured on the VLAN interface from which the querier will act if elected. When serving as the querier, the switch uses this IPv6 address as the query source address. The querier will not start or will disable itself after having started if it detects an IPv6 multicast router on the network.

◆ **Robustness** – MLD Snooping robustness variable. A port will be removed from the receiver list for a multicast service when no MLD reports are detected in response to a number of MLD queries. The robustness variable sets the number of queries on ports for which there is no report.

(Range: 2-10 Default: 2)

◆ **Query Interval** – The interval between sending MLD general queries.

(Range: 60-125 seconds; Default: 125 seconds)

This attribute applies when the switch is serving as the querier. An MLD general query message is sent by the switch at the interval specified by this attribute. When this message is received by downstream hosts, all receivers build an MLD report for the multicast groups they have joined.

◆ **Query Max Response Time** – The maximum response time advertised in MLD general queries.

(Range: 5-25 seconds; Default: 10 seconds)

This attribute controls how long the host has to respond to an MLD Query message before the switch deletes the group if it is the last member.

◆ **Router Port Expiry Time** – The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface that had been receiving query packets) to have expired.

(Range: 300-500 seconds; Default: 300 seconds)

◆ **MLD Snooping Version** – The protocol version used for compatibility with other devices on the network. This is the MLD version the switch uses to send snooping reports.

(Range: 1-2; Default: 2)

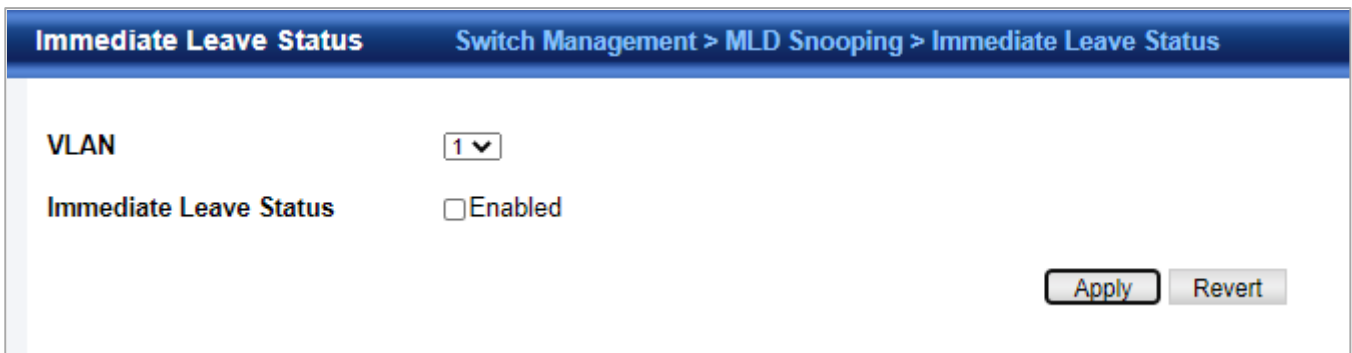
◆ **Unknown Multicast Mode** – The action for dealing with unknown multicast packets. Options include:

- **Flood** – Floods any received IPv6 multicast packets that have not been requested by a host to all ports in the VLAN.
- **To Router Port** – Forwards any received IPv6 multicast packets that have not been requested by a host to ports that are connected to a detected multicast router.

(This is the default action.)

4.2.13.2 Immediate Leave Status

Switch Management > MLD Snooping > Immediate Leave Status page is used to configure Immediate Leave status for a VLAN.

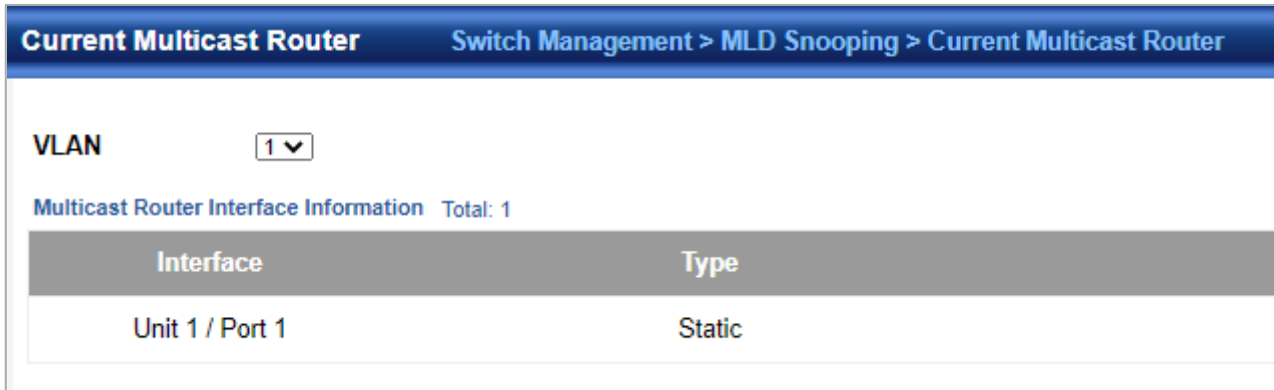


◆ **VLAN** – A VLAN identification number. (Range: 1-4094)

◆ **Immediate Leave Status** – Immediately deletes a member port of an IPv6 multicast service when a leave packet is received at that port and immediate leave is enabled for the parent VLAN. (Default: Disabled) If MLD immediate-leave is not used, a multicast router (or querier) will send a group-specific query message when an MLD group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. If MLD immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one MLD-enabled device, either a service host or a neighbor running MLD snooping.

4.2.13.3 Current Multicast Router

Switch Management > MLD Snooping > Current Multicast Router page is used to statically show an interface to an IPv6 multicast router/switch.



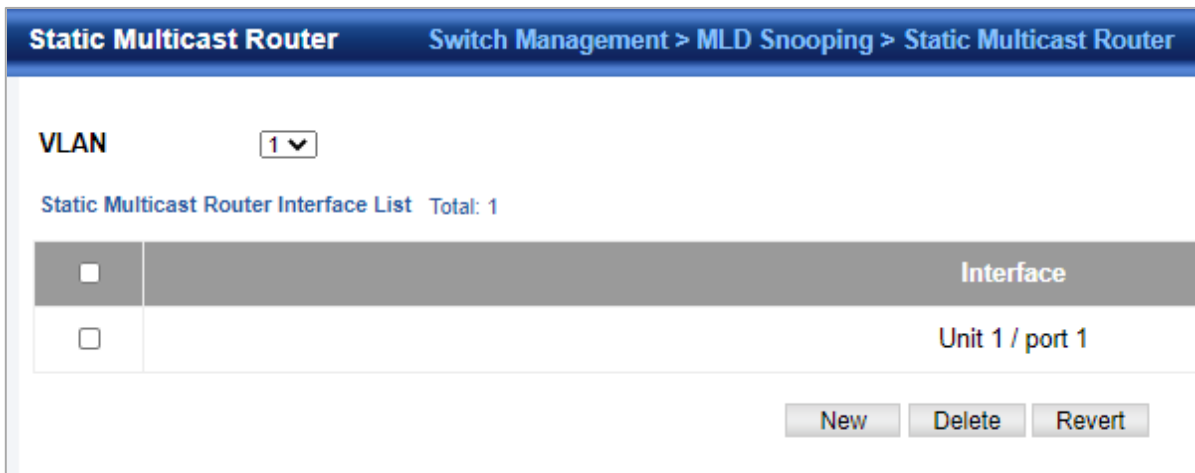
Interface	Type
Unit 1 / Port 1	Static

◆ **VLAN** – Selects the VLAN which is to propagate all IPv6 multicast traffic coming from the attached multicast router. (Range: 1-4094)

◆ **Interface** – Activates the Port or group scroll down list.

4.2.13.4 Static Multicast Router

Switch Management > MLD Snooping > Static Multicast Router page is used to statically add an interface to an IPv6 multicast router/switch.



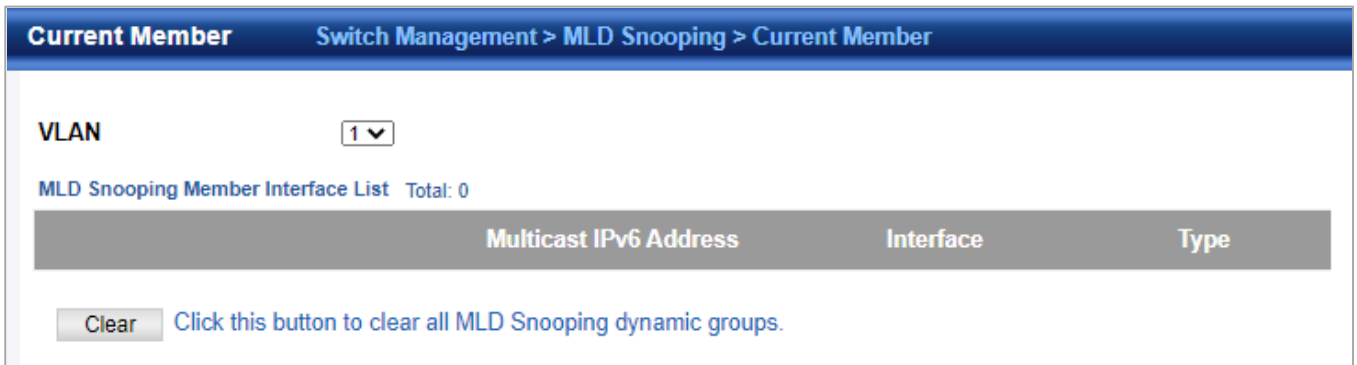
<input type="checkbox"/>	Interface
<input type="checkbox"/>	Unit 1 / port 1

◆ **VLAN** – Selects the VLAN which is to propagate all IPv6 multicast traffic coming from the attached multicast router. (Range: 1-4094)

◆ **Interface** – Activates the Port or group scroll down list.

4.2.13.5 Current Member

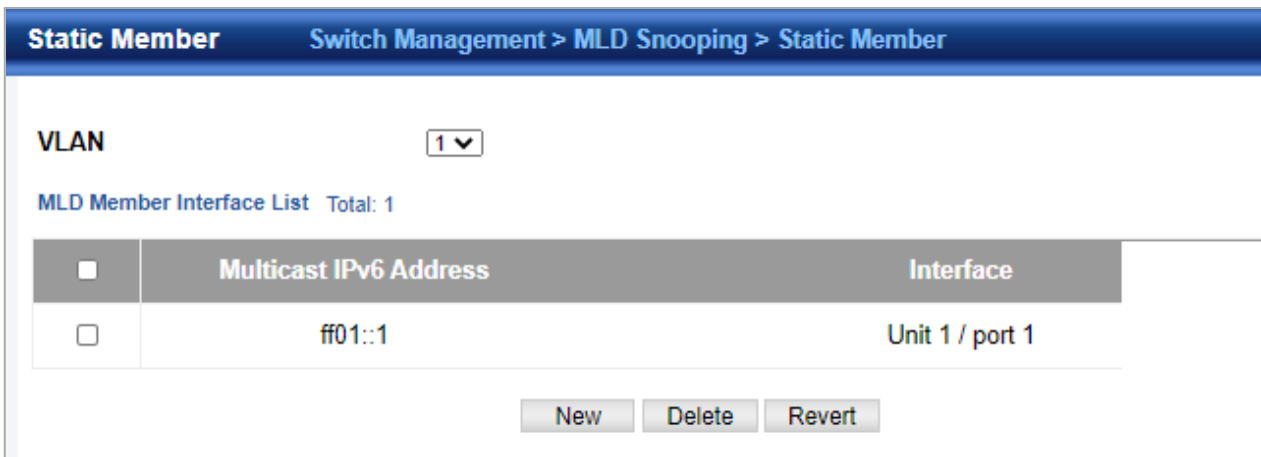
Switch Management > MLD Snooping > Current Member page is used to statically show an IPv6 multicast service to an interface.



- ◆ **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4094)
- ◆ **Multicast IPv6 Address** – The IP address for a specific multicast service.
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port or Group** – Specifies the interface assigned to a multicast group.
- ◆ **Type (Show Current Member)** – Shows if this multicast stream was statically configured by the user, discovered by MLD Snooping, or is a data stream to which no other ports are subscribing (i.e., the stream is flooded onto VLAN instead of being trapped to the CPU for processing, or is being processed by MVR6).

4.2.13.6 Static Member

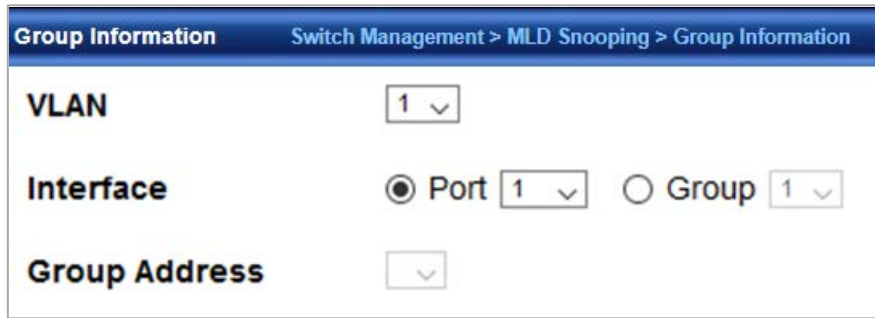
Switch Management > MLD Snooping > Static Member page is used to statically add an IPv6 multicast service to an interface.



- ◆ **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4094)
- ◆ **Multicast IPv6 Address** – The IP address for a specific multicast service.
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port or Group** – Specifies the interface assigned to a multicast group.
- ◆ **Type (Show Current Member)** – Shows if this multicast stream was statically configured by the user, discovered by MLD Snooping, or is a data stream to which no other ports are subscribing (i.e., the stream is flooded onto VLAN instead of being trapped to the CPU for processing, or is being processed by MVR6).

4.2.13.7 Group Information

Switch Management > MLD Snooping > Group Information page is used to display and set known multicast groups, member ports, the means by which each group was learned, and the corresponding source list.



- ◆ **VLAN** – VLAN identifier. (Range: 1-4094)
- ◆ **Interface** – Port or group identifier.
- ◆ **Group Address** – The IP address for a specific multicast service.
- ◆ **Type** – The means by which each group was learned – MLD Snooping or Multicast Data.
- ◆ **Filter Mode** – The filter mode is used to summarize the total listening state of a multicast address to a minimum set such that all nodes' listening states are respected. In Include mode, the router only uses the request list, indicating that the reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the hosts' source-list. In Exclude mode, the router uses both the request list and exclude list, indicating that the reception of packets sent to the given multicast address is requested from all IP source addresses, except for those listed in the exclude source-list and for any other sources where the source timer status has expired.
- ◆ **Filter Timer Elapse** – The Filter timer is only used when a specific multicast address is in Exclude mode. It represents the time for the multicast address filter mode to expire and change to Include mode.
- ◆ **Request List** – Sources included on the router's request list.
- ◆ **Exclude List** – Sources included on the router's exclude list.

4.2.13.8 Statistics

Switch Management > MLD Snooping > Statistics pages is used to display MLD Snooping protocol related statistics for the specified interface.

Statistics							
Switch Management > MLD Snooping > Statistics							
Type <input checked="" type="radio"/> Input <input type="radio"/> Output <input type="radio"/> Query <input type="radio"/> Clear							
Input Statistics Total: 28							
Interface	Report	Leave	G Query	G(-S)-S Query	Drop	Join Success	Group
Eth 1/1	0	0	0	0	0	0	0
Eth 1/2	0	0	0	0	0	0	0
Eth 1/3	0	0	0	0	0	0	0
Eth 1/4	0	0	0	0	0	0	0
Eth 1/5	0	0	0	0	0	0	0
Eth 1/6	0	0	0	0	0	0	0
Eth 1/7	0	0	0	0	0	0	0
Eth 1/8	0	0	0	0	0	0	0
Eth 1/9	0	0	0	0	0	0	0
Eth 1/10	0	0	0	0	0	0	0

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Group** – group identifier. (Range: 1-12) Query Statistics
- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and group Statistics Input Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR groups active on this interface. Output Statistics
- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR groups active on this interface.

To display statistics for MLD Snooping input:

Statistics Switch Management > MLD Snooping > Statistics							
Type <input checked="" type="radio"/> Input <input type="radio"/> Output <input type="radio"/> Query <input type="radio"/> Clear							
Input Statistics Total: 28							
Interface	Report	Leave	G Query	G(-S)-S Query	Drop	Join Success	Group
Eth 1/1	0	0	0	0	0	0	0
Eth 1/2	0	0	0	0	0	0	0
Eth 1/3	0	0	0	0	0	0	0
Eth 1/4	0	0	0	0	0	0	0
Eth 1/5	0	0	0	0	0	0	0
Eth 1/6	0	0	0	0	0	0	0
Eth 1/7	0	0	0	0	0	0	0
Eth 1/8	0	0	0	0	0	0	0
Eth 1/9	0	0	0	0	0	0	0
Eth 1/10	0	0	0	0	0	0	0

To display statistics for MLD Snooping output:

Statistics Switch Management > MLD Snooping > Statistics						
Type <input type="radio"/> Input <input checked="" type="radio"/> Output <input type="radio"/> Query <input type="radio"/> Clear						
Output Statistics Total: 28						
Interface	Report	Leave	G Query	G(-S)-S Query	Drop	Group
Eth 1/1	0	0	0	0	0	0
Eth 1/2	0	0	0	0	0	0
Eth 1/3	0	0	0	0	0	0
Eth 1/4	0	0	0	0	0	0
Eth 1/5	0	0	0	0	0	0
Eth 1/6	0	0	0	0	0	0
Eth 1/7	0	0	0	0	0	0
Eth 1/8	0	0	0	0	0	0
Eth 1/9	0	0	0	0	0	0

To display statistics for MLD Snooping Query:

Statistics
Switch Management > MLD Snooping > Statistics

Type Input Output Query Clear

VLAN

Query Statistics

Other Querier Address	None
Other Querier Expire	0(m):0(s)
Other Querier Uptime	0(h):0(m):0(s)
Self Querier Address	::
Self Querier Expire Time	0(m):0(s)
Self Querier Uptime	0(h):0(m):0(s)
General Query Received	0
General Query Sent	0
Specific Query Received	0
Specific Query Sent	0

Statistics
Switch Management > MLD Snooping > Statistics

Type Input Output Query Clear

Interface All

VLAN

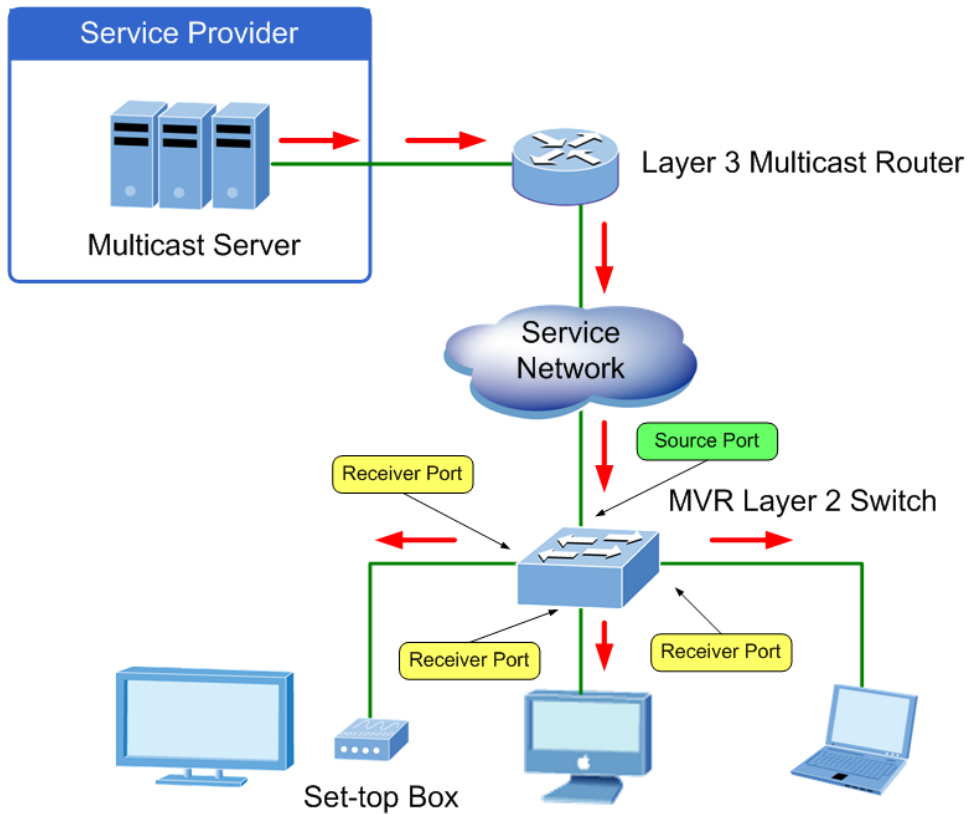
Unit / Port

Group

4.2.14 MVR For IPv4

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

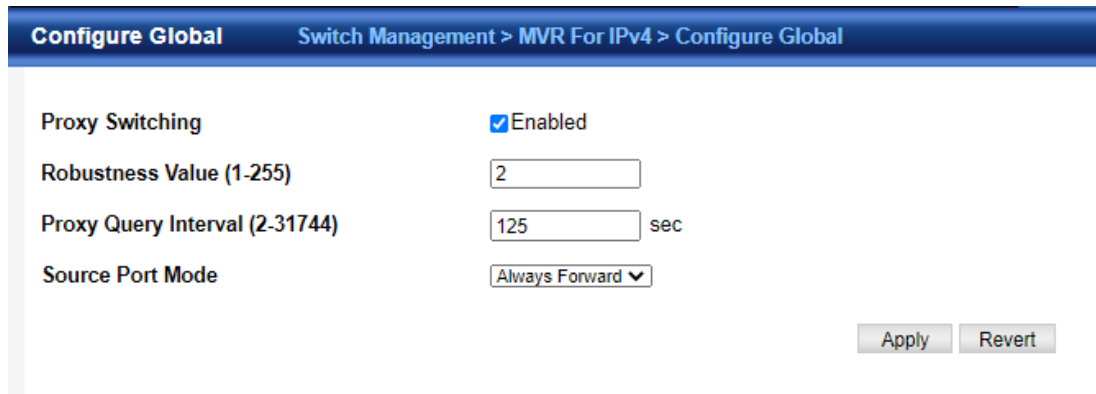
- In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream.
 - Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top 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.



4.2.14.1 Configure Global

Switch Management > MVR for IPv4 > Configure Global page is used to configure proxy switching and the robustness variable.

◆ **Proxy Switching** – Configures MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. (Default: Enabled)



- When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface, and the MVR receiver port serves as the querier. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.
- Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by
 - maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.
 - When the source port receives report and leave messages, it only forwards them to other source ports.
 - When receiver ports receive any query messages, they are dropped.
 - When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.
- When MVR proxy switching is disabled:
 - Any membership reports received from receiver/source ports are forwarded to all source ports.
 - When a source port receives a query message, it will be forwarded to all downstream receiver ports.
 - When a receiver port receives a query message, it will be dropped.

◆ **Robustness Value** – Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. (Range: 1-255; Default: 2)

- This parameter is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
- This parameter only takes effect when MVR proxy switching is enabled.

◆ **Proxy Query Interval** – Configures the interval at which the receiver port sends out general queries. (Range: 2-31744 seconds; Default: 125 seconds)

- This parameter sets the general query interval at which active receiver ports send out general queries.
- This interval is only effective when proxy switching is enabled.

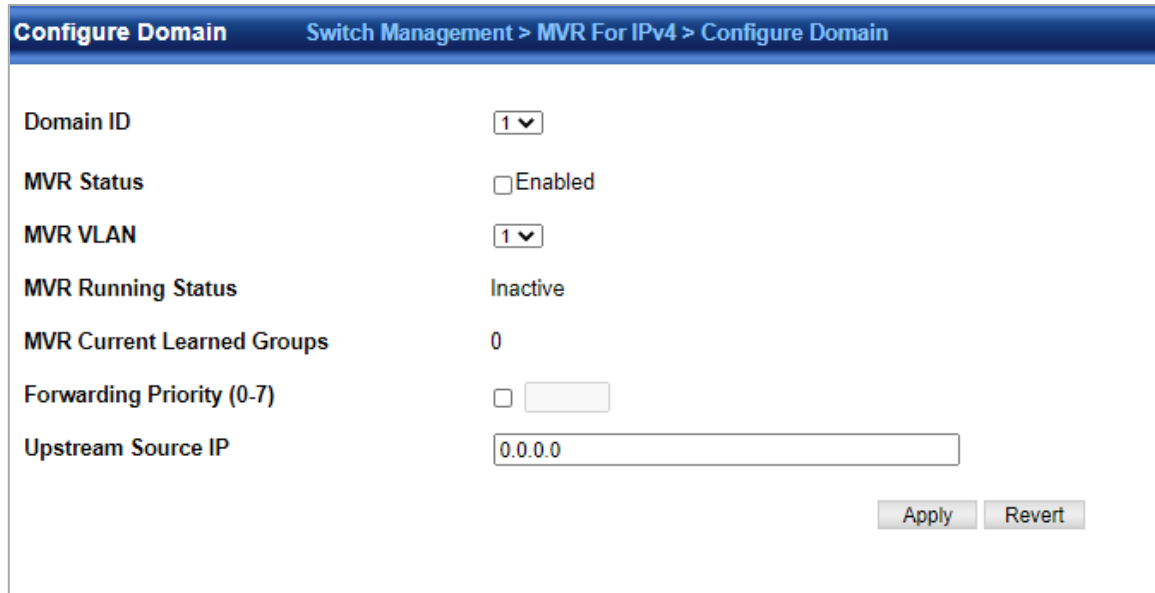
◆ **Source Port Mode** – Configures the switch to forward any multicast streams within the parameters set by a profile, or to only forward multicast streams which the source port has dynamically joined.

- **Always Forward** – By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.

- Dynamic** – When dynamic mode is enabled, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

4.2.14.2 Configure Domain

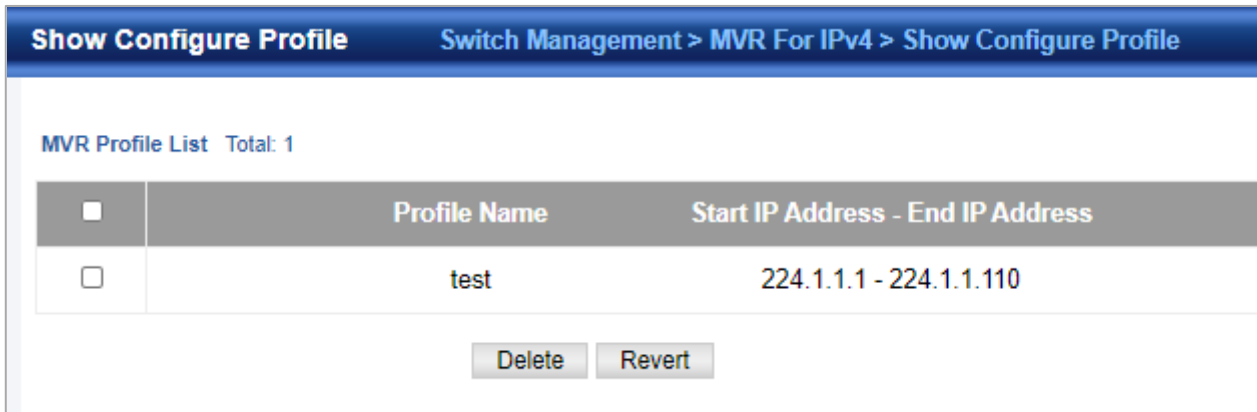
Switch Management > MVR For IPv4 > Configure Domain page is used to enable MVR globally on the switch, and select the VLAN that will serve as the sole channel for common multicast streams supported by the service provider.



- ◆ Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ MVR Status** – When MVR is enabled on the switch, any multicast data associated with an MVR group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group. (Default: Disabled)
- ◆ MVR VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR. MVR source ports should be configured as members of the MVR VLAN (see "[Adding Static Members to VLANs](#)"), but MVR receiver ports should not be manually configured as members of this VLAN. (Default: 1)
- ◆ MVR Running Status** – Indicates whether or not all necessary conditions in the MVR environment are satisfied. Running status is Active as long as MVR is enabled, the specified MVR VLAN exists, and a source port with a valid link has been configured (see "[Configuring MVR Interface Status](#)").
- ◆ MVR Current Learned Groups** – The number of MVR groups currently assigned to this domain.
- ◆ Forwarding Priority** – The CoS priority assigned to all multicast traffic forwarded into this domain. (Range: 0-6, where 6 is the highest priority) This parameter can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.
- ◆ Upstream Source IP** – The source IP address assigned to all MVR control packets sent upstream on the specified domain. By default, all MVR reports sent upstream use a null source IP address.

4.2.14.3 Show Configure Profile

Switch Management > MVR for IPv4 > Show Configure Profile pages is used to display the multicast group address for required services to one or more MVR domains.

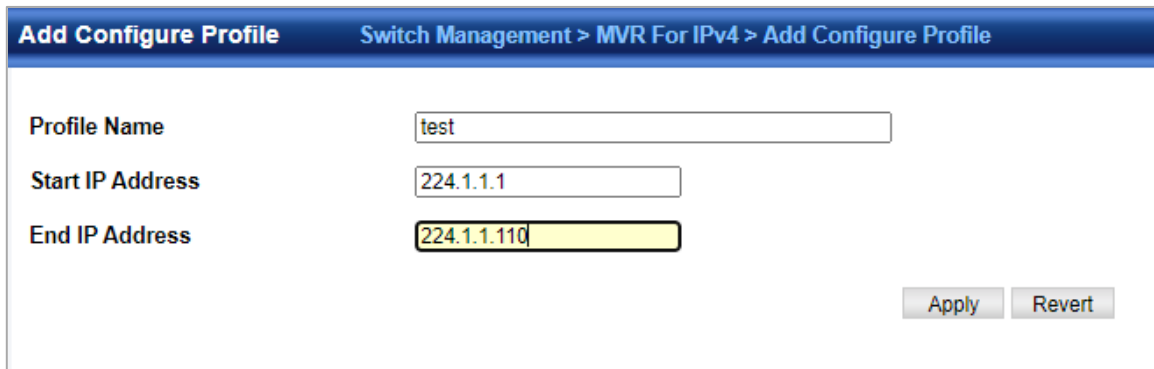


<input type="checkbox"/>	Profile Name	Start IP Address - End IP Address
<input type="checkbox"/>	test	224.1.1.1 - 224.1.1.110

- ◆ **Profile Name** – The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)
- ◆ **Start IP Address** – Starting IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)
- ◆ **End IP Address** – Ending IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255) Associate Profile

4.2.14.4 Add Configure Profile

Switch Management > MVR for IPv4 > Add Configure Profile page is used to assign the multicast group address for required services to one or more MVR domains.



Profile Name

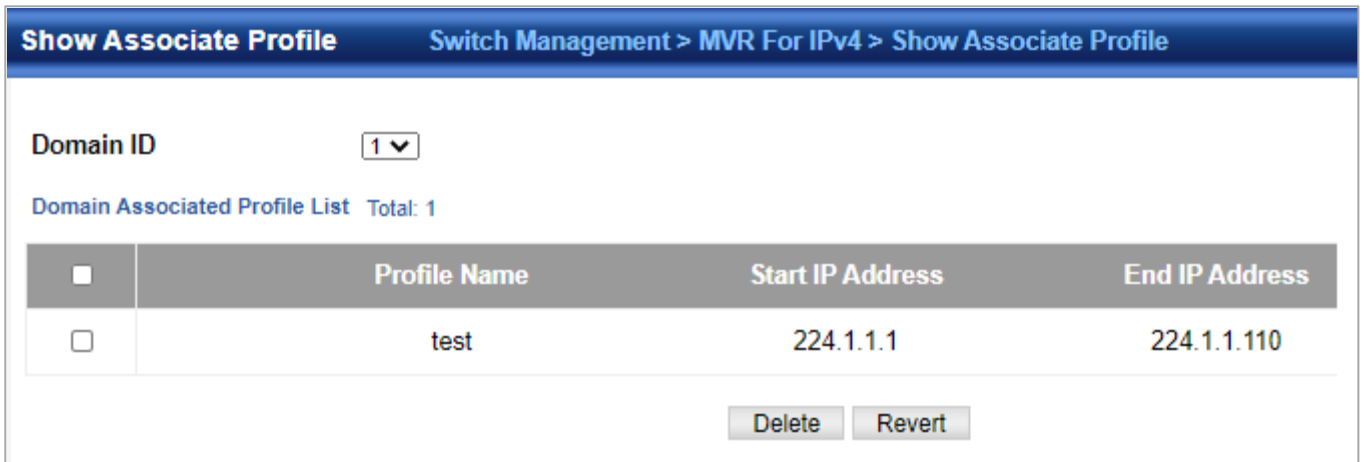
Start IP Address

End IP Address

- ◆ **Profile Name** – The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)
 - ◆ **Start IP Address** – Starting IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)
 - ◆ **End IP Address** – Ending IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255) Associate Profile
- (Range: 1-21 characters)

4.2.14.5 Show Associate Profile

Switch Management > MVR for IPv4 > Show Associate Profile pages is used to show the multicast group address for required services to one or more MVR domains.



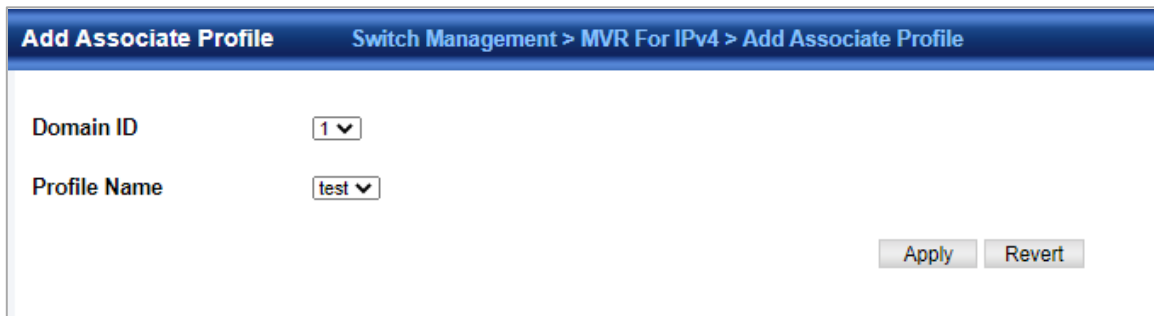
<input type="checkbox"/>	Profile Name	Start IP Address	End IP Address
<input type="checkbox"/>	test	224.1.1.1	224.1.1.110

- ◆ **Profile Name** – The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)
- ◆ **Start IP Address** – Starting IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)
- ◆ **End IP Address** – Ending IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255) Associate Profile
- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)

To show the MVR group address profiles assigned to a domain:

4.2.14.6 Add Associate Profile

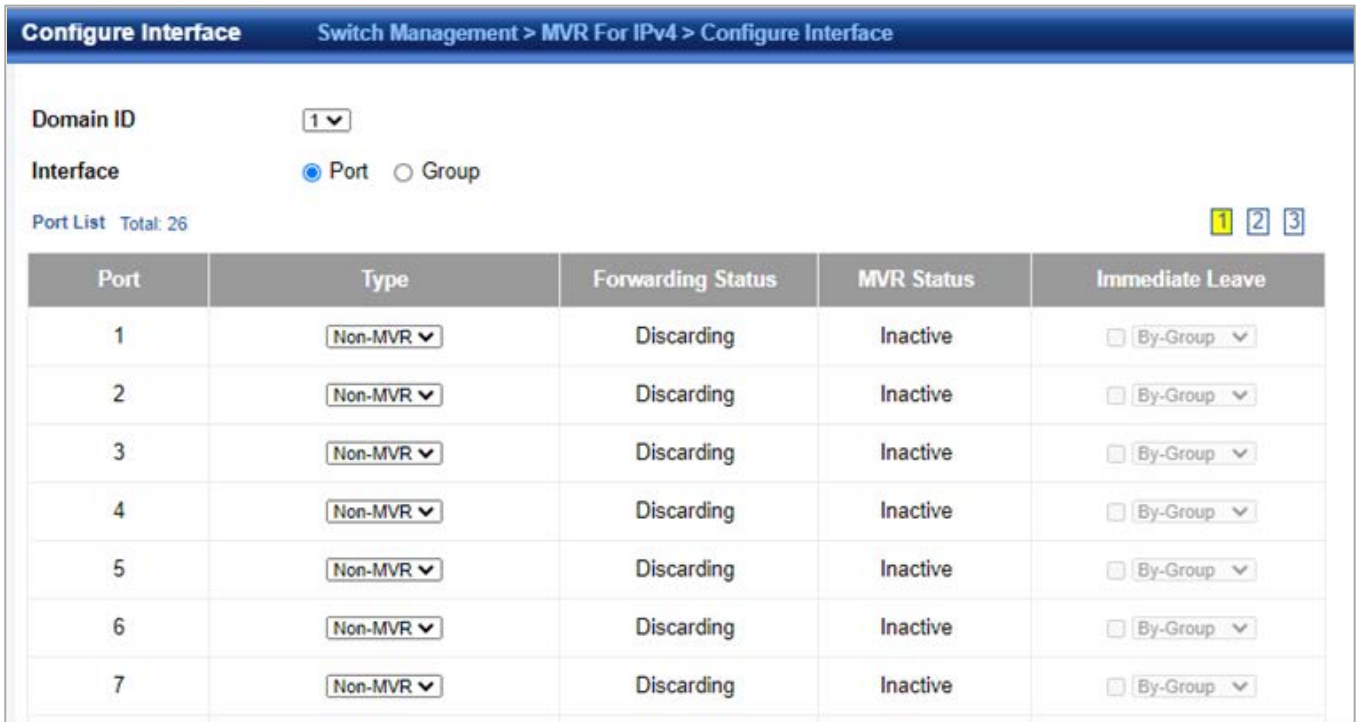
Switch Management > MVR for IPv4 > Add Associate Profile page is used to assign the multicast group address for required services to one or more MVR domains.



- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-21 characters)

4.2.14.7 Configure Interface

Switch Management > MVR for IPv4 > Configure Interface page is used to configure each interface that participates in the MVR protocol as a source port or receiver port.



Port	Type	Forwarding Status	MVR Status	Immediate Leave
1	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
2	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
3	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
4	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
5	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
6	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
7	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Port/Group** – Interface identifier.
- ◆ **Type** – The following interface types are supported:
 - **Source** – An uplink port that can send and receive multicast data for the groups assigned to the MVR VLAN. Note that the source port must be manually configured as a member of the MVR VLAN.
 - **Receiver** – A subscriber port that can receive multicast data sent through the MVR VLAN. Any port configured as an receiver port will be dynamically added to the MVR VLAN when it forwards an IGMP report or join message from an attached host requesting any of the designated multicast services supported by the MVR VLAN. Just remember that only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned.
 - **Non-MVR** – An interface that does not participate in the MVR VLAN. (This is the default type.)
- ◆ **Forwarding Status** – Shows if MVR traffic is being forwarded or discarded.
- ◆ **MVR Status** – Shows the MVR status. MVR status for source ports is “Active” if MVR is globally enabled on the switch. MVR status for receiver ports is “Active” only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface.
- ◆ **Immediate Leave** – Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. (This option only applies to an interface configured as an MVR receiver.)

4.2.14.8 Show Static Group Member

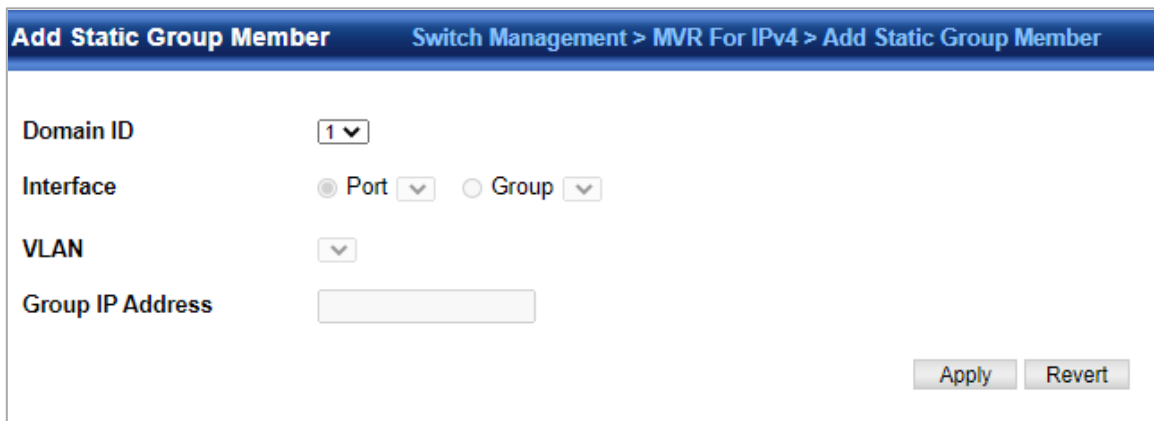
Switch Management > MVR For IPv4 > Show Static Group Member page is used to statically show multicast groups for a port or trunk which will receive long-term multicast streams associated with a stable set of hosts.



- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Interface** – Port or group identifier.
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Group IP Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR group range configured on the Configure General page.

4.2.14.9 Add Static Group Member

Switch Management > MVR For IPv4 > Add Static Group Member page is used to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.



- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Interface** – Port or group identifier.
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Group IP Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR group range configured on the Configure General page.

4.2.14.10 Show Member

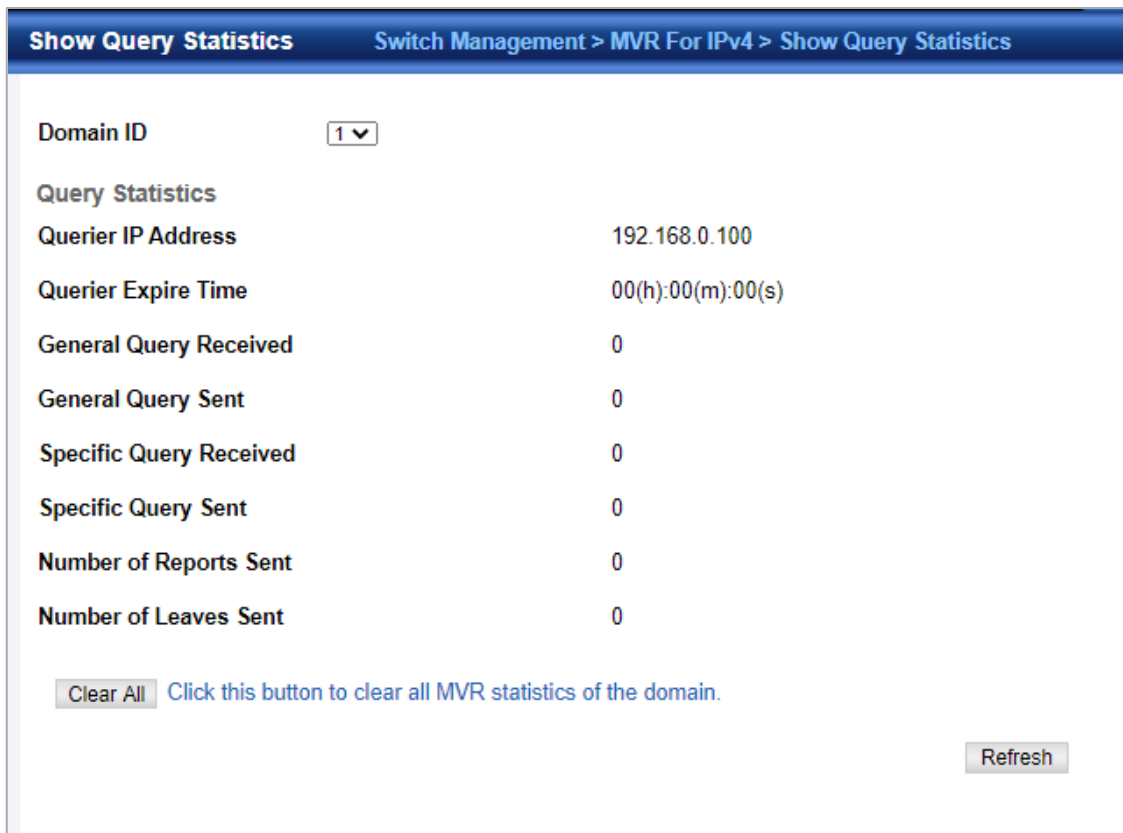
Switch Management > MVR For IPv4 > Show Member page is used to show the multicast groups either statically or dynamically assigned to the MVR receiver groups on each interface.



- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Group IP Address** – Multicast groups assigned to the MVR VLAN.
- ◆ **VLAN** – The VLAN through which the service is received. Note that this may be different from the MVR VLAN if the group address has been statically assigned.
- ◆ **Port** – Shows the interfaces with subscribers for multicast services provided through the MVR VLAN.
- ◆ **Up Time** – Time this service has been forwarded to attached clients.
- ◆ **Expire** – Time before this entry expires if no membership report is received from currently active or new clients.
- ◆ **Count** – The number of multicast services currently being forwarded from the MVR VLAN.

4.2.14.11 Show Query Statistics

Switch Management > MVR for IPv4 > Show Query Statistics page is used to display MVR protocol related statistics for the specified interface.



- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Group** – group identifier. (Range: 1-12) Query Statistics
- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics Input Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR groups active on this interface. Output Statistics
- ◆ **Report** – The number of IGMP membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

4.2.14.12 Show VLAN Statistics

Switch Management > MVR for IPv4 > Show VLAN Statistics page is used to display MVR protocol related statistics for the specified interface.

Show VLAN Statistics
Switch Management > MVR For IPv4 > Show VLAN Statistics

Domain ID 1 ▾

VLAN 1 ▾

Input Statistics

Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		

Output Statistics

Report	0
Leave	0
G Query	0
G(-S)-S Query	0

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Group** – Group identifier. (Range: 1-12) Query Statistics
- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics Input Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.

- ◆ **Group** – The number of MVR groups active on this interface. Output Statistics
- ◆ **Report** – The number of IGMP membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

4.2.14.13 Show Port Statistics

Switch Management > MVR for IPv4 > Show Port Statistics page is used to display MVR protocol related statistics for the specified interface.

Show Port Statistics
Switch Management > MVR For IPv4 > Show Port Statistics

Domain ID 1 ▾

Port 25 ▾

Input Statistics

Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		

Output Statistics

Report	0		
Leave	0		
G Query	0		
G(-S)-S Query	0		

Clear
Refresh

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Group** – Group identifier. (Range: 1-12) Query Statistics
- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics Input Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR groups active on this interface. Output Statistics

- ◆ **Report** – The number of IGMP membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

4.2.14.14 Show Group Statistics

Switch Management > MVR for IPv4 > Show Group Statistics page is used to display MVR protocol related statistics for the specified interface.

Show Group Statistics
Switch Management > MVR For IPv4 > Show Group Statistics

Domain ID

Group

Input Statistics

Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		

Output Statistics

Report	0
Leave	0
G Query	0
G(-S)-S Query	0

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Group** – Group identifier. (Range: 1-12) Query Statistics
- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics Input Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.

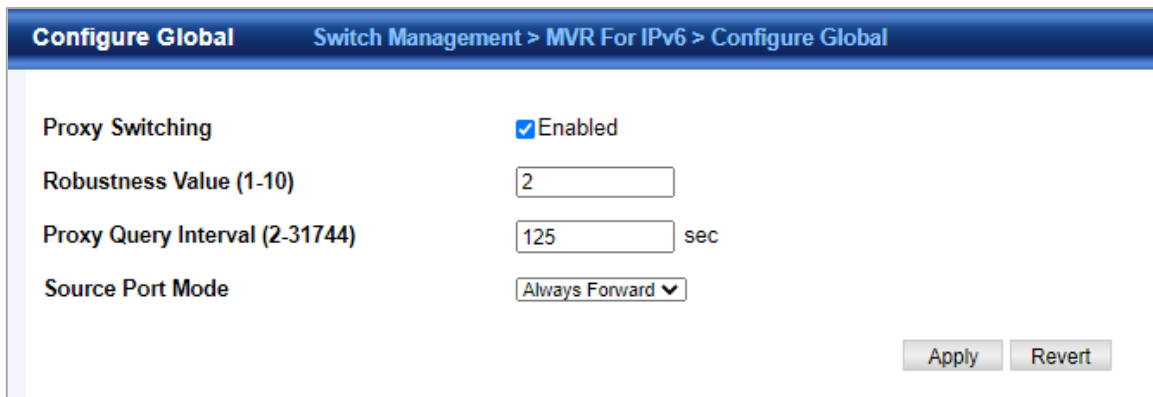
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR groups active on this interface. Output Statistics
- ◆ **Report** – The number of IGMP membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

4.2.15 MVR For IPv6

4.2.15.1 Configure Global

Switch Management > MVR for IPv6 > Configure Global page is used to configure proxy switching and the robustness variable.

- ◆ **Proxy Switching** – Configures MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. (Default: Enabled)



- When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface, and the MVR receiver port serves as the querier. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.
- Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.
- When the source port receives report and leave messages, it only forwards them to other source ports.
- When receiver ports receive any query messages, they are dropped.
- When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.
- When MVR proxy switching is disabled:
 - Any membership reports received from receiver/source ports are forwarded to all source ports.
 - When a source port receives a query message, it will be forwarded to all downstream receiver ports.
 - When a receiver port receives a query message, it will be dropped.

- ◆ **Robustness Value** – Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. (Range: 1-10; Default: 2)

- This parameter is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
- This parameter only takes effect when MVR6 proxy switching is enabled.

- ◆ **Proxy Query Interval** – Configures the interval at which the receiver port sends out general queries. (Range: 2-31744 seconds; Default: 125 seconds)

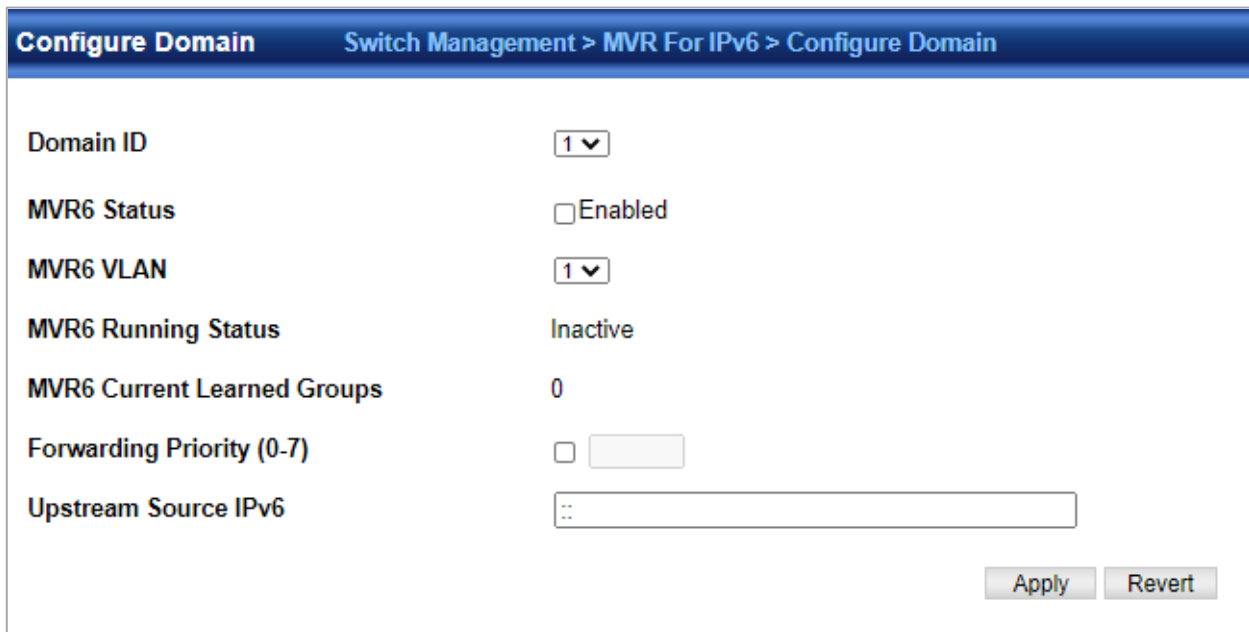
- This parameter sets the general query interval at which active receiver ports send out general queries.
- This interval is only effective when proxy switching is enabled.

◆ **Source Port Mode** – Configures the switch to forward any multicast streams within the parameters set by a profile, or to only forward multicast streams which the source port has dynamically joined.

- **Always Forward** – By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.
- **Dynamic** – When dynamic mode is enabled, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

4.2.15.2 Configure Domain

Switch Management > MVR For IPv6 > Configure Domain page is used to enable MVR6 globally on the switch, and select the VLAN that will serve as the sole channel for common multicast streams supported by the service provider.



- ◆ **Domain ID**– An independent multicast domain. (Range: 1-5)
- ◆ **MVR6 Status** – When MVR6 is enabled on the switch, any multicast data associated with an MVR6 group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group. (Default: Disabled)
- ◆ **MVR6 VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR6. MVR6 source ports should be configured as members of the MVR6 VLAN, but MVR6 receiver ports should not be manually configured as members of this VLAN. (Default: 1)
- ◆ **MVR6 Running Status** – Indicates whether or not all necessary conditions in the MVR6 environment are satisfied. Running status is Active as long as MVR6 is enabled, the specified MVR6 VLAN exists, and a source port with a valid link has been configured.
- ◆ **MVR6 Current Learned Groups** – The number of MVR6 groups currently assigned to this domain.

◆ **Upstream Source IPv6** – The source IPv6 address assigned to all MVR6 control packets sent upstream on the specified domain. This parameter must be a full IPv6 address including the network prefix and host address bits. By default, all MVR6 reports sent upstream use a null source IP address. All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

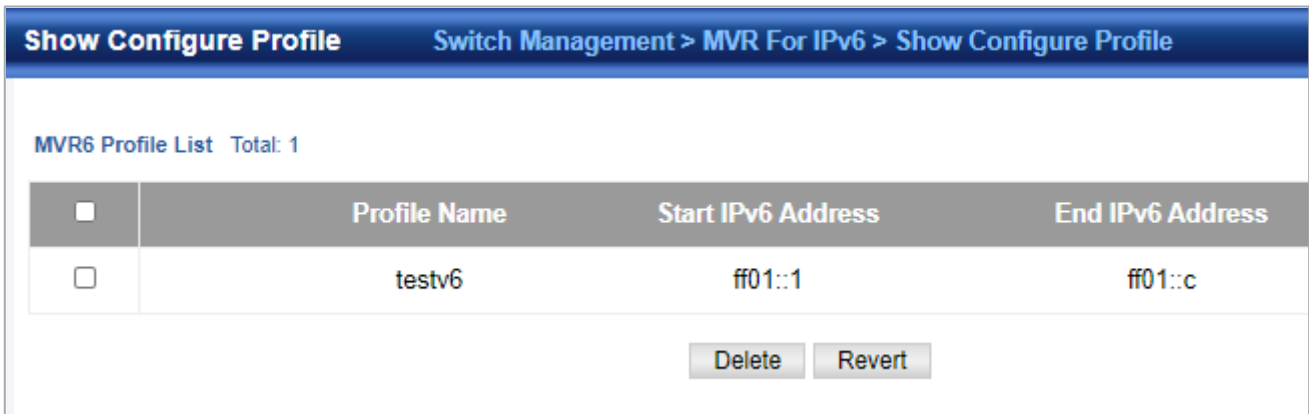
WEB INTERFACE

To configure settings for an MVR6 domain:

1. Click Switch Management > MVR For IPv6 >Configure Domain.
2. Select a domain from the scroll-down list.
3. Enable MVR6 for the selected domain, select the MVR6 VLAN, set the forwarding priority to be assigned to all ingress multicast traffic, and set the source IP address for all control packets sent upstream as required.
4. Click Apply.

4.2.15.3 Show Configure Profile

Switch Management > MVR for IPv6> Show Configure Profile page is used to assign the multicast group address for required services to one or more MVR6 domains.

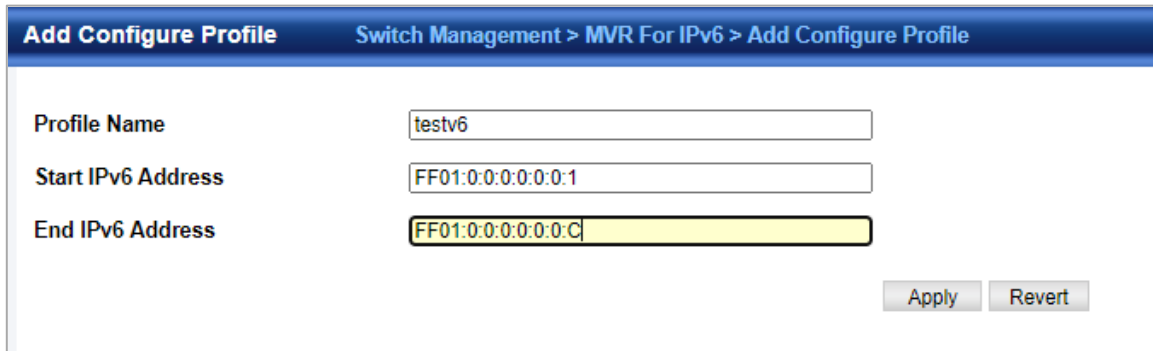


<input type="checkbox"/>	Profile Name	Start IPv6 Address	End IPv6 Address
<input type="checkbox"/>	testv6	ff01::1	ff01::c

- ◆ **Profile Name** – The name of a profile containing one or more MVR6 group addresses. (Range: 1-21 characters)
- ◆ **Start IPv6 Address** – Starting IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.
- ◆ **End IPv6 Address** – Ending IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits. Associate Profile
- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-20 characters)

4.2.15.4 Add Configure Profile

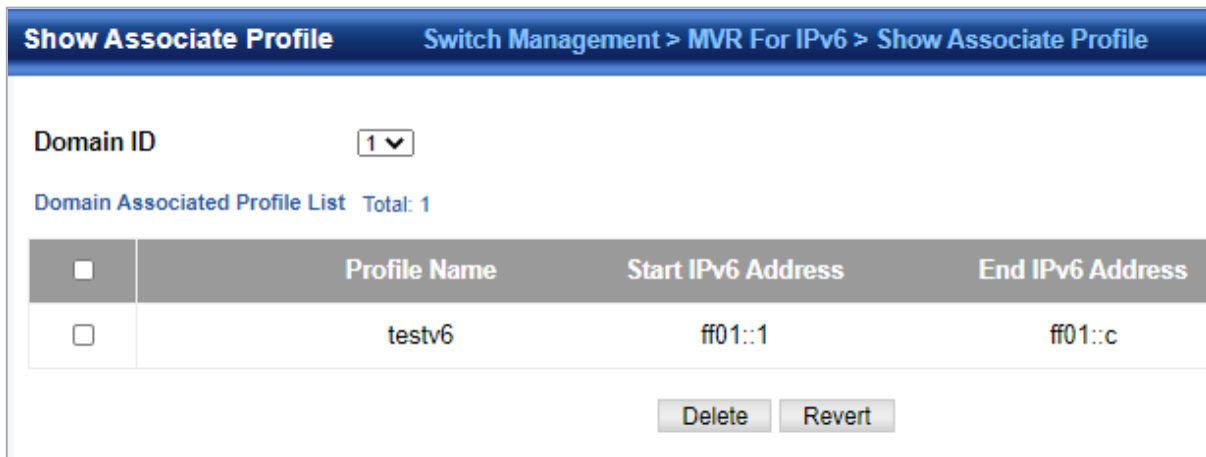
Switch Management > MVR for IPv6 > Add Configure Profile page is used to assign the multicast group address for required services to one or more MVR6 domains.



- ◆ **Profile Name** – The name of a profile containing one or more MVR6 group addresses. (Range: 1-21 characters)
- ◆ **Start IPv6 Address** – Starting IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.
- ◆ **End IPv6 Address** – Ending IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits. Associate Profile
- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-20 characters)

4.2.15.5 Show Associate Profile

Switch Management > MVR For IPv6 > Show Associate Profile page is used to show the multicast group address for required services to one or more MVR6 domains.

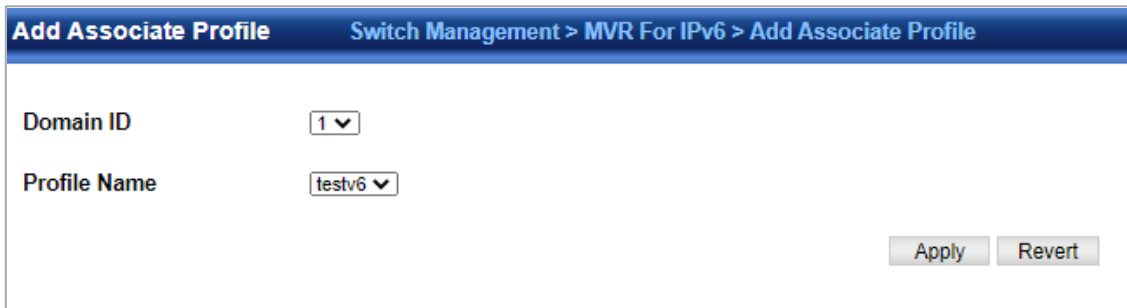


<input type="checkbox"/>	Profile Name	Start IPv6 Address	End IPv6 Address
<input type="checkbox"/>	testv6	ff01::1	ff01::c

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-20 characters)

4.2.15.6 Add Associate Profile

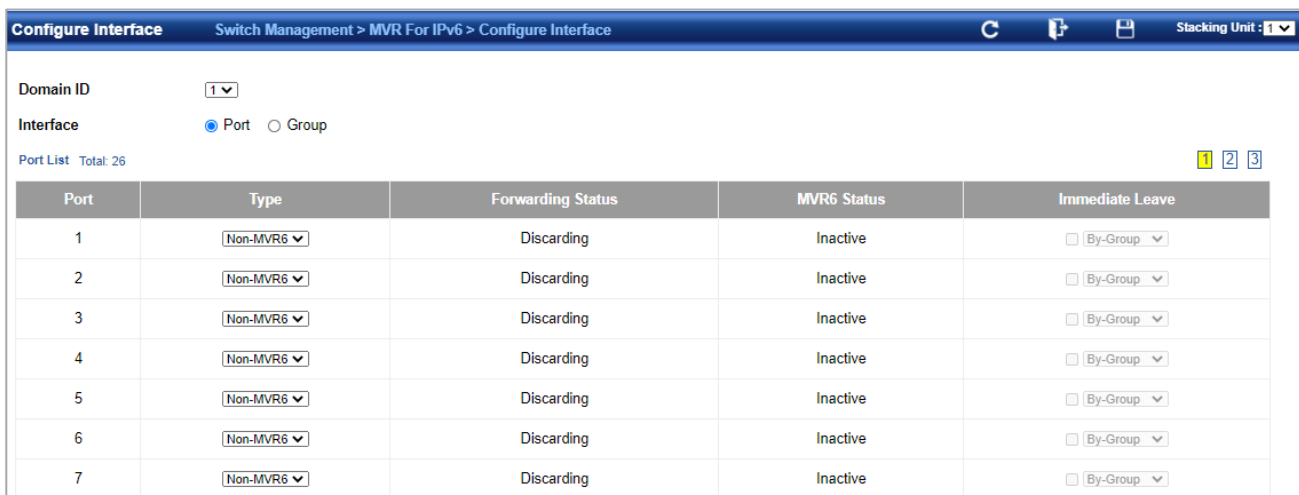
Switch Management > MVR for IPv6 > Add Associate Profile page is used to assign the multicast group address for required services to one or more MVR6 domains.



- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-20 characters)

4.2.15.7 Configure Interface

Switch Management > MVR for IPv6 > Configure Interface page is used to configure each interface that participates in the MVR6 protocol as a source port or receiver port. If you are sure that only one subscriber attached to an interface is receiving multicast services, you can enable the immediate leave function.




Port	Type	Forwarding Status	MVR6 Status	Immediate Leave
1	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> By-Group
2	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> By-Group
3	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> By-Group
4	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> By-Group
5	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> By-Group
6	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> By-Group
7	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> By-Group

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Port/Group** – Interface identifier.
- ◆ **Type** – The following interface types are supported:
 - **Non-MVR6** – An interface that does not participate in the MVR6 VLAN. (This is the default type.)
 - **Source** – An uplink port that can send and receive multicast data for the groups assigned to the MVR6 VLAN. Note that the source port must be manually configured as a member of the MVR6 VLAN.
 - **Receiver** – A subscriber port that can receive multicast data sent through the MVR6 VLAN. Also, note that VLAN membership for MVR receiver ports cannot be set to access mode.
- ◆ **Forwarding Status** – Shows if multicast traffic is being forwarded or blocked.
- ◆ **MVR6 Status** – Shows the MVR6 status. MVR6 status for source ports is “Active” if MVR6 is globally enabled on the switch. MVR6 status for receiver ports is “Active” only if there are subscribers receiving multicast traffic from one of the MVR6 groups, or a multicast group has been statically assigned to an interface.
- ◆ **Immediate Leave** – Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. (This option only applies to an interface configured as an MVR6 receiver.)

4.2.15.8 Show Static Group Member

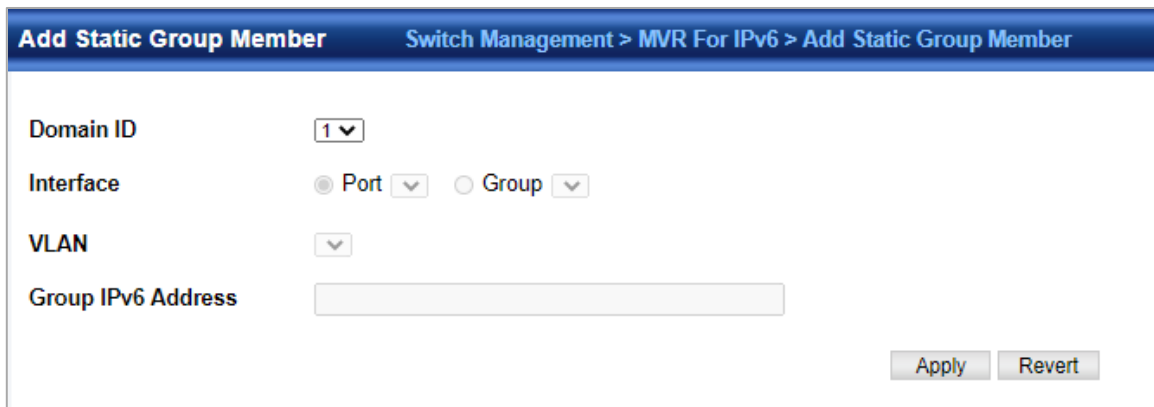
Switch Management > MVR For IPv6> Show Static Group Member page is used to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.



- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Interface** – Port or group identifier.
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Group IPv6 Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR6 group range configured on the Configure General page.

4.2.15.9 Add Static Group Member

Switch Management > MVR For IPv6> Add Static Group Member page is used to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.



- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Interface** – Port or group identifier.
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Group IPv6 Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR6 group range configured on the Configure General page.

4.2.15.10 Show Member

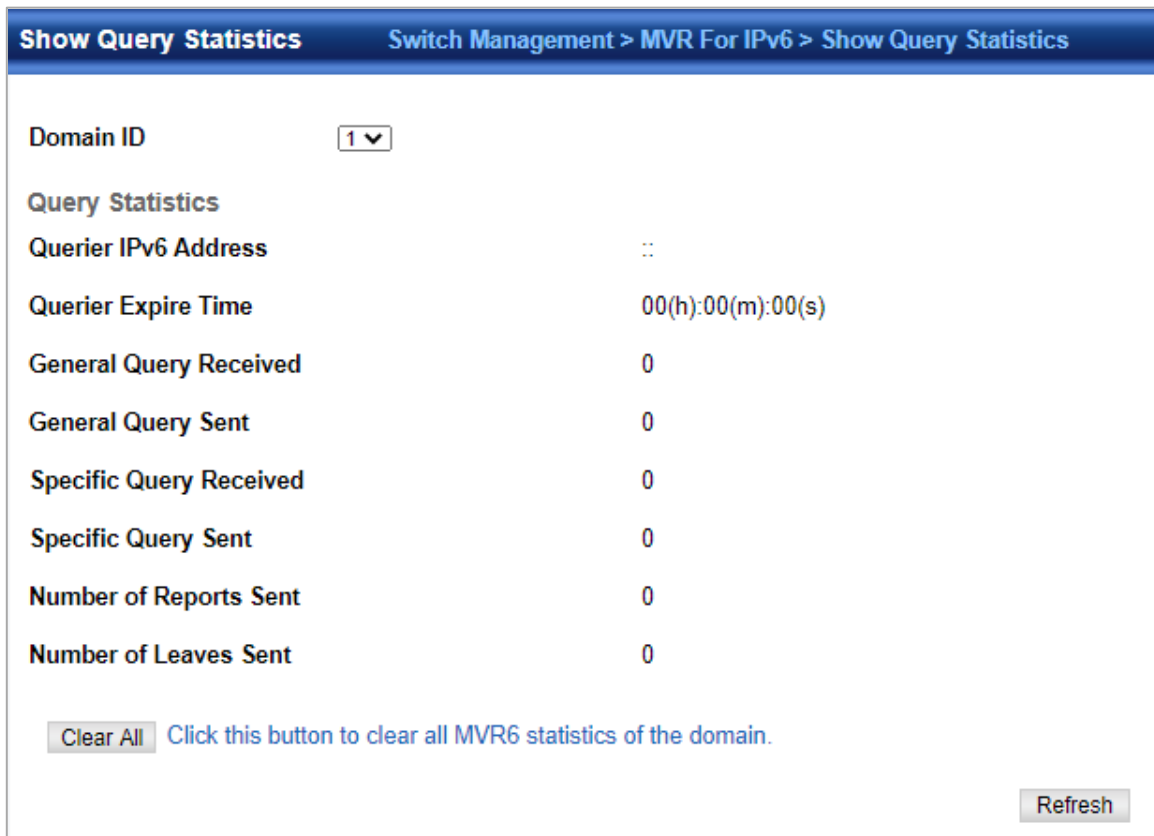
Switch Management > MVR For IPv6>Show Member page is used to show the multicast groups either statically or dynamically assigned to the MVR6 receiver groups on each interface.



- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Group IPv6 Address** – Multicast groups assigned to the MVR6 VLAN.
- ◆ **VLAN** – The VLAN through which the service is received. Note that this may be different from the MVR6 VLAN if the group address has been statically assigned.
- ◆ **Port** – Indicates the source address of the multicast service, or displays an asterisk if the group address has been statically assigned (these entries are marked as “Source”). Also shows the interfaces with subscribers for multicast services provided through the MVR6 VLAN (these entries are marked as “Receiver”).
- ◆ **Up Time** – Time this service has been forwarded to attached clients.
- ◆ **Expire** – Time before this entry expires if no membership report is received from currently active or new clients.
- ◆ **Count** – The number of multicast services currently being forwarded from the MVR6 VLAN.

4.2.15.11 Show Query Statistics

Switch Management > MVR For IPv6>Show Query Statistics page is used to display MVR6protocol-related statistics for the specified interface.



- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-12)
- ◆ **Group** – Group identifier. (Range: 1-12) Query Statistics
- ◆ **Querier IPv6 Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics Input Statistics

- ◆ **Report** – The number of MLD membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR6 group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR6 groups active on this interface.

Output Statistics

- ◆ **Report** – The number of MLD membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

4.2.15.12 Show VLAN Statistics

Switch Management > MVR for IPv6>Show VLAN Statistics page is used to display MVR6protocol-related statistics for the specified interface.

Show VLAN Statistics
Switch Management > MVR For IPv6 > Show VLAN Statistics

Domain ID

VLAN

Input Statistics

Report	0	Drop	0
Done	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		

Output Statistics

Report	0
Done	0
G Query	0
G(-S)-S Query	0

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
 - ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
 - ◆ **Port** – Port identifier. (Range: 1-12)
 - ◆ **Group** – Group identifier. (Range: 1-12) Query Statistics
 - ◆ **Querier IPv6 Address** – The IP address of the querier on this interface.
 - ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
 - ◆ **General Query Received** – The number of general queries received on this interface.
 - ◆ **General Query Sent** – The number of general queries sent from this interface.
 - ◆ **Specific Query Received** – The number of specific queries received on this interface.
 - ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
 - ◆ **Number of Reports Sent** – The number of reports sent from this interface.
 - ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.
- VLAN, Port, and Group Statistics Input Statistics
- ◆ **Report** – The number of MLD membership reports received on this interface.
 - ◆ **Leave** – The number of leave messages received on this interface.
 - ◆ **G Query** – The number of general query messages received on this interface.
 - ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
 - ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR6 group report received.
 - ◆ **Join Success** – The number of times a multicast group was successfully joined.

◆ **Group** – The number of MVR6 groups active on this interface.

Output Statistics

◆ **Report** – The number of MLD membership reports sent from this interface.

◆ **Leave** – The number of leave messages sent from this interface.

◆ **G Query** – The number of general query messages sent from this interface.

◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

4.2.15.13 Show Port Statistics

Switch Management > MVR For IPv6>Show Port Statistics page is used to display MVR6 protocol-related statistics for the specified interface.

Show Port Statistics
Switch Management > MVR For IPv6 > Show Port Statistics

Domain ID 1 ▼

Port 1 ▼

Input Statistics

Report	0	Drop	0
Done	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		

Output Statistics

Report	0
Done	0
G Query	0
G(-S)-S Query	0

Clear
Refresh

◆ **Domain ID** – An independent multicast domain. (Range: 1-5)

◆ **VLAN** – VLAN identifier. (Range: 1-4093)

◆ **Port** – Port identifier. (Range: 1-12)

◆ **Group** – Group identifier. (Range: 1-12)

Query Statistics

◆ **Querier IPv6 Address** – The IP address of the querier on this interface.

◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.

◆ **General Query Received** – The number of general queries received on this interface.

◆ **General Query Sent** – The number of general queries sent from this interface.

◆ **Specific Query Received** – The number of specific queries received on this interface.

◆ **Specific Query Sent** – The number of specific queries sent from this interface.

◆ **Number of Reports Sent** – The number of reports sent from this interface.

◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Group Statistics Input Statistics

◆ **Report** – The number of MLD membership reports received on this interface.

◆ **Leave** – The number of leave messages received on this interface.

◆ **G Query** – The number of general query messages received on this interface.

◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.

◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR6 group report received.

◆ **Join Success** – The number of times a multicast group was successfully joined.

◆ **Group** – The number of MVR6 groups active on this interface. Output Statistics

◆ **Report** – The number of MLD membership reports sent from this interface.

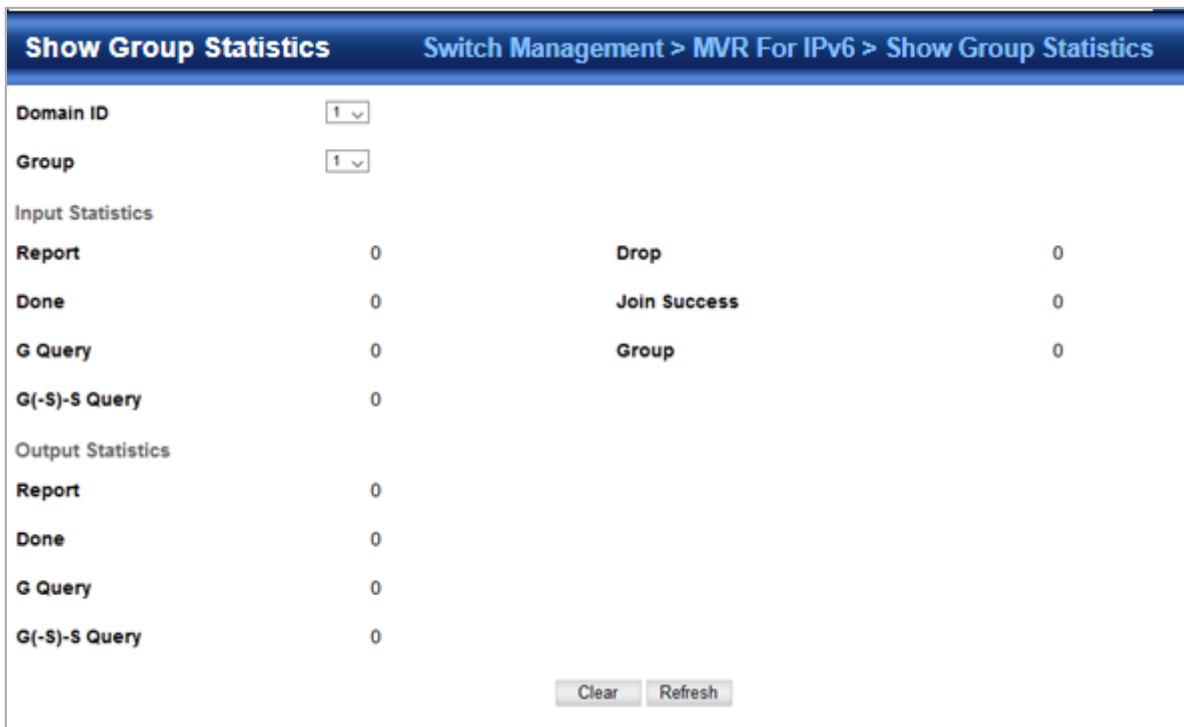
◆ **Leave** – The number of leave messages sent from this interface.

◆ **G Query** – The number of general query messages sent from this interface.

◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

4.2.15.14 Show Group Statistics

Switch Management > MVR For IPv6>Show Trunk Statistics page is used to display MVR6protocol-related statistics for the specified interface.



Input Statistics	
Report	0
Done	0
G Query	0
G(-S)-S Query	0

Output Statistics	
Report	0
Done	0
G Query	0
G(-S)-S Query	0

◆ **Domain ID** – An independent multicast domain. (Range: 1-5)

◆ **VLAN** – VLAN identifier. (Range: 1-4093)

◆ **Port** – Port identifier. (Range: 1-12)

◆ **Group** – Group identifier. (Range: 1-12)

Query Statistics

◆ **Querier IPv6 Address** – The IP address of the querier on this interface.

◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.

◆ **General Query Received** – The number of general queries received on this interface.

◆ **General Query Sent** – The number of general queries sent from this interface.

◆ **Specific Query Received** – The number of specific queries received on this interface.

- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics Input Statistics

- ◆ **Report** – The number of MLD membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR6 group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR6 groups active on this interface.

Output Statistics

- ◆ **Report** – The number of MLD membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

4.2.16 LLDP

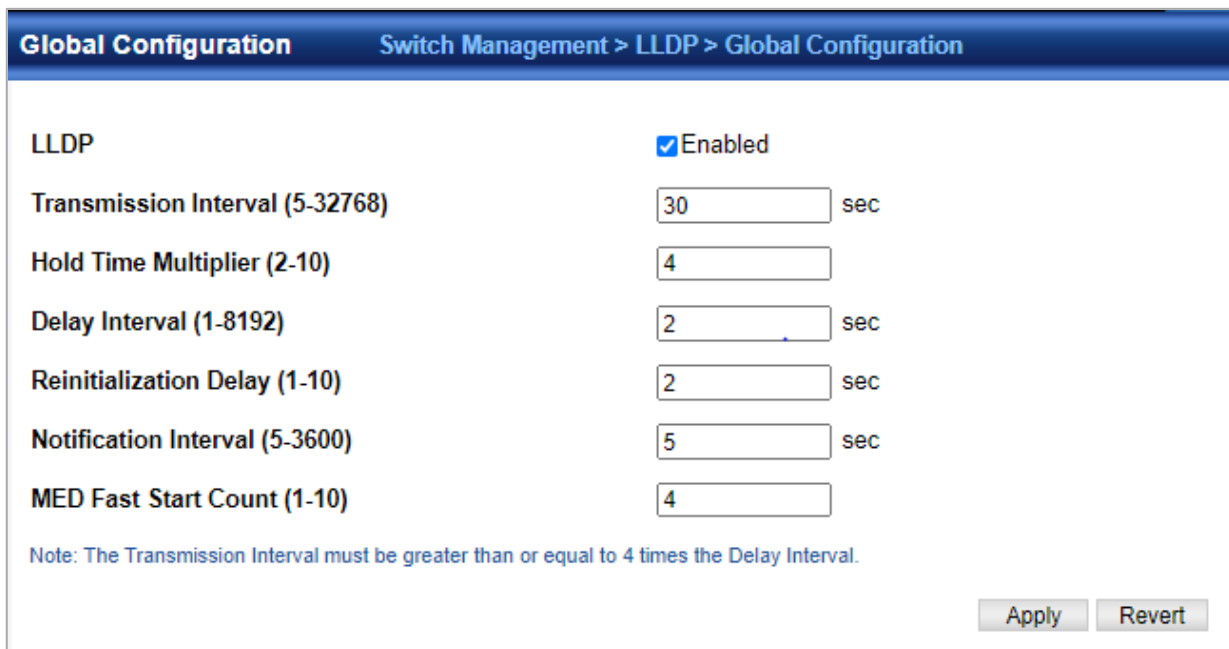
Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in **Type Length Value (TLV)** format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP 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.

4.2.16.1 Global Configuration

Switch Management > LLDP > Global Configuration page is used to set attributes for general functions such as globally enabling LLDP on the switch, setting the message ageout time, and setting the frequency for broadcasting general advertisements or reports about changes in the LLDP MIB.



Global Configuration		Switch Management > LLDP > Global Configuration	
LLDP	<input checked="" type="checkbox"/>	Enabled	
Transmission Interval (5-32768)	<input type="text" value="30"/>	sec	
Hold Time Multiplier (2-10)	<input type="text" value="4"/>		
Delay Interval (1-8192)	<input type="text" value="2"/>	sec	
Reinitialization Delay (1-10)	<input type="text" value="2"/>	sec	
Notification Interval (5-3600)	<input type="text" value="5"/>	sec	
MED Fast Start Count (1-10)	<input type="text" value="4"/>		
Note: The Transmission Interval must be greater than or equal to 4 times the Delay Interval.			
		<input type="button" value="Apply"/>	<input type="button" value="Revert"/>

- ◆ **LLDP** – Enables LLDP globally on the switch. (Default: Enabled)
- ◆ **Transmission Interval** – Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)
- ◆ **Hold Time Multiplier** – Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4) The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner. TTL in seconds is based on the following rule: minimum value ((Transmission Interval * Holdtime Multiplier), or 65535) Therefore, the default TTL is $4 * 30 = 120$ seconds.
- ◆ **Delay Interval** – Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (Range: 1-8192 seconds; Default: 2 seconds) The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission. This attribute must comply with the rule: $(4 * \text{Delay Interval}) \leq \text{Transmission Interval}$

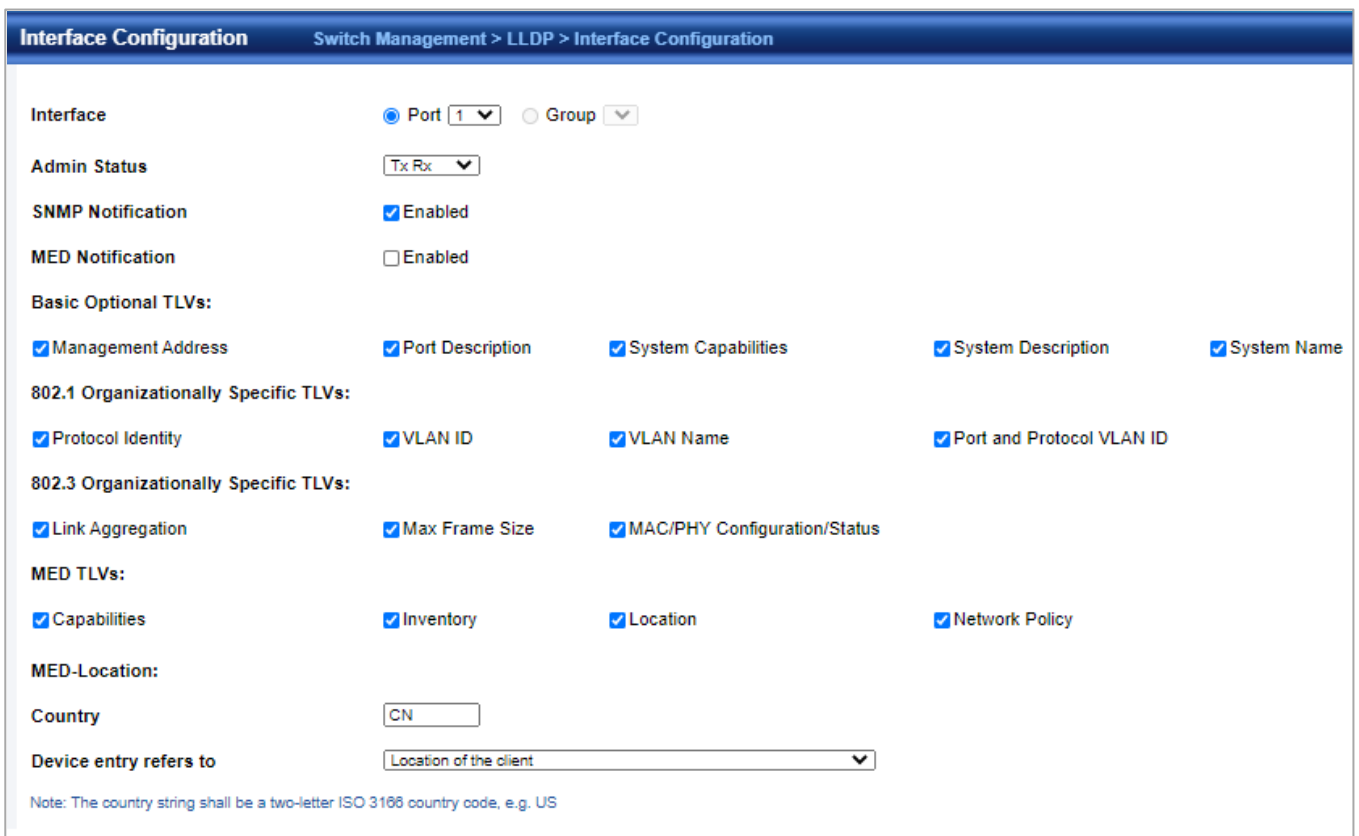
◆ **Reinitialization Delay** – Configures the delay before attempting to reinitialize after LLDP ports are disabled or the link goes down. (Range: 1-10 seconds; Default: 2 seconds) When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

◆ **Notification Interval** – Configures the allowed interval for sending SNMP notifications about LLDP MIB changes. (Range: 5-3600 seconds; Default: 5 seconds) This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management. Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

◆ **MED Fast Start Count** – Configures the amount of LLDP MED Fast Start LLDPDUs to transmit during the activation process of the LLDPMED Fast Start mechanism. (Range: 1-10 packets; Default: 4 packets) The MED Fast Start Count parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDPMED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

4.2.16.2 Interface Configuration

Switch Management > LLDP>Interface Configuration page is used to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received, whether SNMP notifications are sent, and the type of information advertised.



◆ **Admin Status** – Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Tx only, Rx only, TxRx, Disabled; Default: TxRx)

◆ **SNMP Notification** – Enables the transmission of SNMP trap notifications about LLDP and LLDP-MED changes. (Default: Disabled) This option sends out SNMP trap notifications to designated target stations at the interval specified by the Notification Interval in the preceding section. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/ TIA-1057), or vendor-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs. For information on defining SNMP trap destinations, Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the

transmission. An SNMP agent should therefore periodically check the value of `IldpStatsRemTableLastChangeTime` to detect any `IldpRemTablesChange` notification-events missed due to throttling or transmission loss.

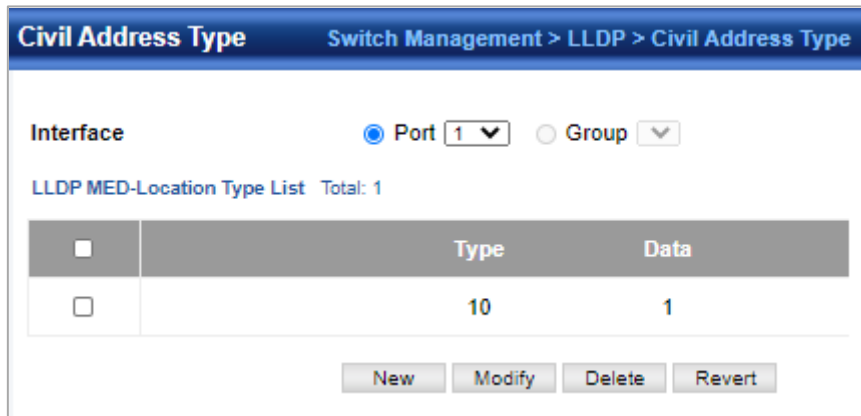
- ◆ **MED Notification** – Enables the transmission of SNMP trap notifications about LLDP-MED changes. (Default: Disabled)
- ◆ **Basic Optional TLVs** – Configures basic information included in the TLV field of advertised messages.
 - **Management Address** – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications in the performance of network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB. Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV. Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.
 - **Port Description** – The port description is taken from the `ifDescr` object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.
 - **System Capabilities** – The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.
 - **System Description** – The system description is taken from the `sysDescr` object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.
 - **System Name** – The system name is taken from the `sysName` object in RFC 3418, which contains the system's administratively assigned name. To configure the system name.
- ◆ **802.1 Organizationally Specific TLVs** – Configures IEEE 802.1 information included in the TLV field of advertised messages.
 - **Protocol Identity** – The protocols that are accessible through this interface.
 - **VLAN ID** – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated.
 - **VLAN Name** – The name of all VLANs to which this interface has been assigned.
 - **Port and Protocol VLAN ID** – The port-based protocol VLANs configured on this interface.
- ◆ **802.3 Organizationally Specific TLVs** – Configures IEEE 802.3 information included in the TLV field of advertised messages.
 - **Link Aggregation** – The link aggregation capabilities, aggregation status of the link, and the IEEE 802.3 aggregated port identifier if this interface is currently a link aggregation member.
 - **Max Frame Size** – The maximum frame size.
 - **MAC/PHY Configuration/Status** – The MAC/PHY configuration and status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.
- ◆ **MED TLVs** – Configures general information included in the MED TLV field of advertised messages.
 - **Capabilities** – This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.
 - **Inventory** – This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.
 - **Location** – This option advertises location identification details.
 - **Network Policy** – This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption.

◆ **MED-Location Civic Address** – Configures information for the location of the attached device included in the MED TLV field of advertised messages, including the country and the device type.

- **Country** – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)
- **Device entry refers to** – The type of device to which the location applies:
 - Location of DHCP server.
 - Location of network element closest to client.
 - Location of client. (This is the default.)

4.2.16.3 Civil Address Type

Switch Management > LLDP > Civil Address Type page is used to specify the physical location of the device attached to an interface.



Civil Address Type Switch Management > LLDP > Civil Address Type

Interface Port 1 Group ▼

LLDP MED-Location Type List Total: 1

	Type	Data
<input type="checkbox"/>	10	1

◆ **CA-Type** – Descriptor of the data civic address value. (Range: 0-255)

◆ **CA-Value** – Description of a location. (Range: 1-32 characters)

4.2.16.4 Local Information

Switch Management > LLDP > Local Information page is used to display information about the switch, such as its MAC address, chassis ID, management IP address, and port information.

Local Information
Switch Management > LLDP > Local Information

General
 Port
 Group

LLDP Local Device Information

Chassis Type	MAC Address
Chassis ID	A8-F7-E0-11-68-34
System Name	SGS-5240-24T4X
System Description	SGS-5240-24T4X
System Capabilities Supported	Bridge, Router
System Capabilities Enabled	Bridge, Router
Management Address	192.168.0.100 (IPv4)

◆ **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.

ID Basis	Reference
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Interface alias	IfAlias (IETF RFC 2863)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Locally assigned	locally assigned

◆ **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.

◆ **System Name** – A string that indicates the system's administratively assigned name.

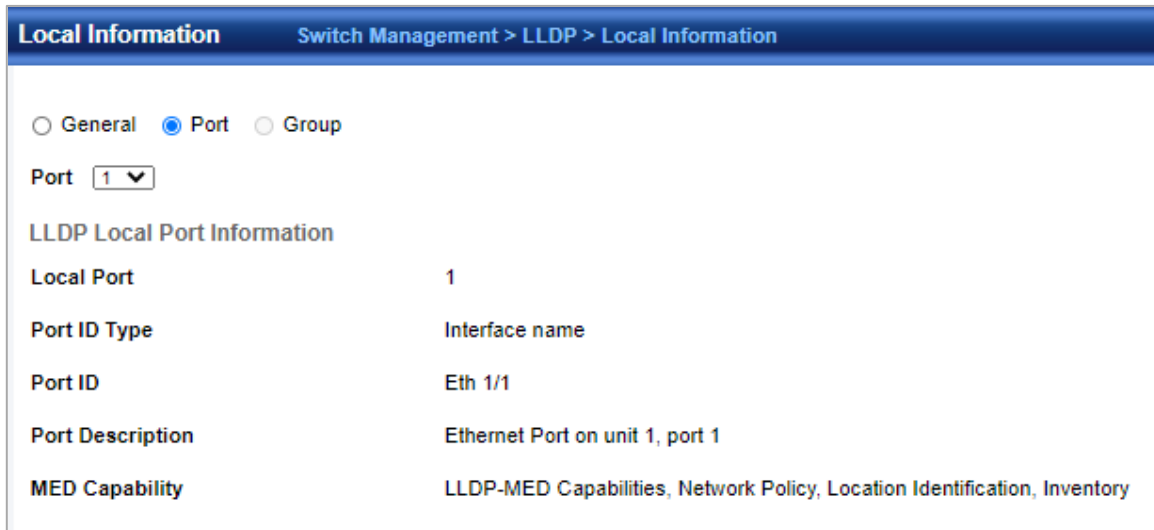
◆ **System Description** – A textual description of the network entity. This field is also displayed by the **show system** command.

◆ **System Capabilities Supported** – The capabilities that define the primary function(s) of the system.

ID Basis	Reference
Other	—
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011
DOCSIS cable device	IETF RFC 2669 and IETF RFC 2670
End Station Only	IETF RFC 2011

◆ **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. Refer to the preceding table.

◆ **Management Address** – The management address associated with the local system. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. Interface Settings. The attributes listed below apply to both port and trunk interface types. When a trunk is listed, the descriptions apply to the first port of the trunk.



The screenshot shows the 'Local Information' page in the switch management interface. The breadcrumb path is 'Switch Management > LLDP > Local Information'. There are three radio buttons: 'General' (unselected), 'Port' (selected), and 'Group' (unselected). Below this is a 'Port' dropdown menu set to '1'. The main content area is titled 'LLDP Local Port Information' and contains the following details:

Local Port	1
Port ID Type	Interface name
Port ID	Eth 1/1
Port Description	Ethernet Port on unit 1, port 1
MED Capability	LLDP-MED Capabilities, Network Policy, Location Identification, Inventory

◆ **Port/Group ID** – A string that contains the specific identifier for the port or trunk from which this LLDPDU was transmitted.

4.2.16.5 Peer Information

Switch Management > LLDP > Peer Information page is used to display information about devices connected directly to the switch's ports which are advertising information through LLDP, or to display detailed information about an LLDP-enabled device connected to a specific port on the local switch.

■ Port's peer brief

Peer Information Switch Management > LLDP > Peer Information

Port's peer brief
 Port's peer Info
 Group's peer Brief
 Group's peer Info

LLDP Remote Device Port List Total: 1

Local Port	Chassis ID	Port ID
Eth 1/22	A8-F7-E0-0C-36-4D	gi26

- ◆ **Local Port** – The local port to which a remote LLDP-capable device is attached.
- ◆ **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- ◆ **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- ◆ **System Name** – A string that indicates the system's administratively assigned name. Port Details

■ Port's peer info

Peer Information
Switch Management > LLDP > Peer Information

Port's peer brief
 Port's peer Info
 Group's peer Brief
 Group's peer Info

Port 22

Remote Index 1

Port's peer Information

Local Port	22
Chassis Type	MAC Address
Chassis ID	A8-F7-E0-0C-36-4D
Port Type	Locally Assigned
Port ID	gi26
Port Description	
System Name	GS-4210-24T2S
System Description	PLANET, GS-4210-24T2S, L2/L4 Managed Switch, v1.305b200904
System Capabilities Supported	Bridge
System Capabilities Enabled	Bridge

Management Address List Total: 2

Address	Address Type
192.168.137.194	IPv4 Address
FE-80-00-00-00-00	IPv6 Address

LLDP-MED Capability

Device Class	Network Connectivity
Supported Capabilities	LLDP-MED Capabilities, Network Policy
Current Capabilities	LLDP-MED Capabilities

- ◆ **Port** – Port identifier on local switch.
- ◆ **Remote Index** – Index of remote device attached to this port.
- ◆ **Local Port** – The local port to which a remote LLDP-capable device is attached.
- ◆ **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.
- ◆ **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- ◆ **System Name** – A string that indicates the system's assigned name.
- ◆ **System Description** – A textual description of the network entity.
- ◆ **Port Type** – Indicates the basis for the identifier that is listed in the Port ID field.

ID Basis	Reference
Interface alias	IfAlias (IETF RFC 2863)
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Agent circuit ID	agent circuit ID (IETF RFC 3046)
Locally assigned	locally assigned

◆ **Port Description** – A string that indicates the port's description. If RFC 2863 is implemented, the ifDescr object should be used for this field.

◆ **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.

◆ **System Capabilities Supported** – The capabilities that define the primary function(s) of the system.

◆ **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled.

◆ **Management Address List** – The management addresses for this device. Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. Port Details – 802.1 Extension Information

◆ **Remote Port VID** – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated.

◆ **Remote Port-Protocol VLAN List** – The port-based protocol VLANs configured on this interface, whether the given port (associated with the remote system) supports port-based protocol VLANs, and whether the port-based protocol VLANs are enabled on the given port associated with the remote system.

◆ **Remote VLAN Name List** – VLAN names associated with a port.

◆ **Remote Protocol Identity List** – Information about particular protocols that are accessible through a port. This object represents an arbitrary local integer value used by this agent to identify a particular protocol identity, and an octet string used to identify the protocols associated with a port of the remote system. Port Details – 802.3 Extension Port Information

◆ **Remote Port Auto-Neg Supported** – Shows whether the given port (associated with remote system) supports auto-negotiation.

◆ **Remote Port Auto-Neg Adv-Capability** – The value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) which is associated with a port on the remote system.

Bit	Capability
0	other or unknown
1	10BASE-T half duplex mode
2	10BASE-T full duplex mode
3	100BASE-T4
4	100BASE-TX half duplex mode
5	100BASE-TX full duplex mode
6	100BASE-T2 half duplex mode
7	100BASE-T2 full duplex mode
8	PAUSE for full-duplex links
9	Asymmetric PAUSE for full-duplex links
10	Symmetric PAUSE for full-duplex links
11	Asymmetric and Symmetric PAUSE for full-duplex links
12	1000BASE-X, -LX, -SX, -CX half duplex mode
13	1000BASE-X, -LX, -SX, -CX full duplex mode
14	1000BASE-T half duplex mode
15	1000BASE-T full duplex mode

◆ **Remote Port Auto-Neg Status** – Shows whether port auto negotiation is enabled on a port associated with the remote system.

◆ **Remote Port MAU Type** – An integer value that indicates the operational MAU type of the sending device. This object contains the integer value derived from the list position of the corresponding dot3MauType as listed in IETF RFC 3636 and is equal to the last number in the respective dot3MauType OID. Port Details – 802.3 Extension Power Information

◆ **Remote Power Class** – The port Class of the given port associated with the remote system (PSE – Power Sourcing Equipment or PD – Powered Device).

◆ **Remote Power MDI Status** – Shows whether MDI power is enabled on the given port associated with the remote system.

◆ **Remote Power Pairs** – “Signal” means that the signal pairs only are in use, and “Spare” means that the spare pairs only are in use.

◆ **Remote Power MDI Supported** – Shows whether MDI power is supported on the given port associated with the remote system.

◆ **Remote Power Pair Controllable** – Indicates whether the pair selection can be controlled for sourcing power on the given port associated with the remote system.

◆ **Remote Power Classification** – This classification is used to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points and others, will be classified according to their power requirements. Port Details – 802.3 Extension Trunk Information

◆ **Remote Link Aggregation Capable** – Shows if the remote port is not in link aggregation state and/or it does not support link aggregation.

◆ **Remote Link Aggregation Status** – The current aggregation status of the link.

◆ **Remote Link Port ID** – This object contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component associated with the remote system. If the remote port is not in link aggregation state and/or it does not support link aggregation, this value should be zero. Port Details – 802.3 Extension Frame Information

◆ **Remote Max Frame Size** – An integer value indicating the maximum supported frame size in octets on the port component associated with the remote system. Port Details – LLDP-MED Capability 8

◆ **Device Class** – Any of the following categories of endpoint devices:

- Class 1 – The most basic class of endpoint devices.
- Class 2 – Endpoint devices that supports media stream capabilities.
- Class 3 – Endpoint devices that directly supports end users of the IP communication systems.
- Network Connectivity Device – Devices that provide access to the IEEE 802 based LAN infrastructure for LLDP-MED endpoint devices. These may be any LAN access device including LAN switch/router, IEEE 802.1 bridge, IEEE 802.3 repeater, IEEE 802.11 wireless access point, or any device that supports the IEEE 802.1AB and MED extensions defined by this Standard and can relay IEEE 802 frames via any method.

◆ **Supported Capabilities** – The supported set of capabilities that define the primary function(s) of the port:

- LLDP-MED Capabilities
- Network Policy
- Location Identification
- Extended Power via MDI – PSE
- Extended Power via MDI – PD
- Inventory

◆ **Current Capabilities** – The set of capabilities that define the primary function(s) of the port which are currently enabled. Port Details – Network Policies

◆ **Application Type** – The primary application(s) defined for this network policy:

- Voice
- Voice Signaling
- Guest Signaling
- Guest Voice Signaling
- Softphone Voice
- Video Conferencing
- Streaming Video
- Video Signaling

◆ **Tagged Flag** – Indicates whether the specified application type is using a tagged or untagged VLAN.

◆ **Layer 2 Priority** – The Layer 2 priority to be used for the specified application type. This field may specify one of eight priority levels (0-7), where a value of 0 represents use of the default priority.

◆ **Unknown Policy Flag** – Indicates that an endpoint device wants to explicitly advertise that this policy is required by the device, but is currently unknown.

◆ **VLAN ID** – The VLAN identifier (VID) for the port as defined in IEEE 802.1Q. A value of zero indicates that the port is using priority tagged frames, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

◆ **DSCP Value** – The DSCP value to be used to provide Diffserv node behavior for the specified application type. This field may contain one of 64 code point values (0-63). A value of 0 represents use of the default DSCP value as defined in RFC 2475. Port Details – Location Identifications

◆ **Location Data Format** – Any of these location ID data formats:

- Coordinate-based LCI₉ – Defined in RFC 3825, includes latitude resolution, latitude, longitude resolution, longitude, altitude type, altitude resolution, altitude, and datum.
- Civic Address LCI₉ – Includes What, Country code, CA type, CA length and CA value.
- ECS ELIN – Emergency Call Service Emergency Location Identification Number supports traditional PSAP-based Emergency Call Service in North America.

◆ **Country Code** – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)

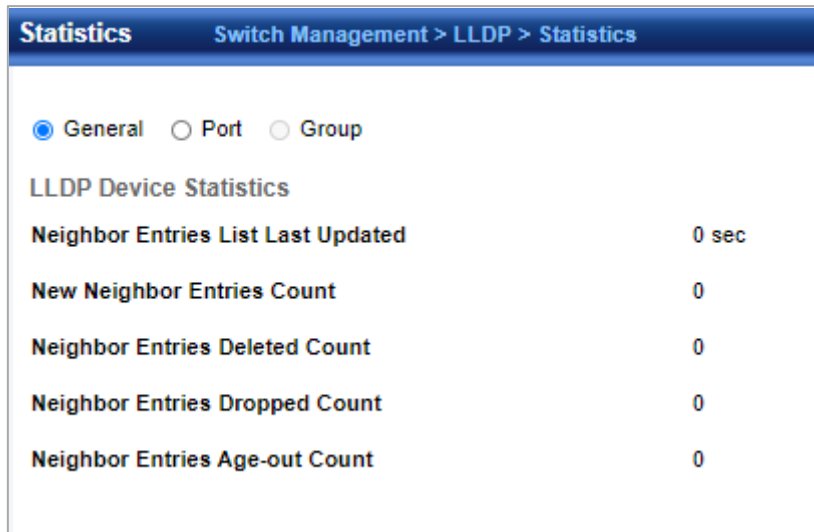
◆ **What** – The type of device to which the location applies as described for the field entry. Port Details – Inventory

◆ **Hardware Revision** – The hardware revision of the end-point device.

- ◆ **Software Revision** – The software revision of the end-point device.
- ◆ **Manufacture Name** – The manufacturer of the end-point device
- ◆ **Asset ID** – The asset identifier of the end-point device. End-point devices are typically assigned asset identifiers to facilitate inventory management and assets tracking.
- ◆ **Firmware Revision** – The firmware revision of the end-point device.
- ◆ **Serial Number** – The serial number of the end-point device.
- ◆ **Model Name** – The model name of the end-point device.
- ◆ **Asset ID** – The asset identifier of the end-point device.

4.2.16.6 Statistics

Switch Management > LLDP > Show Statistics page is used to display statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces.



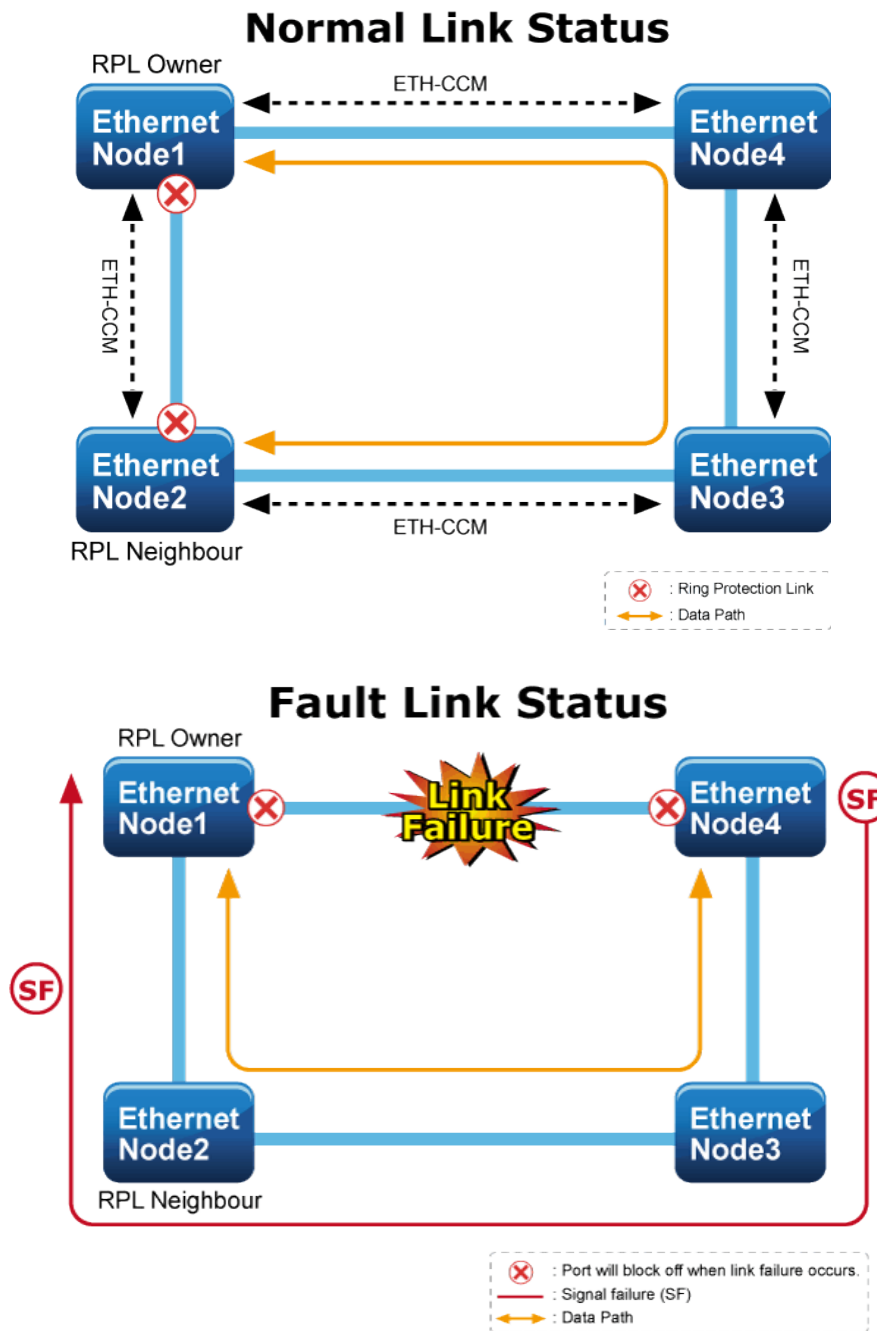
LLDP Device Statistics	
Neighbor Entries List Last Updated	0 sec
New Neighbor Entries Count	0
Neighbor Entries Deleted Count	0
Neighbor Entries Dropped Count	0
Neighbor Entries Age-out Count	0

- ◆ **Neighbor Entries List Last Updated** – The time the LLDP neighbor entry list was last updated.
- ◆ **New Neighbor Entries Count** – The number of LLDP neighbors for which the remote TTL has not yet expired.
- ◆ **Neighbor Entries Deleted Count** – The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.
- ◆ **Neighbor Entries Dropped Count** – The number of times which the remote database on this switch dropped an LLDPDU because of insufficient resources.
- ◆ **Neighbor Entries Age-out Count** – The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired. Port/Trunk
- ◆ **Frames Discarded** – Number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular TLV.
- ◆ **Frames Invalid** – A count of all LLDPDUs received with one or more detectable errors.
- ◆ **Frames Received** – Number of LLDP PDUs received.
- ◆ **Frames Sent** – Number of LLDP PDUs transmitted.
- ◆ **TLVs Unrecognized** – A count of all TLVs not recognized by the receiving LLDP local agent.
- ◆ **TLVs Discarded** – A count of all LLDPDUs received and then discarded due to insufficient memory space, missing or out-of-sequence attributes, or any other reason.
- ◆ **Neighbor Ageouts** – A count of the times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

4.2.17 ERPS

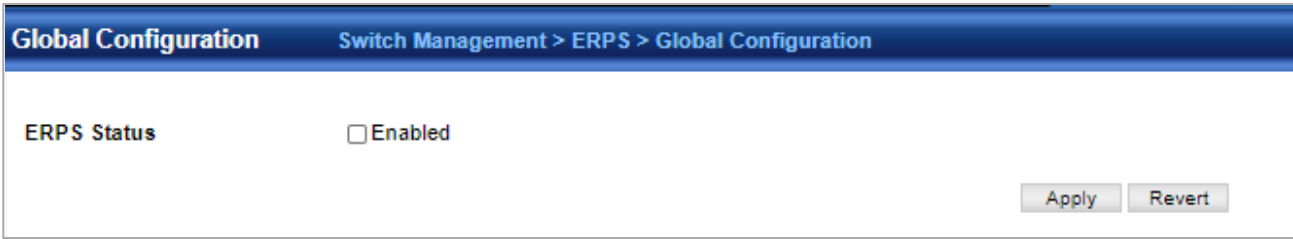
ITU-T G.8032 **Ethernet Ring protection switching (ERPS)** is a link layer protocol applied on Ethernet loop protection to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology.

ERPS provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the Ring topology, every switch should be enabled with Ring function and two ports should be assigned as the member ports in the ERPS. Only one switch in the Ring group would be set as the RPL owner switch that one port would be blocked, called **owner port**, and PRL neighbor switch has one port that one port would be blocked, called **neighbor port** that connect to owner port directly and this link is called the **Ring Protection Link** or **RPL**. Each switch will send ETH-CCM message to check the link status in the ring group. When the failure of network connection occurs, the nodes block the failed link and report the signal failure message, the RPL owner switch will automatically unblocks the PRL to recover from the failure.



4.2.17.1 Global Configuration

Switch Management > ERPS > Global Configuration page is used to globally enable or disable ERPS on the switch.



Global Configuration Switch Management > ERPS > Global Configuration

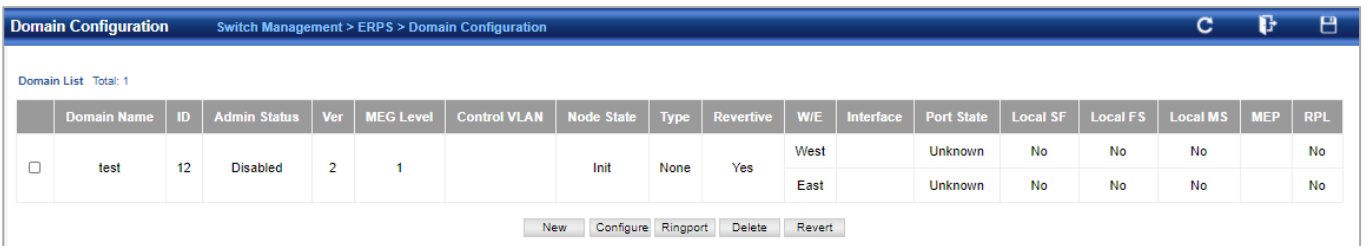
ERPS Status Enabled

Apply Revert

◆ **ERPS Status** – Enables ERPS on the switch. (Default: Disabled) ERPS must be enabled globally on the switch before it can be enabled on an ERPS ring.

4.2.17.2 Domain Configuration

Switch Management > ERPS > Domain Configuration pages is used to add ERPS domain and configure domain details.

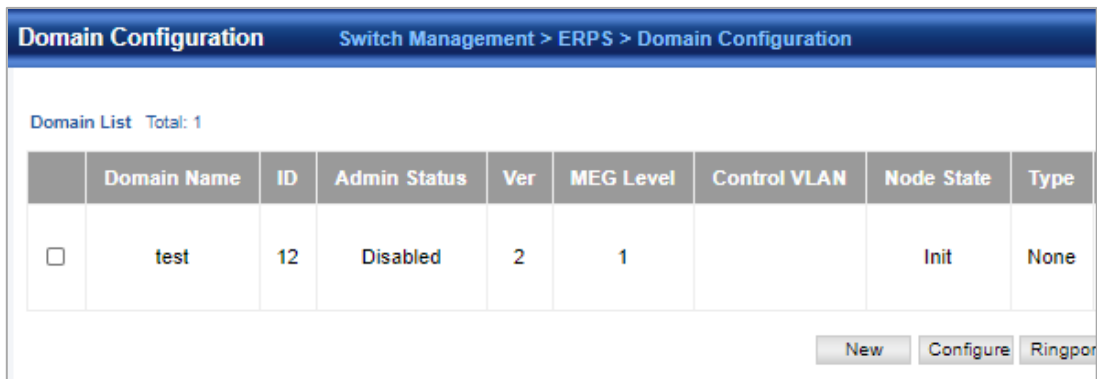


Domain Configuration Switch Management > ERPS > Domain Configuration

Domain List Total: 1

	Domain Name	ID	Admin Status	Ver	MEG Level	Control VLAN	Node State	Type	Revertive	W/E	Interface	Port State	Local SF	Local FS	Local MS	MEP	RPL
<input type="checkbox"/>	test	12	Disabled	2	1		Init	None	Yes	West		Unknown	No	No	No		No
										East		Unknown	No	No	No		No

New Configure Ringport Delete Revert

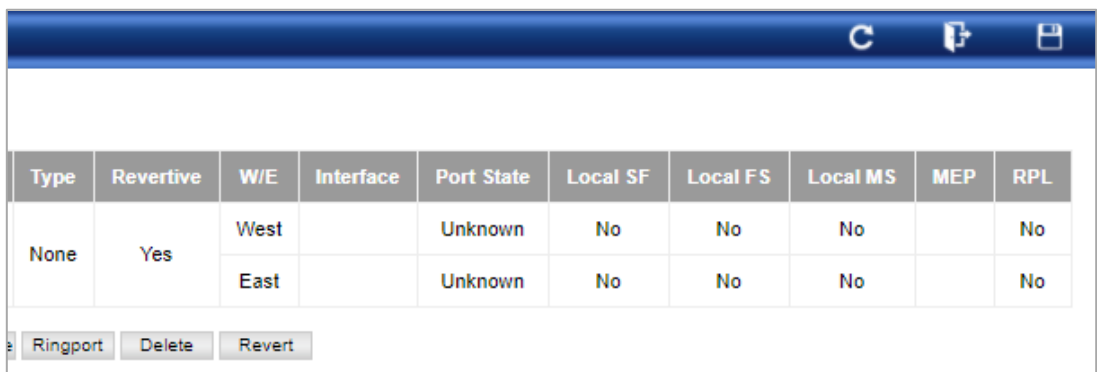


Domain Configuration Switch Management > ERPS > Domain Configuration

Domain List Total: 1

	Domain Name	ID	Admin Status	Ver	MEG Level	Control VLAN	Node State	Type
<input type="checkbox"/>	test	12	Disabled	2	1		Init	None

New Configure Ringport



Domain Configuration Switch Management > ERPS > Domain Configuration

Type	Revertive	W/E	Interface	Port State	Local SF	Local FS	Local MS	MEP	RPL
None	Yes	West		Unknown	No	No	No		No
		East		Unknown	No	No	No		No

Ringport Delete Revert

Domain Name	<input type="text" value="test"/>	Domain ID	12
Admin Status	<input type="checkbox"/> Enabled	R-APS with VC	<input checked="" type="checkbox"/> Enabled
Version	<input type="text" value="2"/>	R-APS Def MAC	<input checked="" type="checkbox"/> Enabled
MEG Level (0-7)	<input type="text" value="1"/>	Propagate TC	<input type="checkbox"/> Enabled
Control VLAN	<input type="checkbox"/> <input type="text" value="1"/>		
Node State	Init	Non-ERPS Dev Protect	<input type="checkbox"/> Enabled
Holdoff Timer (0-10000)	<input type="text" value="0"/> ms	Guard Timer (10-2000)	<input type="text" value="500"/> ms
WTB Timer	5500 ms		
WTR Timer (5-12)	<input type="text" value="5"/> min	Node Type	<input type="text" value="None"/>
WTB Expire		Revertive	<input checked="" type="checkbox"/> Enabled
WTR Expire		Major Domain	<input type="checkbox"/> <input type="text"/>
Node ID	<input type="text" value="64-9D-99-11-88-34"/> (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxxxx)		
West	<input type="checkbox"/> Enabled	East	<input type="checkbox"/> Enabled
Interface	<input type="text"/>	Interface	<input type="text"/>
Port State	Unknown	Port State	Unknown
Local SF	No	Local SF	No
Local FS	No	Local FS	No
Local MS	No	Local MS	No
MEP (1-8191)	<input type="checkbox"/> <input type="text"/>	MEP (1-8191)	<input type="checkbox"/> <input type="text"/>
RPL	No	RPL	No

Note Please disable STP of the ports before configure EAST/WEST ports.

◆ **Domain Name** – Name of a configured ERPS ring.

◆ **Node State** – Shows the following ERPS states:

- Init – The ERPS ring has started but has not yet determined the status of the ring.
- Idle – If all nodes in a ring are in this state, it means that all the links in the ring are up. This state will switch to protection state if a link failure occurs.
- Protection – If a node in this state, it means that a link failure has occurred. This state will switch to idle state if all the failed links recover.

◆ **MEG Level** – The maintenance entity group (MEG) level providing a communication channel for ring automatic protection switching (R-APS) information.

◆ **Admin Status** – Shows whether ERPS is enabled on the switch.

◆ **West Port** – Shows the west ring port for this node.

◆ **East Port** – Shows the east ring port for this node.

◆ **RPL Owner** – Shows if this node is the RPL owner.

◆ **Control VLAN** – Shows the Control VLAN ID.

◆ **Non ERPS Device Protection** – Shows if non-standard health-check packets are sent when in protection state. Configure Details

◆ **Domain Name** – Name of a configured ERPS ring.

◆ **Admin Status** – Activates the current ERPS ring.

Before enabling a ring, the global ERPS function should be enabled, the east and west ring ports configured on each node, the RPL owner specified, and the controlVLAN configured. Once enabled, the RPL owner node and non-owner node state machines will start, and the ring will enter idle state if no signal failures are detected.

◆ **MEG Level** – The maintenance entity group (MEG) level which provides a communication channel for ring automatic protection switching (R-APS) information. (Range: 0-7) This parameter is used to ensure that received R-APS PDUs are directed for this ring. A unique level should be configured for each local ring if there are many R-APS PDUs passing through this switch.

◆ **Node ID** – A MAC address unique to the ring node. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

◆ **Node State** – Refer to the parameters for the Show page.

◆ **West Port** – Connects to next ring node to the west. Each node must be connected to two neighbors on the ring. For convenience, the ports connected are referred to as east and west ports. Alternatively, the closest neighbor to the east should be the next node in the ring in a clockwise direction, and the closest neighbor to the west should be the next node in the ring in a counter-clockwise direction. Note that a ring port cannot be configured as a member of a spanning tree, a dynamic trunk, or a static trunk. Once configured, this field shows the ring port for this node, and the interface state:

- Blocking – The transmission and reception of traffic is blocked and the forwarding of R-APS messages is blocked, but the transmission of locally generated R-APS messages is allowed and the reception of all R-APS messages is allowed.
- Forwarding – The transmission and reception of traffic is allowed; transmission, reception and forwarding of R-APS messages is allowed.
- Down – The interface is not linked up.
- Unknown – The interface is not in a known state.

◆ **East Port** – Connects to next ring node to the east.

◆ **RPL Port** – If node is connected to the RPL, this shows by which interface.

◆ **RPL Owner** – Configures a ring node to be the Ring Protection Link (RPL) owner.

◆ **Holdoff Timer** – The hold-off timer is used to filter out intermittent link faults. Faults will only be reported to the ring protection mechanism if this timer expires. (Range: 0-10000 milliseconds, in steps of 100 milliseconds) In order to coordinate timing of protection switches at multiple layers, a hold-off timer may be required. Its purpose is to allow, for example, a server layer protection switch to have a chance to fix the problem before switching at a client layer. When a new defect or more severe defect occurs (new Signal Failure), this event will not be reported immediately to the protection switching mechanism if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the timer expires, whether a defect still exists or not, the timer will be checked. If one does exist, that defect will be reported to the protection switching mechanism. The reported defect need not be the same one that started the timer.

◆ **Guard Timer** – The guard timer is used to prevent ring nodes from receiving outdated R-APS messages. During the duration of the guard timer, all received R-APS messages are ignored by the ring protection control process, giving time for old messages still circulating on the ring to expire. (Range: 10-2000 milliseconds, in steps of 10 milliseconds) The guard timer duration should be greater than the maximum expected forwarding delay for an R-APS message to pass around the ring. A side-effect of the guard timer is that during its duration, a node will be unaware of new or existing ring requests transmitted from other nodes.

◆ **WTR Timer** – The wait-to-restore timer is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. (Range: 5-12 minutes) If the switch goes into ring protection state due to a signal failure, after the failure condition is cleared, the RPL owner will start the wait-to-restore timer and wait until it expires to verify that the ring has stabilized before blocking the RPL and returning to the Idle (normal operating) state.

◆ **Control VLAN** – A dedicated VLAN used for sending and receiving E-APS protocol messages. (Range: 1-4093) Configure one control VLAN for each ERPS ring. First create the VLAN to be used as the control VLAN, add the ring ports for the east and west interface as tagged members to this VLAN, and then use this parameter to add it to the ring. The following restrictions are recommended to avoid creating a loop in the network or other problems which may occur under some situations:

- The Control VLAN must not be configured as a Layer 3 interface (with an IP address), a dynamic VLAN (with GVRP enabled), nor as a private VLAN.
- In addition, only ring ports may be added to the Control VLAN. No other ports can be members of this VLAN.

- Also, the ring ports of the Control VLAN must be tagged. Once the ring has been activated, the configuration of the control VLAN cannot be modified. Use the Admin Status parameter to stop the ERPS ring before making any configuration changes to the control VLAN.

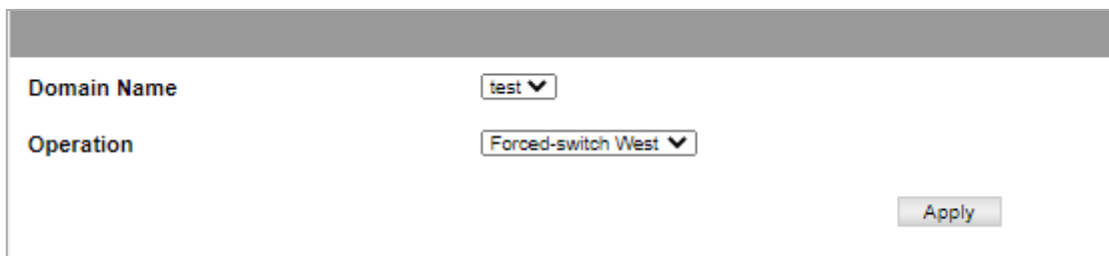
◆ **Propagate TC** – Enables propagation of topology change messages from a secondary ring to the primary ring. (Default: Disabled) When a secondary ring detects a topology change, it can pass a message about this event to the major ring. When the major ring receives this kind of message from a secondary ring, it can clear the MAC addresses on its ring ports to help the secondary ring restore its connections more quickly through protection switching. When the MAC addresses are cleared, data traffic may flood onto the major ring. The data traffic will become stable after the MAC addresses are learned again. The major ring will not be broken, but the bandwidth of data traffic on the major ring may suffer for a short period of time due to this flooding behavior.

◆ **Sub Domain** – A secondary ERPS ring which uses this primary ring for sending control packets.

◆ **Major Domain** – The ERPS ring used for sending control packets. This switch can support up to two rings. However, ERPS control packets can only be sent on one ring. This parameter is used to indicate that the current ring is a secondary ring, and to specify the major ring which will be used to send ERPS control packets. The Ring Protection Link (RPL) is always the west port. So the physical port on a secondary ring must be the west port. In other words, if a domain has two physical ring ports, this ring can only be a major ring, not a secondary ring (or sub-domain) which can have only one physical ring port. The major domain therefore cannot be set if the east port is already configured.

◆ **Non-ERPS Device Protection** – Sends non-standard health-check packets when an owner node enters protection state without any link down event having been detected through Signal Fault messages. (Default: Disabled)

Press Ringport button to configure force or manual mode on ring ports.



The screenshot shows a configuration interface with a grey header bar. Below it, there are two rows of configuration options. The first row is labeled "Domain Name" and has a dropdown menu with "test" selected. The second row is labeled "Operation" and has a dropdown menu with "Forced-switch West" selected. In the bottom right corner of the form, there is a grey "Apply" button.

4.2.17.3 Statistics

Switch Management > ERPS > Statistics pages is used to display or clear statistics information on ring ports.

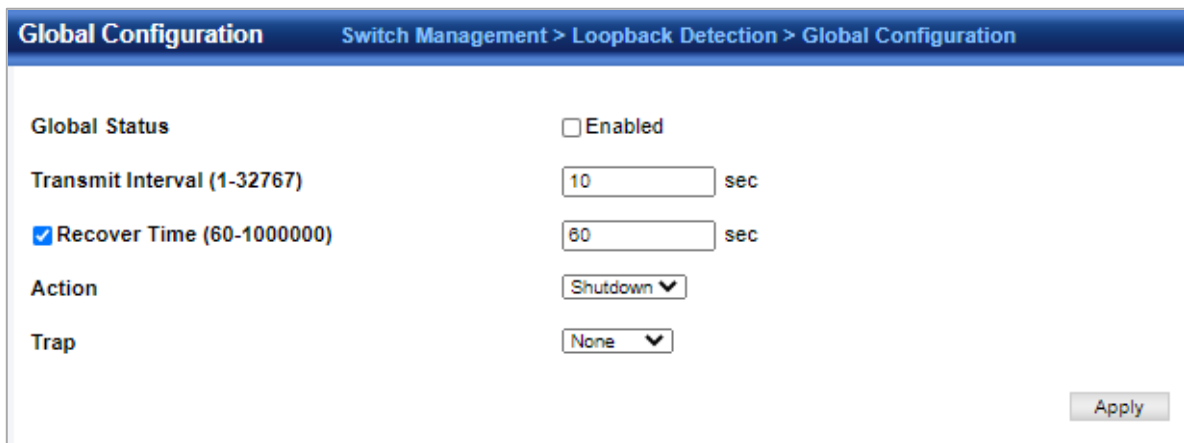
Statistics			
Switch Management > ERPS > Statistics			
Domain Name	<input type="text" value="test"/>		
East			
Interface			
Local SF	0		
Local Clear SF	0		
	Sent	Received	Ignored
SF	0	0	0
NR	0	0	0
NR-RB	0	0	0
FS	0	0	0
MS	0	0	0
EVENT	0	0	0
HEALTH	0	0	0
West			
Interface			
Local SF	0		

4.2.18 Loopback Detection

Switch Management > Loopback Detection page is used to configure loopback detection on an interface. When loopback detection is enabled and a port or group receives its own BPDU, the detection agent drops the loopback BPDU, sends an SNMP trap, and places the interface in discarding mode. This loopback state can be released manually or automatically. If the interface is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:

- The interface receives any other BPDU except for its own, or;
- The interfaces' link status changes to link down and then link up again, or;
- The interface ceases to receive its own BPDUs in a forward delay interval.

4.2.18.1 Global Configuration



- ◆ **Status** – Enables loopback detection on this interface. (Default: Enabled)
- ◆ **Trap** – Enables SNMP trap notification for loopback events on this interface. (Default: Disabled)
- ◆ **Release Mode** – Configures the interface for automatic or manual loopback release. (Default: Auto)
- ◆ **Release** – Allows an interface to be manually released from discard mode. This is only available if the interface is configured for manual release mode.
- ◆ **Action** – Sets the response for loopback detection to block user traffic or shut down the interface. (Default: Block)
- ◆ **Transmit Interval** – The duration to shut down the interface. (Range: 1-32767 seconds; Default: 60 seconds) If an interface is shut down due to a detected loopback, and the release mode is set to “Auto,” the selected interface will be automatically enabled when the shutdown interval has expired. If an interface is shut down due to a detected loopback, and the release mode is set to “Manual,” the interface can be re-enabled using the Release button.

4.2.18.2 Interface Configuration

Enable/disable port loopback detection

Interface Configuration Switch Management > Loopback Detection > Interface Configuration

Interface Port Group

Port List Total: 26

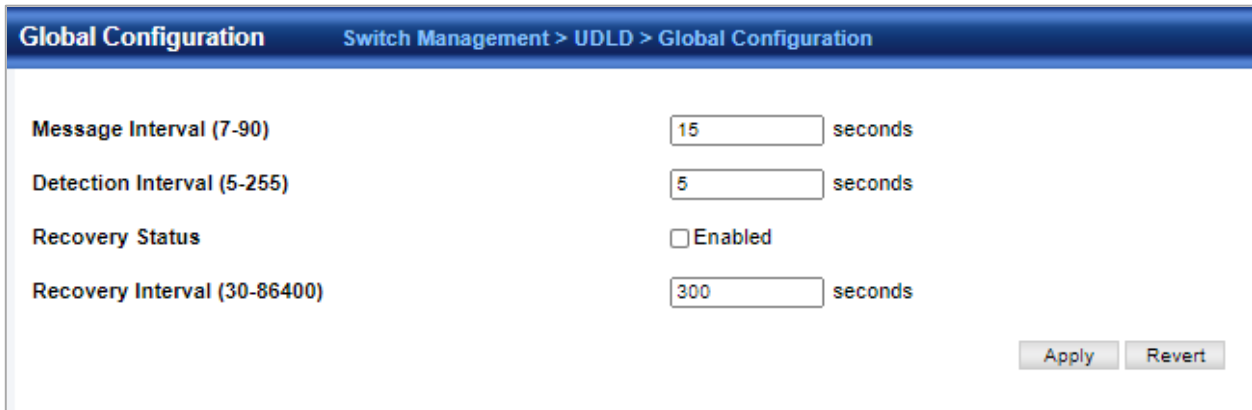
Port	Admin State	Looped VLAN
1	<input type="checkbox"/> Enabled	None
2	<input type="checkbox"/> Enabled	None
3	<input type="checkbox"/> Enabled	None
4	<input type="checkbox"/> Enabled	None
5	<input type="checkbox"/> Enabled	None
6	<input type="checkbox"/> Enabled	None
7	<input type="checkbox"/> Enabled	None
8	<input type="checkbox"/> Enabled	None
9	<input type="checkbox"/> Enabled	None
10	<input type="checkbox"/> Enabled	None

4.2.19 UDLD

The switch can be configured to detect general loopback conditions caused by hardware problems or faulty protocol settings. When enabled, a control frame is transmitted on the participating ports, and the switch monitors inbound traffic to see if the frame is looped back.

4.2.19.1 Global Configuration

Switch Management > UDLD > Global Configuration page is used to configure the Unidirectional Link Detection message probe interval, detection interval, and recovery interval.



Global Configuration	
Message Interval (7-90)	15 seconds
Detection Interval (5-255)	5 seconds
Recovery Status	<input type="checkbox"/> Enabled
Recovery Interval (30-86400)	300 seconds

Apply Revert

◆ Message Interval – Configures the message interval between UDLD probe messages for ports in the advertisement phase and determined to be bidirectional. (Range: 7-90 seconds; Default: 15 seconds)

UDLD probe messages are sent after linkup or detection phases. During the detection phase, messages are exchanged at the maximum rate of one per second. After that, if the protocol reaches a stable state and determines that the link is bidirectional, the message interval is increased to a configurable value based on a curve known as M1(t), a time-based function described in RFC 5171.

If the link is deemed anything other than bidirectional at the end of the detection phase, this curve becomes a flat line with a fixed value of Mfast (7 seconds).

If the link is instead deemed bidirectional, the curve will use Mfast for the first four subsequent message transmissions and then transition to an Mslow value for all other steady-state transmissions. Mslow is the value configured by this command.

◆ Detection Interval – Sets the amount of time the switch remains in detection state after discovering a neighbor. (Range: 5-255 seconds; Default: 5 seconds)

When a neighbor device is discovered by UDLD, the switch enters “detection state” and remains in this state for specified detection-interval. After the detection-interval expires, the switch tries to decide whether or the link is unidirectional based on the information collected during the “detection state.”

◆ Recovery Status – Configures the switch to automatically recover from UDLD disabled port state after a period specified by the Recovery Interval. (Default: Disabled)

When automatic recovery state is changed, any ports shut down by UDLD will be reset.

◆ Recovery Interval – Specifies the period after which to automatically recover from UDLD disabled port state. (Range: 30-86400 seconds; Default: 7 seconds)

When the recovery interval is changed, any ports shut down by UDLD will be reset.

4.2.19.2 Interface Configuration

Switch Management > UDLD > Interface Configuration page is used to enable UDLD and aggressive mode which reduces the shut-down delay after loss of bidirectional connectivity is detected.

Interface Configuration						
Switch Management > UDLD > Interface Configuration						
Port Configuration List Total: 28						
Port	Status	Aggressive Mode	Operation State	Port State	Message Interval (seconds)	Detection Interval (seconds)
1	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Disabled	Unknown	7	5
2	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Disabled	Unknown	7	5
3	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Disabled	Unknown	7	5
4	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Disabled	Unknown	7	5
5	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Disabled	Unknown	7	5
6	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Disabled	Unknown	7	5
7	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Disabled	Unknown	7	5
8	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Disabled	Unknown	7	5
9	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Disabled	Unknown	7	5
10	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	Disabled	Unknown	7	5

Apply Revert

- ◆ Port – Port identifier. (Range: 1-28/52)
 - ◆ UDLD – Enables UDLD on a port. (Default: Disabled)
 - UDLD requires that all the devices connected to the same LAN segment be running the protocol in order for a potential mis-configuration to be detected and for prompt corrective action to be taken.
 - Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-synch neighbor, it (re)starts the detection process on its side of the connection and sends N echo messages in reply. (This mechanism implicitly assumes that N packets are sufficient to get through a link and reach the other end, even though some of them might get dropped during the transmission.) Since this behavior must be the same on all the neighbors, the sender of the echoes expects to receive an echo in reply. If the detection process ends without the proper echo information being received, the link is considered to be unidirectional.
 - ◆ Aggressive Mode – Reduces the shut-down delay after loss of bidirectional connectivity is detected. (Default: Disabled)
- UDLD can function in two modes: normal mode and aggressive mode.
- In normal mode, determination of link status at the end of the detection process is always based on information received in UDLD messages: whether that's information about the exchange of proper neighbor identification or the absence of such. Hence, albeit bound by a timer, normal mode determinations are always based on gleaned information, and as such are "event-based." If no such information can be obtained (e.g., because of a bidirectional loss of connectivity), UDLD follows a conservative approach to minimize false positives during the detection process and deems a port to be in "undetermined" state. In other words, normal mode will shut down a port only if it can explicitly determine that the associated link is faulty for an extended period of time.
 - In aggressive mode, UDLD will also shut down a port if it loses bidirectional connectivity with the neighbor for the same extended period of time (as that mentioned above for normal mode) and subsequently fails repeated last-resort attempts to re-establish communication with the other end of the link. This mode of operation assumes that loss of communication with the neighbor is a meaningful network event in itself, and a symptom of a serious connectivity problem. Because this type of detection can be event-less, and lack of information cannot always be associated to an actual malfunction of the link, this mode is recommended only in certain scenarios (typically only on point-to-point links where no communication failure between two neighbors is admissible).

- ◆ Operation State – Shows the UDLD operational state (Disabled, Link down, Link up, Advertisement, Detection, Disabled port, Advertisement - Single neighbor, Advertisement - Multiple neighbors)
- ◆ Port State – Shows the UDLD port state (Unknown, Bidirectional, Unidirectional, Transmit-to-receive loop, Mismatch with neighbor state reported, Neighbor's echo is empty) The state is Unknown if the link is down or not connected to a UDLD-capable device. The state is Bidirectional if the link has a normal two-way connection to a UDLD-capable device. All other states indicate mis-wiring.
- ◆ Message Interval – The interval between UDLD probe messages used for the indicated operational state.
- ◆ Detection Interval – The period the switch remains in detection state after discovering a neighbor.

4.2.19.3 Neighbor Info

Switch Management > UDLD > Neighbor Info page is used to show UDLD neighbor information, including neighbor state, expiration time, and protocol intervals.



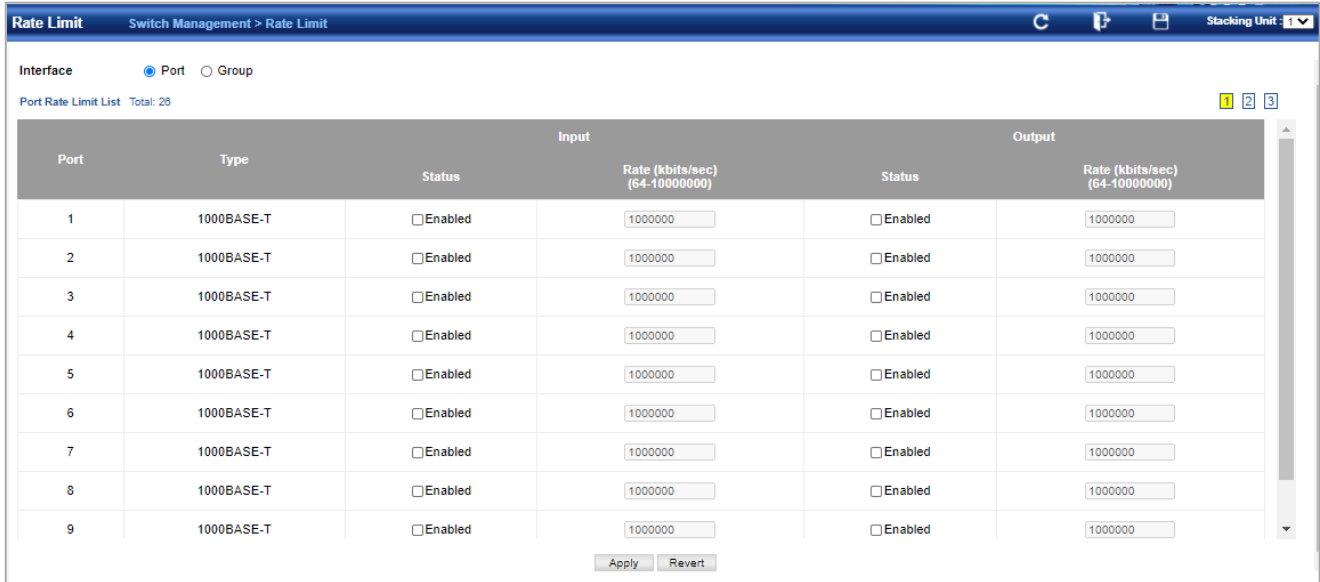
Entry	Device ID	Port ID	Device Name	Neighbor State	Expire (seconds)	Message Interval (seconds)	Detection Interval (seconds)
UDLD Neighbor List Total: 0							

- ◆ Port – Port identifier. (Range: 1-28/52)
- ◆ Entry – Table entry number uniquely identifying the neighbor device discovered by UDLD on a port interface.
- ◆ Device ID – Device identifier of neighbor sending the UDLD packet.
- ◆ Port ID – The physical port the UDLD packet is sent from.
- ◆ Device Name – The device name of this neighbor.
- ◆ Neighbor State – Link status of neighbor device (Values: unknown, neighborsEchoIsEmpty, bidirectional, mismatchWithneighborStateReported, unidirectional).
- ◆ Expire – The amount of time remaining before this entry will expire.
- ◆ Message Interval – The interval between UDLD probe messages for ports in advertisement phase.
- ◆ Detection Interval – The period the switch remains in detection state after discovering a neighbor.

4.2.20 Rate Limit

Interface>Congestion Control >Rate Limit page is used to apply rate limiting to ingress or egress ports.

This function allows the network manager to control the maximum rate for traffic received or transmitted on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped. Rate limiting can be applied to individual ports. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped; conforming traffic is forwarded without any changes.

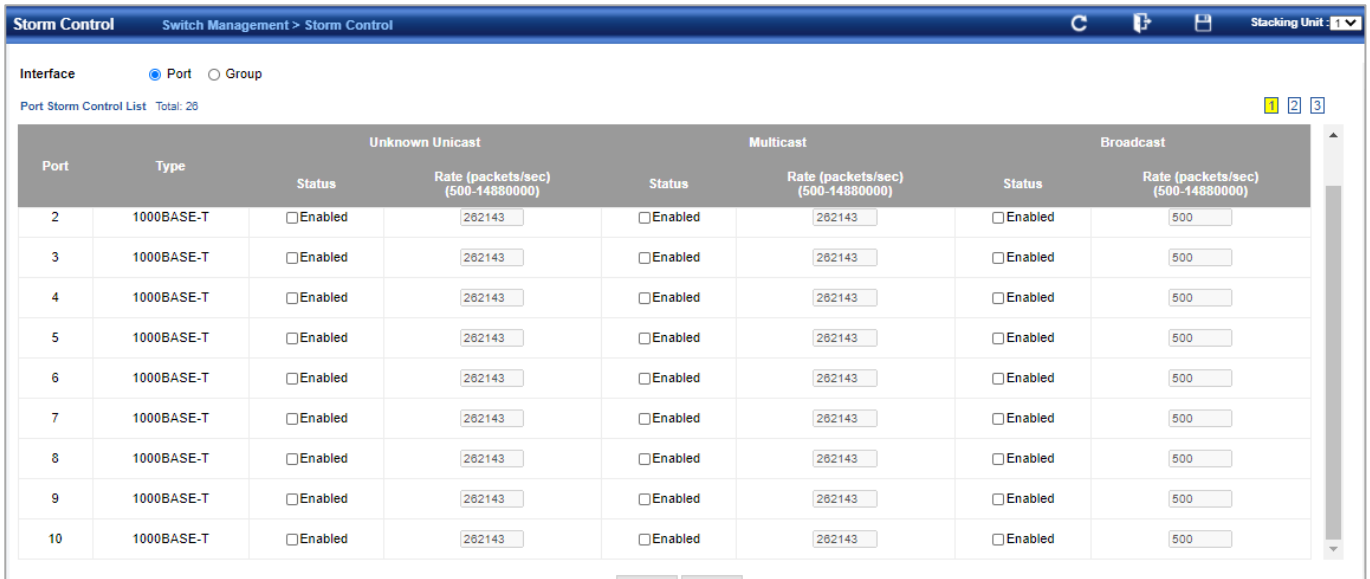


Port	Type	Input		Output	
		Status	Rate (kbts/sec) (64-10000000)	Status	Rate (kbts/sec) (64-10000000)
1	1000BASE-T	<input type="checkbox"/> Enabled	1000000	<input type="checkbox"/> Enabled	1000000
2	1000BASE-T	<input type="checkbox"/> Enabled	1000000	<input type="checkbox"/> Enabled	1000000
3	1000BASE-T	<input type="checkbox"/> Enabled	1000000	<input type="checkbox"/> Enabled	1000000
4	1000BASE-T	<input type="checkbox"/> Enabled	1000000	<input type="checkbox"/> Enabled	1000000
5	1000BASE-T	<input type="checkbox"/> Enabled	1000000	<input type="checkbox"/> Enabled	1000000
6	1000BASE-T	<input type="checkbox"/> Enabled	1000000	<input type="checkbox"/> Enabled	1000000
7	1000BASE-T	<input type="checkbox"/> Enabled	1000000	<input type="checkbox"/> Enabled	1000000
8	1000BASE-T	<input type="checkbox"/> Enabled	1000000	<input type="checkbox"/> Enabled	1000000
9	1000BASE-T	<input type="checkbox"/> Enabled	1000000	<input type="checkbox"/> Enabled	1000000

- ◆ **Interface**– Displays the switch’s ports or Groups.
- ◆ **Type** – Indicates the port type. (1000BASE-T, 10GBASE SFP+)
- ◆ **Status** – Enables or disables the rate limit. (Default: Disabled)
- ◆ **Rate** – Sets the rate limit level. (Range: 64 - 1,000,000 kbts per second for Gigabit Ethernet ports;64 - 10,000,000 kbts per second for 10 Gigabit Ethernet ports)

4.2.21 Storm Control

Interface>Congestion Control >Storm Control page is used to configure broadcast, multicast, and unknown unicast storm control thresholds.



Port	Type	Unknown Unicast		Multicast		Broadcast	
		Status	Rate (packets/sec) (500-14880000)	Status	Rate (packets/sec) (500-14880000)	Status	Rate (packets/sec) (500-14880000)
2	1000BASE-T	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	500
3	1000BASE-T	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	500
4	1000BASE-T	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	500
5	1000BASE-T	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	500
6	1000BASE-T	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	500
7	1000BASE-T	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	500
8	1000BASE-T	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	500
9	1000BASE-T	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	500
10	1000BASE-T	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	262143	<input type="checkbox"/> Enabled	500

- ◆ **Interface** – Displays a list of ports or groups.
- ◆ **Type** – Indicates interface type. (1000BASE-T or 10GBASE SFP)
- ◆ **Unknown Unicast** – Specifies storm control for unknown unicast traffic.
- ◆ **Multicast** – Specifies storm control for multicast traffic.
- ◆ **Broadcast** – Specifies storm control for broadcast traffic.
- ◆ **Status** – Enables or disables storm control. (Default: Enabled for broadcast storm control, disabled for multicast and unknown unicast storm control)
- ◆ **Rate** – Threshold level in Kilobits per second. (Range: 64-10,000,000 Kbps; Default: 64 Kbps)

4.2.22 Stacking

4.2.22.1 Global Configuration

Switch Management > Stacking > Global Configuration page is used to convert switch mode between stacking and non-stacking and reset unit numbers.

Press Change Status button:

Global Configuration Switch Management > Stacking > Global Configuration

Current Status	Enabled
Status After Reboot	Enabled
Stacking Up Port	27
Stacking Down Port	28

Note: When the configured status is different from the current status, the configured status takes effect after reboot.

Change Status
Re-assign Unit ID

Status	<input checked="" type="checkbox"/> Enabled
Current Status	Enabled
Stacking Up Port	27
Stacking Down Port	28

Note: When the configured status is different from the current status, the configured status takes effect after reboot.

Apply
Revert

4.2.22.2 Master Configuration

Switch Management > Stacking > Master Configuration page is used to set master button on the switch.

Master Configuration Switch Management > Stacking > Master Configuration

Master Button List Total: 1

Unit	Master Flag
1	<input checked="" type="checkbox"/> Enabled

Apply
Revert

4.2.23 Pepo

4.2.23.1 Global Configuration

Switch Management > Pepo > Global Configuration page is used to set the global configuration of Pepo.

Global Configuration Switch Management > PPPoE > Global Configuration

Status Enabled

Access Node Identifier

Current Access Node Identifier 192.168.0.100

Generic Error Message

Current Generic Error Message PPPoE Discover packet too large to process. Try reducing the number of tags added.

4.2.23.2 Interface Configuration

Switch Management > Pepo > Interface Configuration page is used to set the parameters of interface for Pepo.

Interface Configuration Switch Management > PPPoE > Interface Configuration Stacking Unit: 1

Interface Port Group

PPPoE Intermediate Agent Port List Total: 26

Port	Status	Trust	Vendor Tag Strip	Circuit ID	Remote ID	Remote ID Delimiter	Delimiter ASCII (0-255)
1	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	1/1:vid	64-0D-09-11-68-35	<input type="checkbox"/> Enabled	35
2	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	1/2:vid	64-0D-09-11-68-36	<input type="checkbox"/> Enabled	35
3	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	1/3:vid	64-0D-09-11-68-37	<input type="checkbox"/> Enabled	35
4	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	1/4:vid	64-0D-09-11-68-38	<input type="checkbox"/> Enabled	35
5	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	1/5:vid	64-0D-09-11-68-39	<input type="checkbox"/> Enabled	35
6	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	1/6:vid	64-0D-09-11-68-3A	<input type="checkbox"/> Enabled	35
7	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	1/7:vid	64-0D-09-11-68-3B	<input type="checkbox"/> Enabled	35
8	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	1/8:vid	64-0D-09-11-68-3C	<input type="checkbox"/> Enabled	35
9	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	1/9:vid	64-0D-09-11-68-3D	<input type="checkbox"/> Enabled	35
10	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	1/10:vid	64-0D-09-11-68-3E	<input type="checkbox"/> Enabled	35

4.2.23.3 Statistics

Switch Management > Pepo > Statistics page is used to display the counters of Pepo.

Statistics Switch Management > LLDP > Statistics

General Port Group

LLDP Device Statistics

Neighbor Entries List Last Updated	0 sec
New Neighbor Entries Count	0
Neighbor Entries Deleted Count	0
Neighbor Entries Dropped Count	0
Neighbor Entries Age-out Count	0

4.3 Route Management

4.3.1 IPv4 Interface Configuration

This section describes how to configure an IPv4 interface for management access over the network.

Route Management > IPv4 Interface Configuration page is used to configure an IPv4 address for the switch.

IPv4 Interface Configuration		Route Management > IPv4 Interface Configuration			
Routing Interface IP List Total: 1					
<input type="checkbox"/>	Vlan	Mode	Type	Address	Subnet Mask
<input type="checkbox"/>	1	Static	Primary	192.168.0.100	255.255.255.0
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>					

VLAN

Mode

Type

IP Address

Subnet Mask

[Click this button to resend DHCP client request.](#)

◆ **VLAN** – ID of the configured VLAN (1-4093). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.

◆ **Mode** – Specifies whether IP functionality is enabled via manual configuration (User Specified), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. DHCP/BOOTP responses can include the IP address, subnet mask, and default gateway. (Default: DHCP)

◆ **Type** – Specifies a primary or secondary IP address. An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface. For initial configuration, set this parameter to Primary. (Options: Primary, Secondary; Default: Primary)
 Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router or switch in a network segment uses a secondary address, all other routers/switches in that segment must also use a secondary address from the same network or subnet address space.

◆ **IP Address** – Address of the VLAN to which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: None)

◆ **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: None)

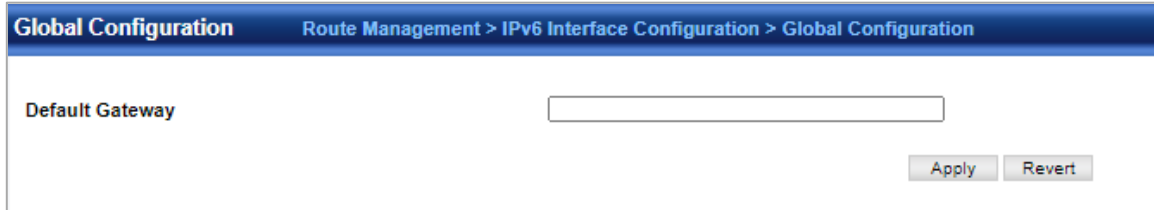
◆ **Restart DHCP** – Requests a new IP address from the DHCP server.

4.3.2 IPv6 Interface Configuration

This section describes how to configure an IPv6 interface for management access over the network.

4.3.2.1 Global Configuration

Route Management > IPv6 Interface Configuration > Global Configuration page is used to configure an IPv6 default gateway for the switch.

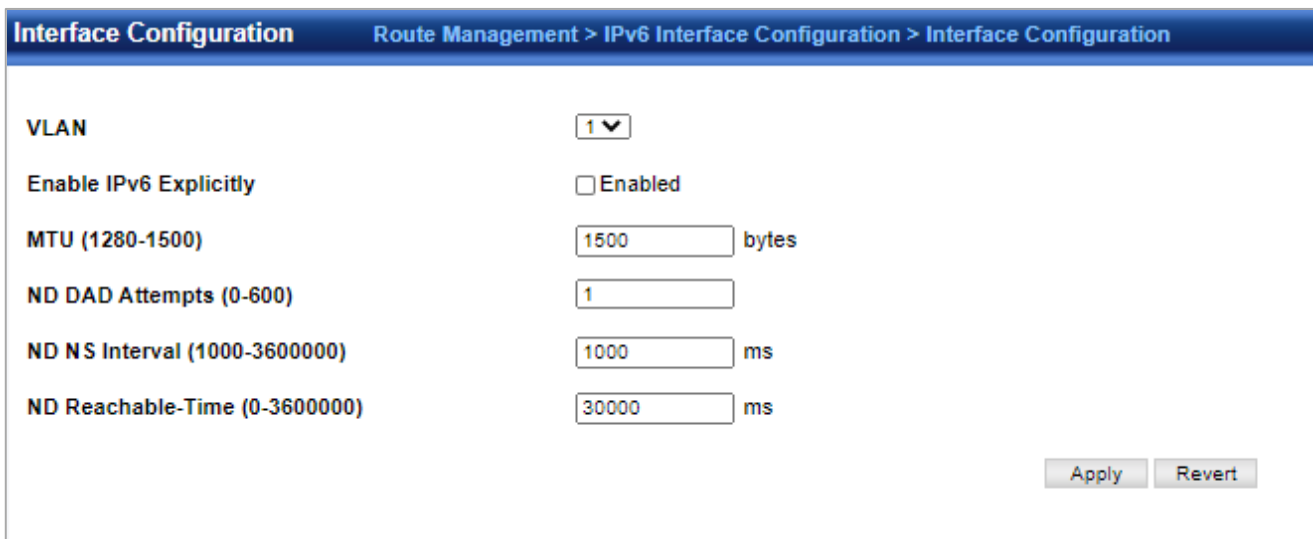


◆ **Default Gateway** – Sets the IPv6 address of the default next hop router.

- An IPv6 default gateway must be defined if the management station is located in a different IPv6 segment.
- An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

4.3.2.2 Interface Configuration

Route Management > IPv6 Interface Configuration > Interface Configuration page is used to configure general IPv6 settings for the selected VLAN, including auto-configuration of global unicast address, explicit configuration of a link local interface address, the MTU size, and neighbor discovery protocol settings for duplicate address detection and the neighbor solicitation interval.



◆ **VLAN** – ID of a configured VLAN which is to be used for management access. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)

◆ **Address Autoconfig** – Enables stateless autoconfiguration of IPv6 addresses on an interface and enables IPv6 functionality on that interface. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host portion is automatically generated using the modified EUI-64 form of the interface identifier (i.e., the switch's MAC address).

- If the router advertisements have the “other stateful configuration” flag set, the switch will attempt to acquire other non-address configuration information (such as a default gateway).
- If auto-configuration is not selected, then an address must be manually configured using the Add Interface page described below.

◆ **Enable IPv6 Explicitly** – Enables IPv6 on an interface. Note that when an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed. (Default: Disabled) Disabling this parameter does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.

◆ **MTU** – Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. (Range: 1280-65535 bytes; Default: 1500 bytes)

- The maximum value set in this field cannot exceed the MTU of the physical interface, which is currently fixed at 1500 bytes.
- IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.
- All devices on the same physical medium must use the same MTU in order to operate correctly.
- IPv6 must be enabled on an interface before the MTU can be set. If an IPv6 address has not been assigned to the switch, "N/A" is displayed in the MTU field.

◆ **ND DAD Attempts** – The number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. (Range: 0-600, Default: 3)

- Configuring a value of 0 disables duplicate address detection.
- Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
- Duplicate address detection is stopped on any interface that has been suspended. While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a "pending" state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.
- An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface's link-local address, the other IPv6 addresses remain in a "tentative" state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
- If a duplicate address is detected, it is set to "duplicate" state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in "duplicate" state.
- If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

◆ **ND NS Interval** – The interval between transmitting IPv6 neighbor solicitation messages on an interface. (Range: 1000-3600000 milliseconds; Default: 1000 milliseconds is used for neighbor discovery operations, 0 milliseconds is advertised in router advertisements. This attribute specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

◆ **ND Reachable-Time** – The amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred. (Range: 0-3600000 milliseconds; Default: 30000 milliseconds)

4.3.2.3 RA-Guard

Route Management > IPv6 Interface Configuration > RA-Guard page is used to configure RA guard status on a port or group.

RA-Guard
Route Management > IPv6 Interface Configuration > RA-Guard

Interface Port Group

Port List Total: 26

Port	RA Guard
1	<input type="checkbox"/> Enabled
2	<input type="checkbox"/> Enabled
3	<input type="checkbox"/> Enabled
4	<input type="checkbox"/> Enabled
5	<input type="checkbox"/> Enabled
6	<input type="checkbox"/> Enabled
7	<input type="checkbox"/> Enabled
8	<input type="checkbox"/> Enabled
9	<input type="checkbox"/> Enabled
10	<input type="checkbox"/> Enabled
11	<input type="checkbox"/> Enabled

◆ **Interface** – Shows port or trunk configuration page.

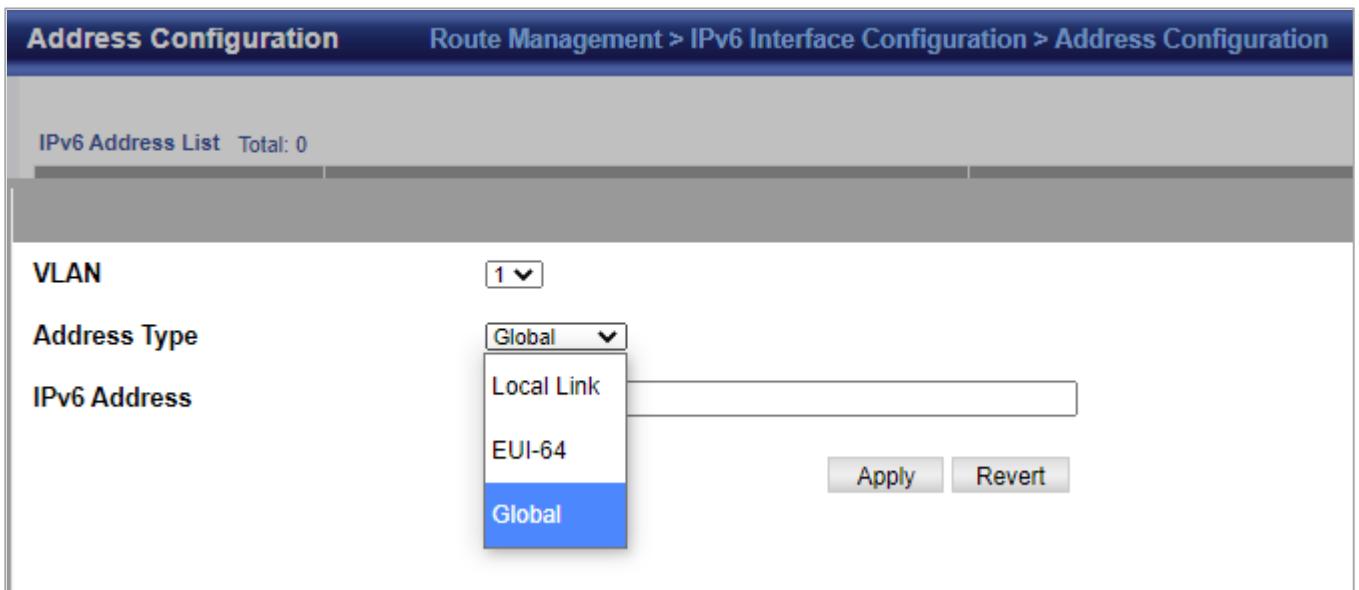
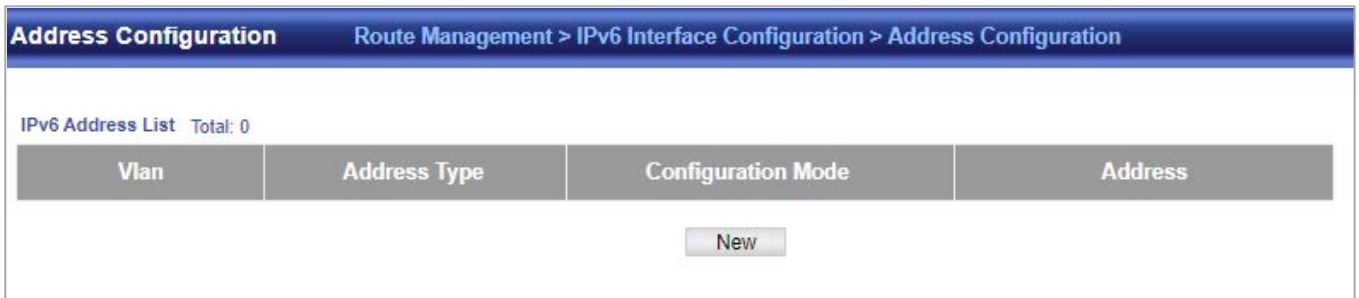
◆ **RA Guard** – Blocks incoming Router Advertisement and Router Redirect packets. (Default: Disabled)

IPv6 Router Advertisements (RA) convey information that enables nodes to auto-configure on the network. This information may include the default router address taken from the observed source address of the RA message, as well as on-link prefix information. However, note that unintended misconfigurations, or possibly malicious attacks on the network, may lead to bogus RAs being sent, which in turn can cause operational problems for hosts on the network.

RA Guard can be used to block RAs and Router Redirect (RR) messages on the specified interface. Determine which interfaces are connected to known routers, and enable RA Guard on all other untrusted interfaces.

4.3.2.4 Address Configuration

Route Management > IPv6 Interface Configuration > Address Configuration page is used to configure an IPv6 interface for management access over the network.



◆ **VLAN** – ID of a configured VLAN which is to be used for management access. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)

◆ **Address Type** – Defines the address type configured for this interface.

- **Global** – Configures an IPv6 global unicast address with a full IPv6 address including the network prefix and host address bits, followed by a forward slash, and a decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).
- **EUI-64 (Extended Universal Identifier)** – Configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits.
- **Link Local** – Configures an IPv6 link-local address.

◆ **IPv6 Address** – IPv6 address assigned to this interface.

4.3.2.5 Neighbor List

Route Management > IPv6 Interface Configuration > Neighbor List page is used to display the IPv6 addresses detected for neighbor devices.

Neighbor List		Route Management > IPv6 Interface Configuration > Neighbor List		
Current Neighbor Cache Table Total: 0				
VLAN	Address	Mac Address	State	Age

4.3.2.6 Statistics

Route Management > IPv6 Interface Configuration > Statistics page is used to display statistics about IPv6 traffic passing through this switch.

Statistics		Route Management > IPv6 Interface Configuration > Statistics	
IPv6 Statistics			
Total Received	5	Received Reassembly Succeeded	0
Received Header Errors	0	Received Reassembly Failed	0
Received Too Big Errors	0	Transmitted Forwards Datagrams	0
Received No Routes	0	Transmitted Requests	2
Received Address Errors	0	Transmitted Discards	0
Received Unknown Protocols	0	Transmitted No Routes	0
Received Truncated Packets	0	Transmitted Generated Fragments	0
Received Discards	0	Transmitted Fragment Succeeded	0
Received Delivers	5	Transmitted Fragment Failed	0
Received Reassembly Request Datagrams	0		
<input type="button" value="Clear"/>			

4.3.2.7 MTU

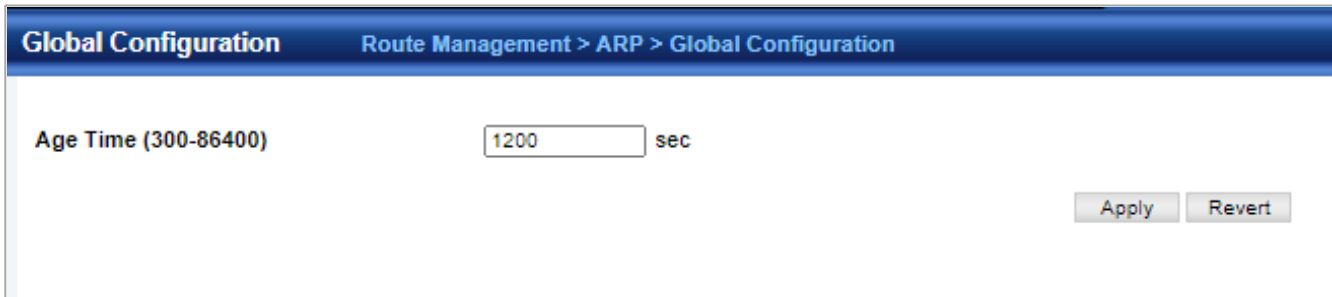
Route Management > IPv6 Interface Configuration > MTU page is used to display the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch.



4.3.3 ARP

4.3.3.1 Global Configuration

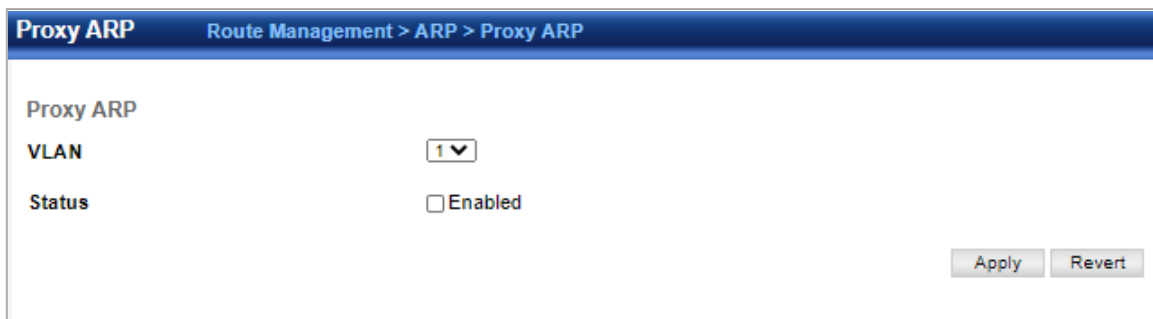
Route Management > ARP > Global Configuration page is used to set the timeout for ARP entry.



◆ **Age time**—Sets the aging time for dynamic entries in the ARP cache. (Range: 300 - 86400 seconds; Default: 1200 seconds or 20 minutes) The ARP aging timeout can be set for any configured VLAN. The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table. When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.

4.3.3.2 Proxy ARP

Route Management > ARP > Proxy ARP page is used to enable Proxy ARP for specific VLAN interfaces.



◆ **Proxy ARP**—Enables or disables Proxy ARP for specified VLAN interfaces, allowing a non-routing device to determine the MAC address of a host on another subnet or network. (Default: Disabled) End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices. Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

4.3.3.3 Static Arp

Route Management > ARP > Static Arp page is used to manually map an IP address to the corresponding physical address in the ARP cache.

Static Arp
Route Management > ARP > Static Arp

Static Address List Total: 1

	IP Address	MAC Address
<input type="checkbox"/>	10.0.0.1	00-00-00-00-00-01

IP Address

MAC Address (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)

◆ **IP Address** – IP address statically mapped to a physical MAC address. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)

◆ **MAC Address** – MAC address statically mapped to the corresponding IP address. (Valid MAC addresses are hexadecimal numbers in the format: xx-xxxx-xx-xx-xx)

4.3.3.4 ARP Address List

Route Management > ARP > ARP Address List page is used to display dynamic or local entries in the ARP cache and statistics for ARP messages crossing all interfaces on this router. The ARP cache contains static entries, and entries for local interfaces, including subnet, host, and broadcast addresses. However, most entries will be dynamically learned through replies to broadcast messages.

ARP Address List
Route Management > ARP > ARP Address List

ARP Address List Total: 0

IP Address	MAC Address	Type	Interface
------------	-------------	------	-----------

4.3.4 Routing Table

Route Management > Routing Table > Routing Table page is used to display all routes that can be accessed via local network interfaces, through static routes, or through a dynamically learned route. If route information is available through more than one of these methods, the priority for route selection is local, static, and then dynamic (except when the distance parameter of a dynamic route is set to a value that makes its priority exceed that of a static route). Also note that the route for local interface is not enabled (i.e., listed in the routing table) unless there is at least one active link connected to that interface.

Routing Table					
Route Management > Routing Table					
Routing Table	Static Routes				
Routing Table List Total: 2					
Interface	Destination IP Address	Net Mask / Prefix Length	Next Hop	Metric	Protocol
lo	127.0.0.0	255.0.0.0	--	0	Local
Loopback	::1	128	--	0	Local

- ◆ **VLAN**—VLAN identifier (i.e., configured as a valid IP subnet).
- ◆ **Destination IP Address**— IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.
- ◆ **Net Mask / Prefix Length**—Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- ◆ **Next Hop**—The IP address of the next hop (or gateway) in this route.
- ◆ **Metric**—Cost for this interface.
- ◆ **Protocol**—The protocol which generated this route information. (Options: Local, Static, RIP, OSPF, Others)

Routing Table				
Route Management > Routing Table				
Routing Table	Static Routes			
Static Table List Total: 1				
<input type="checkbox"/>	Destination IP Address	Net Mask / Prefix Length	Next Hop	Distance
<input type="checkbox"/>	0.0.0.0	0.0.0.0	192.168.0.254	1
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>				

Route Management > Routing Table > Static Routes page is used to enter static routes in the routing table. Static routes may be required to access network segments where dynamic routing is not supported, or can be set to force the use of a specific route to a subnet, rather than using dynamic routing. Static routes do not automatically change in response to changes in network topology, so you should only configure a small number of stable routes to ensure network accessibility.

- ◆ **Destination IP Address** – IP address of the destination network, subnetwork, or host.
- ◆ **Net Mask / Prefix Length**—Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- ◆ **Next Hop**—IP address of the next router hop used for this route.
- ◆ **Distance**—An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used

by the dynamic unicast routing protocols is 110 for OSPF, 120 for RIP, 20 for eBGP, and 200 for iBGP. (Range: 1-255, Default: 1)

Destination IP Address

Net Mask / Prefix Length

Next Hop

4.4 ACL

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

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

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

4.4.1 ACL Configuration

ACL > ACL Configuration page is used to configure ACL.

ACL Configuration
ACL > ACL Configuration

ACL List Total: 1

	ACL Name	Type
<input type="checkbox"/>	TEST	IP Standard

ACL Name

Type

◆ **ACL Name** – Name of the ACL. (Maximum length: 32 characters)

◆ **Type** – The following filter modes are supported:

- **IP Standard:** IPv4 ACL mode filters packets based on the source IPv4 address.
- **IP Extended:** IPv4 ACL mode filters packets based on the source or destination IPv4 address, as well as the protocol type and protocol port number. If the "TCP" protocol is specified, then you can also filter packets based on the TCP control code.

- **IPv6 Standard:** IPv6 ACL mode filters packets based on the source IPv6 address.
- **IPv6 Extended:** IPv6 ACL mode filters packets based on the source or destination IP address, as well as DSCP, and the next header type.
- **MAC** – MAC ACL mode filters packets based on the source or destination MAC address and the Ethernet frame type.
- **ARP** – ARP ACL specifies static IP-to-MAC address bindings used for ARP inspection.

4.4.2 Rule Configuration

ACL > Rule Configuration page is used to configure the rule in acl.



The screenshot shows the 'Rule Configuration' page with the following details:

- Type:** IP Standard (selected), IP Extended, IPv6 Standard, IPv6 Extended, MAC, ARP.
- ACL Name:** TEST
- ACL Rule List Total:** 1

■	Action	Source IP Address	Time-Range
<input type="checkbox"/>	Permit	10.0.0.1 / 255.255.0.0	

- Buttons:** New, Delete, Revert

Standard Ipv4 Acl

ACL > Rule Configuration > Ip Standard page is used to configure a Standard IPv4 ACL.

- ◆ **ACL Name** – Shows the names of ACLs.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Address Type** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)
- ◆ **Source IP Address** – Source IP address.
- ◆ **Source Subnet Mask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bit to indicate “match” and 0 bits to indicate “ignore.” The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- ◆ **Time Range** – Name of a time range.



The screenshot shows the configuration form for an IP Standard ACL with the following fields:

- ACL Name:** TEST
- Type:** IP Standard
- Action:** Permit
- Address Type:** IP
- Source IP Address:** 10.0.0.1
- Source Subnet Mask:** 255.255.0.0
- Time-Range:** (unchecked)
- Buttons:** Apply, Revert

Extended Ipv4 Acl

ACL > Rule Configuration > Ip Extended page is used to configure an Extended IPv4 ACL.

ACL Name	<input type="text" value="aaa"/>		
Type	IP Extended		
Source Address Type	<input type="text" value="Any"/>	Destination Address Type	<input type="text" value="Any"/>
Source IP Address	<input type="text" value="0.0.0.0"/>	Destination IP Address	<input type="text" value="0.0.0.0"/>
Source Subnet Mask	<input type="text" value="0.0.0.0"/>	Destination Subnet Mask	<input type="text" value="0.0.0.0"/>
Source Port (0-65535)	<input type="text"/>	Destination Port (0-65535)	<input type="text"/>
Source Port Bit Mask (0-65535)	<input type="text"/>	Destination Port Bit Mask (0-65535)	<input type="text"/>
IP Protocol	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other IP Protocol ID <input type="text"/>		
Control Code (0-63)	<input type="text"/>	Service Type	<input type="radio"/> ToS (0-15) <input type="text"/> <input checked="" type="radio"/> Precedence (0-7) <input type="text"/> <input type="radio"/> DSCP (0-63) <input type="text"/>
Control Code Bit Mask (0-63)	<input type="text"/>		
Time-Range	<input type="text"/>		
Action	<input type="text" value="Permit"/>		
	<input type="button" value="Apply"/>	<input type="button" value="Revert"/>	

- ◆ **ACL Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Source/Destination Address Type** – Specifies the source or destination IP address type. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)
- ◆ **Source/Destination IP Address** – Source or destination IP address.
- ◆ **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask .)
- ◆ **Source/Destination Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)
- ◆ **Source/Destination Port Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)
- ◆ **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: Others)
- ◆ **Service Type** – Packet priority settings based on the following criteria:
 - **Precedence** – IP precedence level. (Range: 0-7)
 - **DSCP** – DSCP priority level. (Range: 0-63)
- ◆ **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- ◆ **Control Code Bit Mask** – Decimal number representing the code bits to match. (Range: 0-63) The control bit mask is a decimal number (for an equivalent binary bitmask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:
 - 1 (fin) – Finish
 - 2 (syn) – Synchronize
 - 4 (rst) – Reset
 - 8 (psh) – Push
 - 16 (ack) – Acknowledgement
 - 32 (urg) – Urgent pointer For example, use the code value and mask below to catch packets with the following flags set:
 - SYN flag valid, use control-code 2, control bit mask 2
 - Both SYN and ACK valid, use control-code 18, control bit mask 18

- SYN valid and ACK invalid, use control-code 2, control bit mask 18

◆Time Range – Name of a time range.

Standard Ipv6 Cal

ACL > Rule Configuration > IPv6 Standard page is used to configure a Standard IPv6ACL.

ACL Name	12 ▼
Type	IPv6 Standard
Action	Permit ▼
Source Address Type	Any ▼
Source IPv6 Address	::
Source Prefix Length (0-128)	0
<input type="checkbox"/> Time-Range	▼

◆ACL Name – Shows the names of ACLs matching the selected type.

◆Action – An ACL can contain any combination of permit or deny rules.

◆Source Address Type – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IPv6-Prefix” to specify a range of addresses. (Options: Any, Host, IPv6-Prefix; Default: Any)

◆Source IPv6 Address – An IPv6 source address or network class. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

◆Source Prefix-Length – A decimal value indicating how many contiguous bits (from the left) of the address comprising the prefix (i.e. the network portion of the address). (Range: 0-128 bits)

◆Time Range – Name of a time range.

Extended Ipv6 Acl

ACL > Rule Configuration > IPv6 Extended page is used to configure an Extended IPv6 ACL.

ACL Name	15 ▼		
Type	IPv6 Extended		
Action	Permit ▼		
<input type="checkbox"/> Protocol	Next Header ▼		
Source Address Type	Any ▼	Destination Address Type	Any ▼
Source IPv6 Address	::	Destination IPv6 Address	::
Source Prefix Length (0-128)	0	Destination Prefix Length (0-128)	0
DSCP (0-63)			
<input type="checkbox"/> Time-Range	▼		
<input type="button" value="Apply"/> <input type="button" value="Revert"/>			

◆ **ACL Name** – Shows the names of ACLs matching the selected type.

◆ **Action** – An ACL can contain any combination of permit or deny rules.

◆ **Source/Destination Address Type** – Specifies the source or destination IP address type. Use “Any” to include all possible addresses, or “IPv6-Prefix” to specify a range of addresses. (Options: Any, IPv6-Prefix; Default: Any)

◆ **Source/Destination IPv6 Address** – An IPv6 address or network class. The address must be formatted according to RFC 2373 “IPv6Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

◆ **Source/Destination Prefix-Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprising the prefix i.e., the network portion of the address. (Range: 0-128 bits for the source address; 0-8 bits for the destination address)

◆ **DSCP** – DSCP traffic class. (Range: 0-63)

◆ **Next Header** – Identifies the type of header immediately following the IPv6 header. (Range: 0-255) Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. IPv6 supports the values defined for the IPv4 Protocol field in RFC 1700, and includes these commonly used headers:

- 0 : Hop-by-Hop Options (RFC 2460)
- 6 : TCP Upper-layer Header (RFC 1700)
- 17 : UDP Upper-layer Header (RFC 1700)
- 43 : Routing (RFC 2460)
- 44 : Fragment (RFC 2460)
- 50 : Encapsulating Security Payload (RFC 2406)
- 51 : Authentication (RFC 2402)
- 60 : Destination Options (RFC 2460)

◆ **Time Range** – Name of a time range.

Mac Acl

ACL > Rule Configuration > MAC page is used to configure a MAC ACL based on hardware addresses, packet format, and Ethernet type.

Type	MAC	
ACL Name	16	
Action	Permit	
Destination Address Type	Any	Source Address Type
Destination MAC Address	00-00-00-00-00-00	Source MAC Address
Destination Bit Mask	00-00-00-00-00-00	Source Bit Mask
Packet Format	Any	
Ethernet Type		VID (1-4094)
(0000-FFFF, hexadecimal value)		
Ethernet Type Bit Mask		VID Bit Mask (0-4095)
(0000-FFFF, hexadecimal value)		
CoS (0-7)		
CoS Bit Mask (0-7)		
<input type="checkbox"/> Time-Range		
<input type="button" value="Apply"/> <input type="button" value="Revert"/>		

- ◆ **ACL Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Source/Destination Address Type** – Use “Any” to include all possible addresses, “Host” to indicate a specific MAC address, or “MAC” to specify an address range with the Address and Bit Mask fields.(Options: Any, Host, MAC; Default: Any)
- ◆ **Source/Destination MAC Address** – Source or destination MAC address.
- ◆ **Source/Destination Bit Mask** – Hexadecimal mask for source or destination MAC address.
- ◆ **Packet Format** – This attribute includes the following packet types:
 - **Any** – Any Ethernet packet type.
 - **Untagged-eth2** – Untagged Ethernet II packets.
 - **Untagged-802.3** – Untagged Ethernet 802.3 packets.
 - **Tagged-eth2** – Tagged Ethernet II packets.
 - **Tagged-802.3** – Tagged Ethernet 802.3 packets.
- ◆ **VID** – VLAN ID. (Range: 1-4094)
- ◆ **VID Bit Mask** – VLAN bit mask. (Range: 0-4095)
- ◆ **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-ffff hex.) A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).
- ◆ **Ethernet Type Bit Mask** – Protocol bit mask. (Range: 600-ffff hex)
- ◆ **CoS** – CoS value. (Range: 0-7)
- ◆ **CoS Bit Mask** – CoS bit mask. (Range: 0-7)
- ◆ **Time Range** – Name of a time range.

Arp Acl

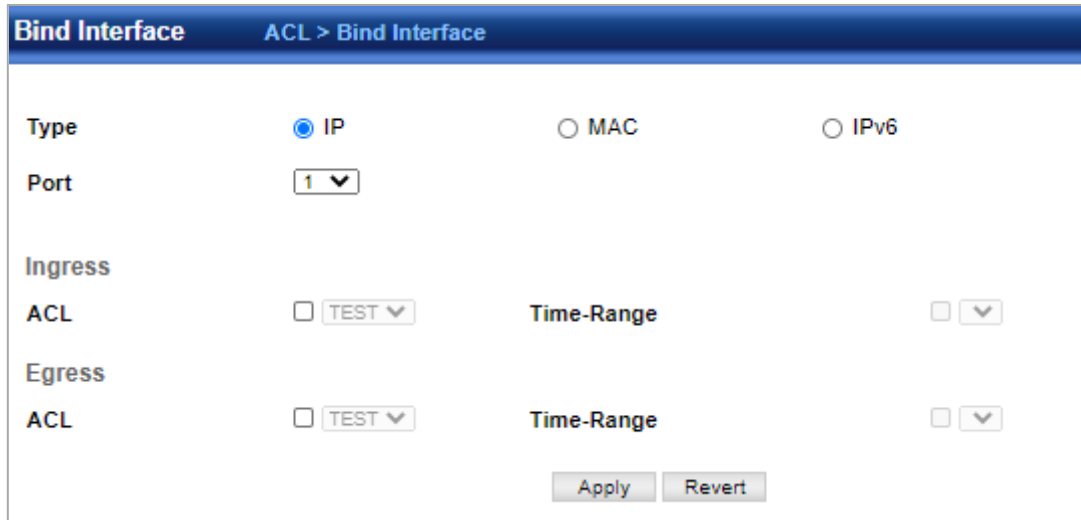
ACL > Rule Configuration > ARP page is used to configure ACLs based on ARP message addresses. ARP Inspection can then use these ACLs to filter suspicious traffic.

ACL Name	17 ▼		
Type	ARP		
Packet Type	Request-Response ▼		
Source IP Address Type	Any ▼	Destination IP Address Type	Any ▼
Source IP Address	0.0.0.0	Destination IP Address	0.0.0.0
Source IP Subnet Mask	0.0.0.0	Destination IP Subnet Mask	0.0.0.0
Source MAC Address Type	Any ▼	Destination MAC Address Type	Any ▼
Source MAC Address	00-00-00-00-00-00	Destination MAC Address	00-00-00-00-00-00
Source MAC Bit Mask	00-00-00-00-00-00	Destination MAC Bit Mask	00-00-00-00-00-00
Action	Permit ▼	<input type="checkbox"/> Log when packet match	
<input type="button" value="Apply"/> <input type="button" value="Revert"/>			

- ◆ **ACL Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Packet Type** – Indicates an ARP request, ARP response, or either type. (Range: IP, Request, Response; Default: IP)
- ◆ **Source/Destination IP Address Type** – Specifies the source or destination IPv4 address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Mask fields. (Options: Any, Host, IP; Default: Any)
- ◆ **Source/Destination IP Address** – Source or destination IP address.
- ◆ **Source/Destination IP Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask .)
- ◆ **Source/Destination MAC Address Type** – Use “Any” to include all possible addresses, “Host” to indicate a specific MAC address, or “MAC” to specify an address range with the Address and Mask fields. (Options: Any, Host, MAC; Default: Any)
- ◆ **Source/Destination MAC Address** – Source or destination MAC address.
- ◆ **Source/Destination MAC Bit Mask** – Hexadecimal mask for source or destination MAC address.
- ◆ **Log when packet match** – Logs a packet when it matches the access control entry.

4.4.3 Bind Interface

ACL > Bind Interface page is used to bind the ports that need to filter traffic to the appropriate ACLs. You can assign one IP access list and one MAC access list to any port.



- ◆ **Type** – Selects the type of ACLs to bind to a port.
- ◆ **Port** – Port identifier.
- ◆ **ACL** – ACL used for ingress or egress packets.
- ◆ **Time Range** – Name of a time range.

4.5 CoS

CoS > Cos page is used to specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

◆ **Port** – Displays a list of ports or trunks.

◆ **CoS** – The priority that is assigned to untagged frames received on the specified interface. (Range: 0-7; Default: 0)

CoS
CoS

Interface Port Group

Port VLAN CoS for Untagged packet Total: 26

Port	CoS (0-7)
1	<input type="text" value="0"/>
2	<input type="text" value="0"/>
3	<input type="text" value="0"/>
4	<input type="text" value="0"/>
5	<input type="text" value="0"/>
6	<input type="text" value="0"/>
7	<input type="text" value="0"/>
8	<input type="text" value="0"/>
9	<input type="text" value="0"/>
10	<input type="text" value="0"/>

4.6 Qu's

4.6.1 Egress Queue

Qu's > Egress Queue page is used to set the queue mode for the egress queues on any interface. The switch can be set to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before the lower priority queues are serviced, or Weighted Round-Robin (WRR) queuing which specifies a scheduling weight for each queue. It can also be configured to use a combination of strict and weighted queuing.

Egress Queue
QoS > Egress Queue

Port 1 ▼

Queue Mode WRR ▼

Queue Setting Table Total: 8

Egress Queue ID	Weight (1-15)
0	1
1	2
2	4
3	6
4	8
5	10
6	12
7	14

◆ Queue Mode

- **Strict** – Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.
- **WRR** – Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights, and servicing each queue in a round-robin fashion. (This is the default setting.)
- **Strict and WRR** – Uses strict priority on the high-priority queues and WRR on the remaining queues.

◆ **Queue ID** – The ID of the priority queue. (Range: 0-7)

◆ **Strict Mode** – If “Strict and WRR” mode is selected, then a combination of strict services is used for the high priority queues and weighted service for the remaining queues. Use this parameter to specify the queues assigned to use strict priority. (Default: Disabled)

◆ **Weight** – Sets a weight for each queue which is used by the WRR scheduler. (Range: 1-255; Default: Weights 1, 2, 4, 6, 8, 10, 12 and 14 are assigned to queues 0 - 7 respectively)

4.6.2 Trust Mode

The switch allows a choice between using DSCP or CoS priority processing methods. Qu's> Trust Mode page is used to select the required processing method.

Trust Mode
QoS > Trust Mode

Trust Mode(Classify ingress packet with which value) List Total: 26

Port	Trust Mode
1	CoS ▼
2	CoS ▼
3	CoS ▼
4	CoS ▼
5	CoS ▼
6	CoS ▼
7	CoS ▼
8	CoS ▼
9	CoS ▼
10	CoS ▼

◆ **Port** – Port identifier. (Range: 1-28)

◆ **Trust Mode**

- **CoS** – Maps layer 3/4 priorities using Class of Service values. (This is the default setting.)
- **DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point values.

4.6.3 Qu's Map

Qu's> Qu's Map page is used to map DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing.

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

DHCP to PHB/DP

- ◆ **Port** – Specifies a port.
- ◆ **DSCP** – DSCP value in ingress packets. (Range: 0-63)
- ◆ **PHB** – Per-hop behavior, or the priority used for this router hop.(Range: 0-7)
- ◆ **Drop Precedence** – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

Port 1 ▼

DSCP (0-63)

PHB (0-7)

Drop Precedence 0: Green ▼

To show the DHCP to PHB/DP precedence map:

QoS Map
QoS > QoS Map

DSCP to PHB/DP
 COS to PHB/DP
 PHB/DP to COS
 IP Precedence to PHB/DP
 TCP/UDP Port to PHB/DP
 PHB to Queue

Port 1 ▼

DSCP to DSCP Mapping List Total: 64

□	DSCP of Ingress Packet	PHB	Drop Precedence
□	0	0	0: Green
□	1	0	1: Red
□	2	0	0: Green
□	3	0	3: Yellow
□	4	0	0: Green
□	5	0	1: Red
□	6	0	0: Green
□	7	0	3: Yellow
□	8	1	0: Green
□	9	1	1: Red

CoS to PHB/DP

- ◆ **Port** – Specifies a port.
- ◆ **CoS** – CoS value in ingress packets. (Range: 0-7)
- ◆ **CFI** – Canonical Format Indicator. Set to this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)
- ◆ **PHB** – Per-hop behavior, or the priority used for this router hop.(Range: 0-7)
- ◆ **Drop Precedence** – Drop precedence used in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

Port	<input type="text" value="1"/>
CoS (0-7)	<input type="text"/>
CFI (0-1)	<input type="text"/>
PHB (0-7)	<input type="text"/>
Drop Precedence	<input type="text" value="0: Green"/>

To show the **CoS to PHB/DP** precedence map:

QoS Map QoS > QoS Map

DSCP to PHB/DP
 COS to PHB/DP
 PHB/DP to COS
 IP Precedence to PHB/DP
 TCP/UDP Port to PHB/DP
 PHB to Queue

Port:

CoS to DSCP Mapping List Total: 16 1 2

☐	CoS of ingress packet	CFI of Ingress packet	PHB	Drop Precedence
<input type="checkbox"/>	0	0	0	0: Green
<input type="checkbox"/>	0	1	0	0: Green
<input type="checkbox"/>	1	0	1	0: Green
<input type="checkbox"/>	1	1	1	0: Green
<input type="checkbox"/>	2	0	2	0: Green
<input type="checkbox"/>	2	1	2	0: Green
<input type="checkbox"/>	3	0	3	0: Green
<input type="checkbox"/>	3	1	3	0: Green
<input type="checkbox"/>	4	0	4	0: Green
<input type="checkbox"/>	4	1	4	0: Green

PHB/DP to CoS

PHB/DP to CoS page is used to map internal per-hop behavior and drop precedence value pairs to CoS values used in tagged egress packets on a Layer 2 interface.

- ◆ **Port** – Specifies a port.
- ◆ **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- ◆ **Drop Precedence** – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)
- ◆ **CoS** – Class-of-Service value. (Range: 0-7)
- ◆ **CFI** – Canonical Format Indicator. Set this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)

Port	<input type="text" value="1"/>
PHB (0-7)	<input type="text"/>
Drop Precedence	<input type="text" value="0: Green"/>
CoS (0-7)	<input type="text"/>
CFI (0-1)	<input type="text"/>

To show the **PHB/DP to CoS** precedence map:

QoS Map QoS > QoS Map

DSCP to PHB/DP
 COS to PHB/DP
 PHB/DP to COS
 IP Precedence to PHB/DP
 TCP/UDP Port to PHB/DP
 PHB to Queue

Port

DSCP to CoS Mapping List Total: 24

	PHB	Drop Precedence	CoS	CFI
<input type="checkbox"/>	0	0	0	0
<input type="checkbox"/>	0	1	0	0
<input type="checkbox"/>	0	3	0	0
<input type="checkbox"/>	1	0	1	0
<input type="checkbox"/>	1	1	1	0
<input type="checkbox"/>	1	3	1	0
<input type="checkbox"/>	2	0	2	0
<input type="checkbox"/>	2	1	2	0
<input type="checkbox"/>	2	3	2	0
<input type="checkbox"/>	3	0	3	0

IP Precedence to PHB/DP

IP Precedence to PHB/DP page is used to map IP precedence values in incoming packets to per-hop behavior and drop precedence values for priority processing.

- ◆ **Port** – Specifies a port.
- ◆ **IP Precedence** – IP Precedence value in ingress packets. (Range: 0-7)
- ◆ **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- ◆ **Drop Precedence** – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

Port 1 ▼

IP Precedence (0-7)

PHB (0-7)

Drop Precedence 0: Green ▼

Apply
Revert

To show the IP Precedence to PHB/DP precedence map:

QoS Map QoS > QoS Map

DSCP to PHB/DP
 COS to PHB/DP
 PHB/DP to COS
 IP Precedence to PHB/DP
 TCP/UDP Port to PHB/DP
 PHB to Queue

Port 1 ▼

[IP Precedence to DSCP Mapping List](#) Total: 8

IP Precedence of Ingress packet	PHB	Drop Precedence
0	0	0: Green
1	1	0: Green
2	2	0: Green
3	3	0: Green
4	4	0: Green
5	5	0: Green
6	6	0: Green
7	7	0: Green

Configure
Default
Revert

TCP/UDP Port to DSCP

TCP/UDP Port to DSCP page is used to map network applications designated by a TCP/UDP destination port number in the frame header to per-hop behavior and drop precedence values for internal priority processing.

- ◆ **Port** – Specifies a port.
- ◆ **IP Protocol**
- **TCP** – Transport Control Protocol
- **UDP** – User Datagram Protocol
- ◆ **Destination Port Number** – 16-bit TCP/UDP destination port number. (Range: 0-65535)
- ◆ **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- ◆ **Drop Precedence** – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

Port 1 ▼

IP Protocol TCP ▼

Destination Port (0-65535)

PHB (0-7)

Drop Precedence 0: Green ▼

To show the TCP/UDP Port to DSCP precedence map:

QoS Map
QoS > QoS Map

DSCP to PHB/DP
 COS to PHB/DP
 PHB/DP to COS
 IP Precedence to PHB/DP
 TCP/UDP Port to PHB/DP
 PHB to Queue

Port 1 ▼

IP Port to DSCP Mapping List Total: 0

Protocol of Ingress packet	Protocol port of Ingress packet	PHB	Drop Precedence
<input type="button" value="Configure"/>			

PHB to Queue

PHB to Queue page is used to specify the hardware output queues to use based on the internal per-hop behavior value.

- ◆ **Port** – Specifies a port.
- ◆ **PHB** – Per-hop behavior, or the priority used for this router hop.(Range: 0-7, where 7 is the highest priority)
- ◆ **Queue** – Output queue buffer. (Range: 0-7, where 7 is the highest CoS priority queue)

PHB (0-7)

Queue (0-7)

To show the TCP/UDP Port to DSCP precedence map:

QoS Map QoS > QoS Map

DSCP to PHB/DP
 COS to PHB/DP
 PHB/DP to COS
 IP Precedence to PHB/DP
 TCP/UDP Port to PHB/DP
 PHB to Queue

PHB to Queue Mapping List Total: 8

<input type="checkbox"/>	PHB	Queue
<input type="checkbox"/>	0	2
<input type="checkbox"/>	1	0
<input type="checkbox"/>	2	1
<input type="checkbox"/>	3	3
<input type="checkbox"/>	4	4
<input type="checkbox"/>	5	5
<input type="checkbox"/>	6	6
<input type="checkbox"/>	7	7

4.6.4 Class

A class map is used for matching packets to a specified class. Qu's > Class page is used to configure a class map. Add

Class QoS > Class

Class List Total: 0

Class Name

Type

Description

- ◆ **Class Name** – Name of the class map. (Range: 1-32 characters)
- ◆ **Type** – The criteria specified by the match command.
 - **Match Any** – Match any condition within a class map.
- ◆ **Description** – A brief description of a class map. (Range: 1-64characters)

4.6.5 Class Match

To edit the rules for a class map:

Class Name

Type Match Any

Rule:

ACL

IP DSCP (0-63)

IP Precedence (0-7)

IPv6 DSCP (0-63)

VLAN ID (1-4094)

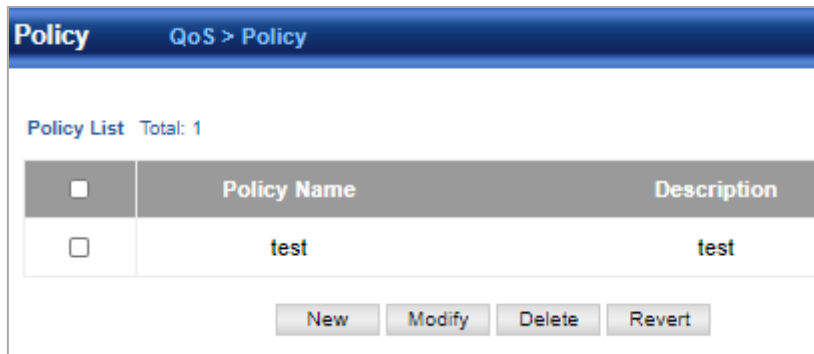
CoS (0-7)

Class Match		
QoS > Class Match		
Class Name	<input type="text" value="test"/>	
Match Type	Match Any	
Match Entry List	Total: 1	
<input type="checkbox"/>	Entry Type	Entry Content
<input type="checkbox"/>	ACL	16
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>		

4.6.6 Policy

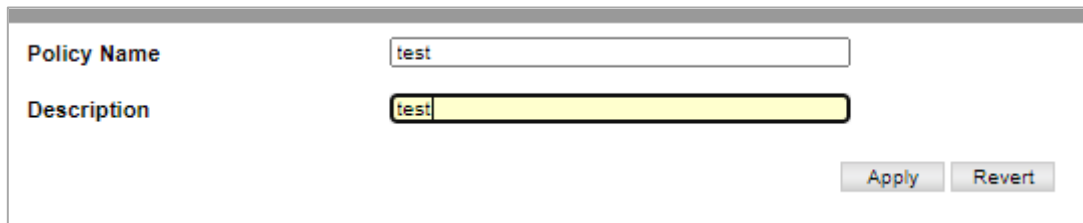
Qu's> Policy page is used to create a policy map that can be attached to multiple interfaces. A policy map is used to group one or more class map statements, modify service tagging, and enforce bandwidth policing.

A policy map can then be bound by a service policy to one or more interfaces.



Policy		QoS > Policy	
Policy List Total: 1			
<input type="checkbox"/>	Policy Name	Description	
<input type="checkbox"/>	test	test	
<input type="button" value="New"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>			

New



Policy Name	<input type="text" value="test"/>
Description	<input type="text" value="test"/>
<input type="button" value="Apply"/> <input type="button" value="Revert"/>	

- ◆ **Policy Name** – Name of policy map. (Range: 1-32 characters)
- ◆ **Description** – A brief description of a policy map. (Range: 1-256 characters)

4.6.7 Policy Map

To edit the rules for a policy map:

Policy Name	<input type="text" value="test"/>
Map Entry:	
Bound Class Name	<input type="text" value="test"/>
Action	<input type="text" value="Disable"/> <input type="text" value="Set"/> <input type="text" value="CoS (0-7)"/> <input type="text"/>
Meter	<input type="text" value="Disable"/>
Meter Mode	<input type="text" value="Flow"/>
Committed Information Rate (0-10000000)	<input type="text"/> kbps
Committed Burst Size (4000-16000000)	<input type="text"/> bytes
Excess Burst Size (4000-16000000)	<input type="text"/> bytes
Peak Information Rate (0-10000000)	<input type="text"/> kbps
Peak Burst Size (4000-16000000)	<input type="text"/> bytes
Action for Conform	<input type="text" value="Set IP DSCP (0-83)"/> <input type="text"/>

- ◆ **Policy Name** – Name of policy map.
- ◆ **Bound Class Name** – Name of a class map that defines a traffic classification upon which a policy can act.
- ◆ **Action** – This attribute is used to set an internal Qu's value in hardware for matching packets.
The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion with the srTCM and trTCM metering functions.
- ◆ **Meter** – Check this to define the maximum throughput, burst rate, and the action that results from a policy violation.
- ◆ **Meter Mode** – Selects one of the following policing methods.
- ◆ **Committed Information Rate (CIR)** – Rate in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)The rate cannot exceed the configured interface speed.
- ◆ **Committed Burst Size (BC)** – Burst in bytes.(Range: 64-16000000 at a granularity of 4k bytes)The burst size cannot exceed 16 Mbytes.
- ◆ **Excess Burst Size (BE)** – Burst in excess of committed burst size. (Range: 0-16000000 at a granularity of 4k bytes).The burst size cannot exceed 16 Mbytes.
- ◆ **Peak Information Rate (PIR)** – Rate in kilobits per second. (Range: 0-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower). The rate cannot exceed the configured interface speed.
- ◆ **Peak Burst Size (BP)** – Burst size in bytes.(Range: 0-16000000 at a granularity of 4k bytes).The burst size cannot exceed 16 Mbytes.
- ◆ **Action for Conform** – Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.
- ◆ **Action for Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the excess burst size (BE) will be dropped or the DSCP service level will be reduced.
- ◆ **Action for Violate** – Specifies whether the traffic that exceeds the excess burst size (BE) will be dropped or the DSCP service level will be reduced.

To show the rules for a policy map:

Policy Map QoS > Policy Map

Policy Name:

Rule List Total: 1

Class Name	Action	Meter								
		Meter Mode	Committed Information Rate (kbps)	Committed Burst Size (bytes)	Excess Burst Size (bytes)	Peak Information Rate (kbps)	Peak Burst Size (bytes)	Conform	Exceed	Violate
<input type="checkbox"/> test			0	0				N/A	N/A	N/A

4.6.8 Bind Interface

Qu's > Bind Interface page is used to bind a policy map to a port.

First define a class map, define a policy map, and bind the service policy to the required interface.

Bind Interface QoS > Bind Interface

Policy bind list Total: 28

Port	Policy for Ingress	Policy for Egress
1	<input type="checkbox"/> test	<input type="checkbox"/> test
2	<input type="checkbox"/> test	<input type="checkbox"/> test
3	<input type="checkbox"/> test	<input type="checkbox"/> test
4	<input type="checkbox"/> test	<input type="checkbox"/> test
5	<input type="checkbox"/> test	<input type="checkbox"/> test
6	<input type="checkbox"/> test	<input type="checkbox"/> test
7	<input type="checkbox"/> test	<input type="checkbox"/> test
8	<input type="checkbox"/> test	<input type="checkbox"/> test
9	<input type="checkbox"/> test	<input type="checkbox"/> test
10	<input type="checkbox"/> test	<input type="checkbox"/> test

- ◆ **Port** – Specifies a port.
- ◆ **Policy for Ingress** – Applies the selected rule to ingress traffic.
- ◆ **Policy for Egress** – Applies the selected rule to egress traffic.

4.7 Security

4.7.1 AAA

This section is to control the access to the Managed Switch, including the user access and management control.

The Authentication section contains links to the following main topics:

- **User Authentication**
- **IEEE 802.1X Port-based Network Access Control**
- **MAC-based 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 SGS-5240 series to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and Web browser. This SGS-5240 series 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 SGS-5240 Series PoE Switch.

Understanding IEEE 802.1X Port-based Authentication

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

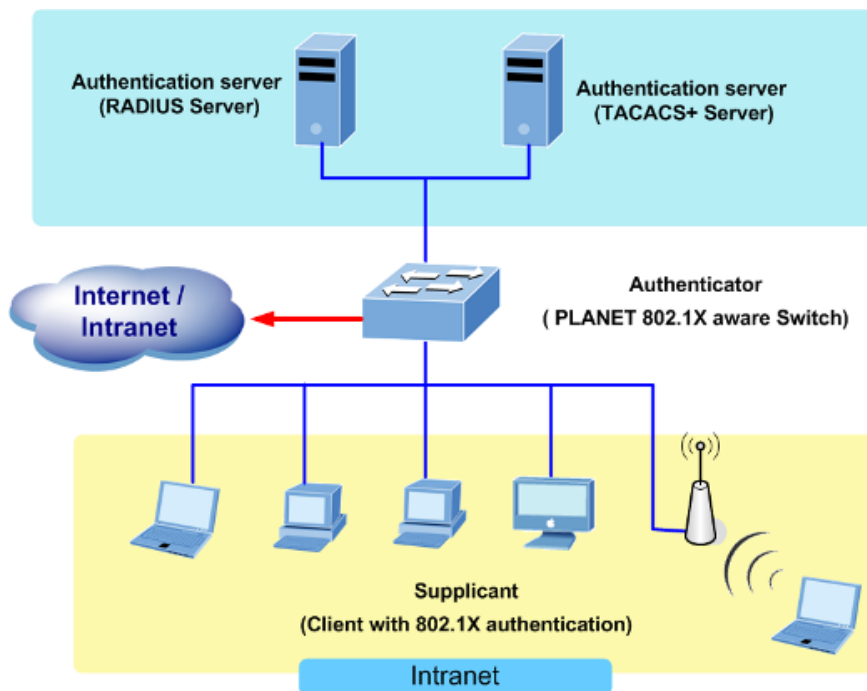
Until the client is authenticated, 802.1X access control allows only **Extensible Authentication Protocol over LAN (EAPOL)** traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

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.



- **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 4-5-2" shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

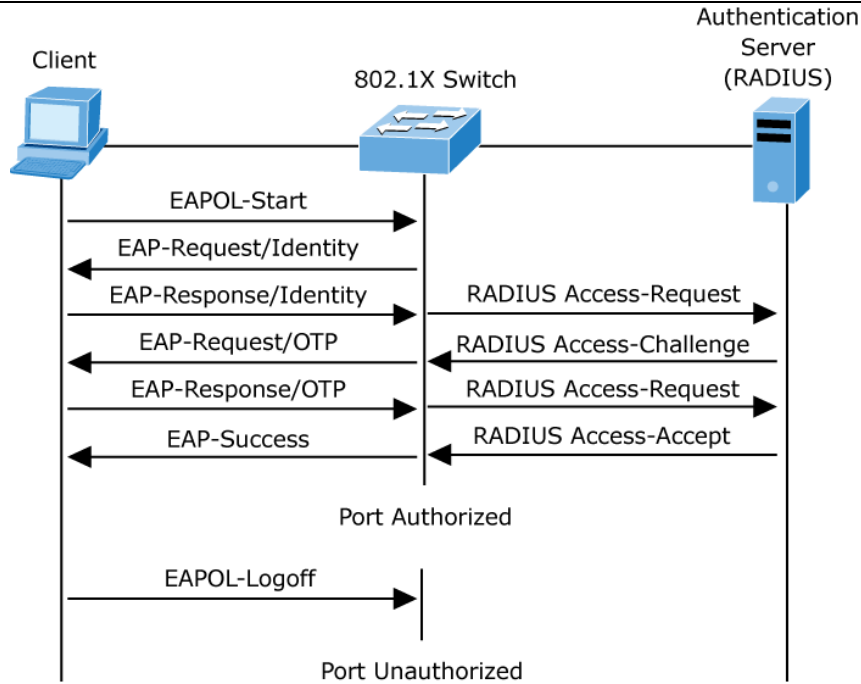


Figure 4-5-2-2: EAP Message Exchange

■ 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.

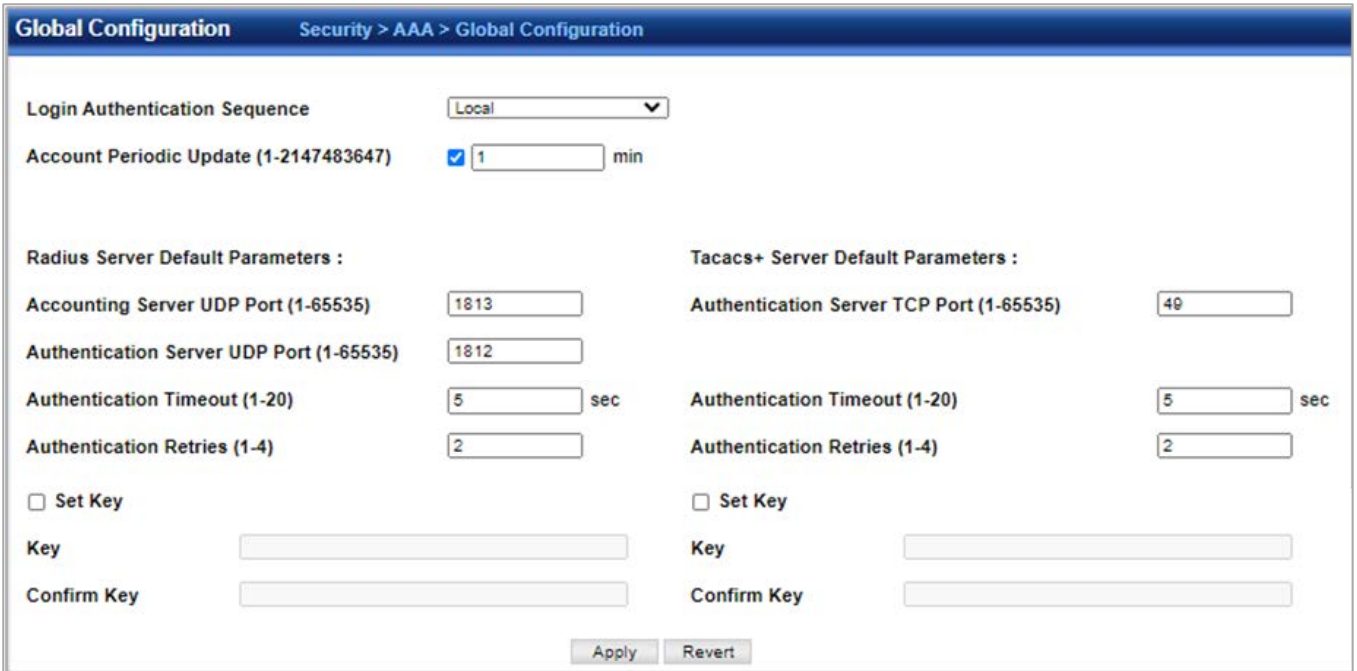
If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

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.

4.7.1.1 Global Configuration

Security > AAA > Global Configuration page to set global configuration .



◆ **Authentication Sequence** –set the sequence of authentication. There are three methods of authentication.

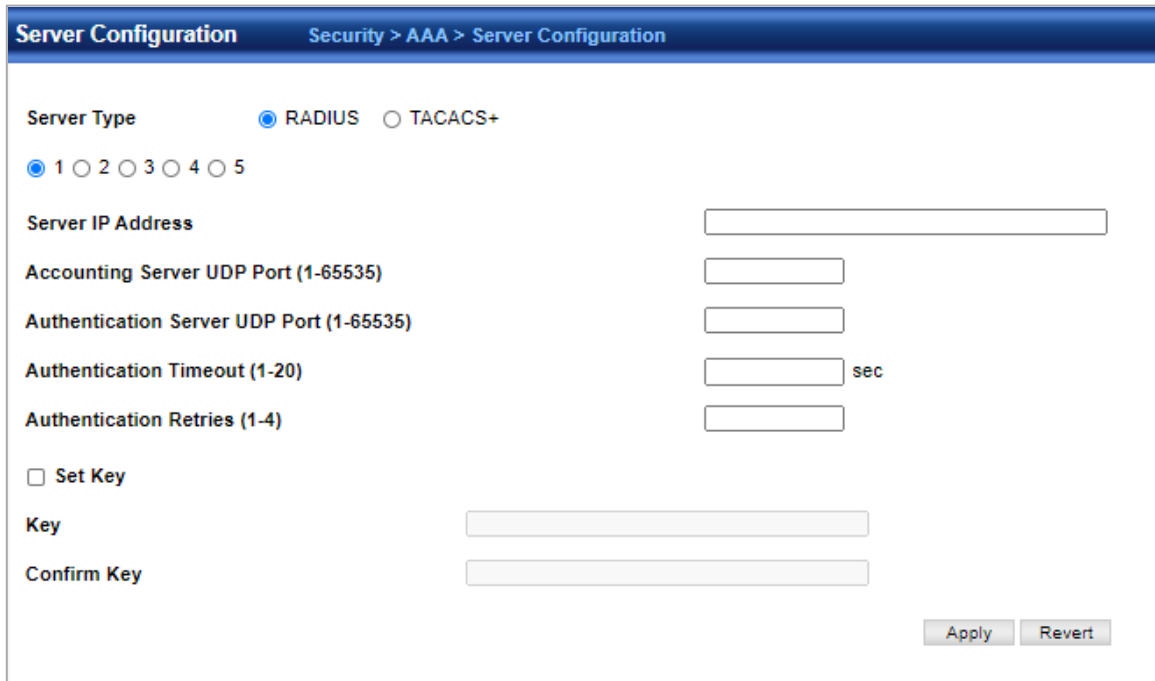
- **Local** – User authentication is performed only locally by the switch.
- **RADIUS** – User authentication is performed using a RADIUS server only.
- **TACACS** – User authentication is performed using a TACACS+ server only.

◆ **RADIUS Server Default Parameters:** if a RADIUS server does not set these parameters, the default parameter will be active.

◆ **TACACS+ Server Default Parameters:** if the TACACS+ server does not set these parameters, the default parameter will be active.

4.7.1.2 Server Configuration

Security>AAA>Server configuration page is used to configure the parameters of RADIUS or TACACS+ server for AAA:



4.7.1.3 Server List

Security>AAA>Server List page is used to configure the RADIUS or TACACS+ server groups for accounting and authorization.

Server list includes a list of servers.



	List Name	Server Sequence
<input type="checkbox"/>	radius	

4.7.1.4 Accounting Strategy

Security>AAA>Accounting Strategy page is used to configure the strategy for Accounting.

Accounting Strategy Security > AAA > Accounting Strategy

Strategy List Total: 2

	Strategy Name	Accounting Type	Accounting Message	Server List Name
<input type="checkbox"/>	default	Network-Access	Start-Stop	radius
<input type="checkbox"/>	default	Login	Start-Stop	tacacs+

4.7.1.5 Interface Accounting

Security>AAA>Interface Accounting page is used to configure the strategy used on the interface.

Interface Accounting Security > AAA > Interface Accounting

Accounting Type Network-Access Login

Port Strategy List Total: 28

Port	Strategy Name
1	<input type="checkbox"/> default ▼
2	<input type="checkbox"/> default ▼
3	<input type="checkbox"/> default ▼
4	<input type="checkbox"/> default ▼
5	<input type="checkbox"/> default ▼
6	<input type="checkbox"/> default ▼
7	<input type="checkbox"/> default ▼
8	<input type="checkbox"/> default ▼
9	<input type="checkbox"/> default ▼
10	<input type="checkbox"/> default ▼

4.7.1.6 Authorization Strategy

Security>AAA>Authorization Strategy page is used to configure the strategy for authorization.

Authorization Strategy			
Security > AAA > Authorization Strategy			
Strategy List Total: 2			
<input type="checkbox"/>	Authorization Type	Strategy Name	Server List Name
<input type="checkbox"/>	Login	default	tacacs+
<input type="checkbox"/>	Login	test	radius
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>			

Authorization Type	<input type="text" value="Login"/>
Strategy Name	<input type="text" value="test"/>
Server List Name	<input checked="" type="radio"/> <input type="text" value="radius"/> <input type="radio"/> <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Revert"/>	

4.7.1.7 Authorization configuration

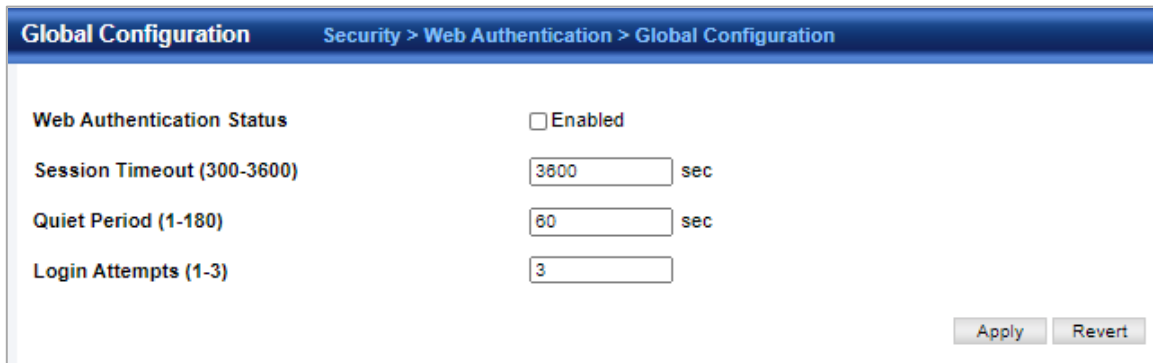
Security>AAA>Authorization Configuration page is used to configure the authorization strategy for console login and vty (telnet, ssh) login.

Authorization Configuration	
Security > AAA > Authorization Configuration	
Authorization Type	<input type="text" value="Login"/>
Console Strategy Name	<input type="text"/>
VTY Strategy Name	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Revert"/>	

4.7.2 Web Authentication

4.7.2.1 Global Configuration

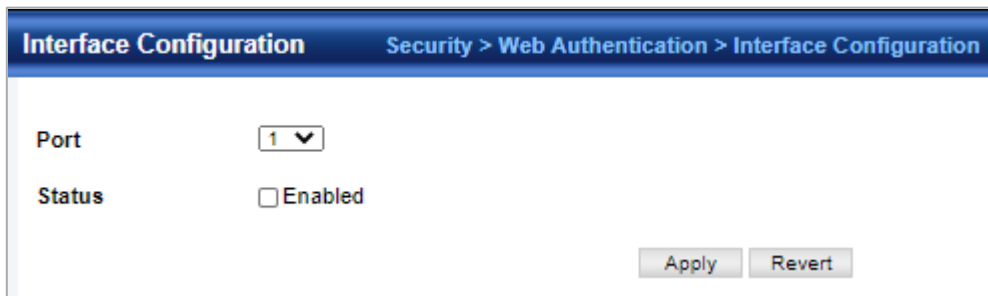
Security > Web Authentication > Global Configuration page is used to edit the global parameters for web authentication.



- ◆ **Web Authentication Status** – Enables web authentication for the switch. (Default: Disabled)
Note that this feature must also be enabled for any port where required under the Configure Interface menu.
- ◆ **Session Timeout** – Configures how long an authenticated session stays active before it must re-authenticate itself. (Range: 300-3600 seconds; Default: 3600 seconds)
- ◆ **Quiet Period** – Configures how long a host must wait to attempt authentication again after it has exceeded the maximum allowable failed login attempts. (Range: 1-180 seconds; Default: 60 seconds)
- ◆ **Login Attempts** – Configures the amount of times a supplicant may attempt and fail authentication before it must wait the configured quiet period. (Range: 1-3 attempts; Default: 3 attempts)

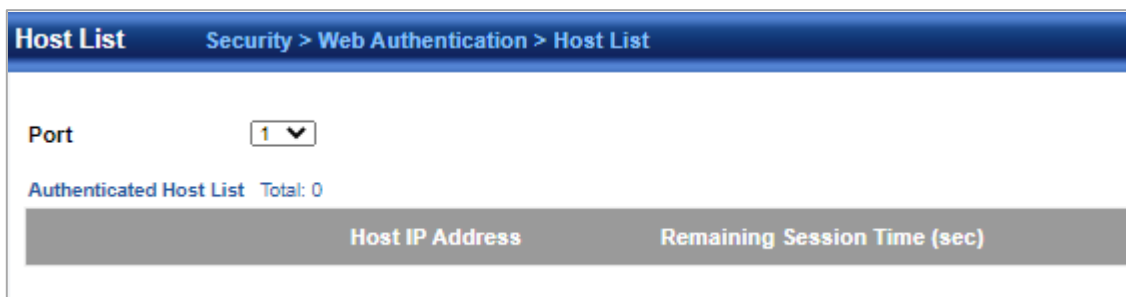
4.7.2.2 Interface Configuration

Security > Web Authentication > Interface Configuration page is used to configure the interface.



4.7.2.3 Host List

Security > Web Authentication > Host List page is used to show the Host information.



4.7.3 802.1X

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.

4.7.3.1 Global Configuration

Security > 802.1x > Global Configuration page is used to configure the global parameter of 802.1x.



- ◆ 802.1X Status – Sets the global setting for 802.1X. (Default: Disabled)
- ◆ **EAPOL Pass-through** – Passes EAPOL frames through all ports in STP forwarding state when dot1x is globally disabled. (Default: Disabled)

4.7.3.2 Interface Configuration

Security > 802.1x > Interface Configuration page is used to configure the parameters of a port.

Interface Configuration			
Security > 802.1X > Interface Configuration			
Port	<input type="text" value="1"/>		
Status	Disabled	Authorized	N/A
Control Mode	<input type="text" value="Force-Authorized"/>	Operation Mode	<input type="text" value="Single-Host"/>
Max Count (1-1024)	<input type="text" value="5"/>	Max Request (1-10)	<input type="text" value="2"/>
Quiet Period (1-65535)	<input type="text" value="60"/> sec	Tx Period (1-65535)	<input type="text" value="30"/> sec
Supplicant Timeout (1-65535)	<input type="text" value="30"/> sec	Server Timeout	<input type="text" value="0"/> sec
Re-authentication Status	<input type="checkbox"/> Enabled	Re-authentication Period (1-65535)	<input type="text" value="3600"/> sec
Re-authentication Max Retries (1-10)	<input type="text" value="2"/>		
Authentication Fail Action	<input type="text" value="Block Traffic"/>	Guest VLAN	<input type="text" value="0"/>
<input type="button" value="Apply"/> <input type="button" value="Revert"/>			

4.7.3.3 Statistics

Security > 802.1x > Statistics page is used to display the statistics of 802.1x.

Statistics			
Security > 802.1X > Statistics			
Port	<input type="text" value="1"/>		
Port Authentication Authenticator Statistics			
Rx EAPOL Start	0	Rx EAP Resp/Id	0
Rx EAPOL Logoff	0	Rx EAP Resp/Oth	0
Rx EAPOL Invalid	0	Rx EAP LenError	0
Rx EAPOL Total	0	Tx EAP Req/Id	0
Rx Last EAPOLVer	0	Tx EAP Req/Oth	0
Rx Last EAPOL Src	00-00-00-00-00-00	Tx EAPOL Total	0
<input type="button" value="Refresh"/>			

4.7.4 MAC Authentication

Overview of MAC-based Authentication

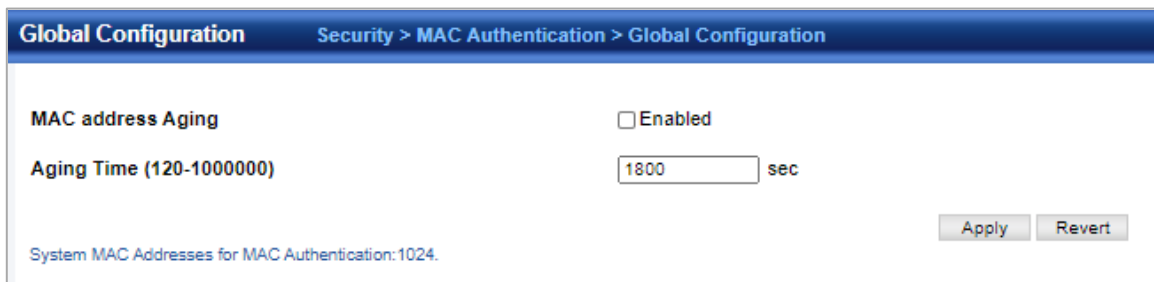
Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by 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.

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.

4.7.4.1 Global Configuration

Security > MAC Authentication > Global Configuration page is used to configure MAC Authentication global.



Global Configuration Security > MAC Authentication > Global Configuration

MAC address Aging Enabled

Aging Time (120-1000000) sec

System MAC Addresses for MAC Authentication: 1024.

4.7.4.2 Interface Configuration

Security > MAC Authentication > Interface Configuration page is used to configure interface.

Interface Configuration Security > MAC Authentication > Interface Configuration

Port List Total: 28

Port	Status	Authentication Fail Action	MAC Filter ID (1-64)
1	<input type="checkbox"/> Enabled	Block ▼	<input type="checkbox"/> <input style="width: 40px;" type="text"/>
2	<input type="checkbox"/> Enabled	Block ▼	<input type="checkbox"/> <input style="width: 40px;" type="text"/>
3	<input type="checkbox"/> Enabled	Block ▼	<input type="checkbox"/> <input style="width: 40px;" type="text"/>
4	<input type="checkbox"/> Enabled	Block ▼	<input type="checkbox"/> <input style="width: 40px;" type="text"/>
5	<input type="checkbox"/> Enabled	Block ▼	<input type="checkbox"/> <input style="width: 40px;" type="text"/>
6	<input type="checkbox"/> Enabled	Block ▼	<input type="checkbox"/> <input style="width: 40px;" type="text"/>
7	<input type="checkbox"/> Enabled	Block ▼	<input type="checkbox"/> <input style="width: 40px;" type="text"/>
8	<input type="checkbox"/> Enabled	Block ▼	<input type="checkbox"/> <input style="width: 40px;" type="text"/>
9	<input type="checkbox"/> Enabled	Block ▼	<input type="checkbox"/> <input style="width: 40px;" type="text"/>
10	<input type="checkbox"/> Enabled	Block ▼	<input type="checkbox"/> <input style="width: 40px;" type="text"/>

4.7.4.3 MAC Filter

Security > MAC Authentication > MAC Filter page is used to configure Mac Filter.

MAC Filter Security > MAC Authentication > MAC Filter

MAC Filter List Total: 1

	Filter ID	MAC Address	MAC Address Mask
<input type="checkbox"/>	12	11-11-11-12-11-12	FF-FF-FF-FF-FF-FF

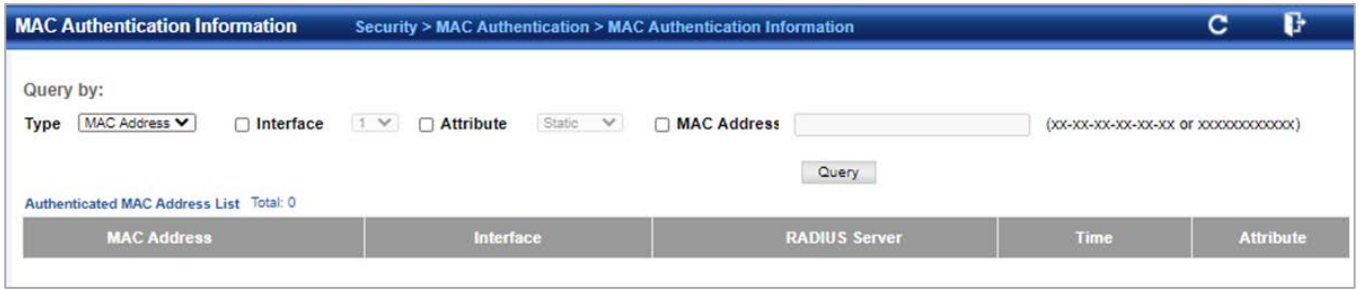
Filter ID (1-64)

MAC Address (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)

MAC Address Mask (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)

4.7.4.4 MAC Authentication Information

Security > MAC Authentication > MAC Authentication Information page is used to show information of MAC Authentication.

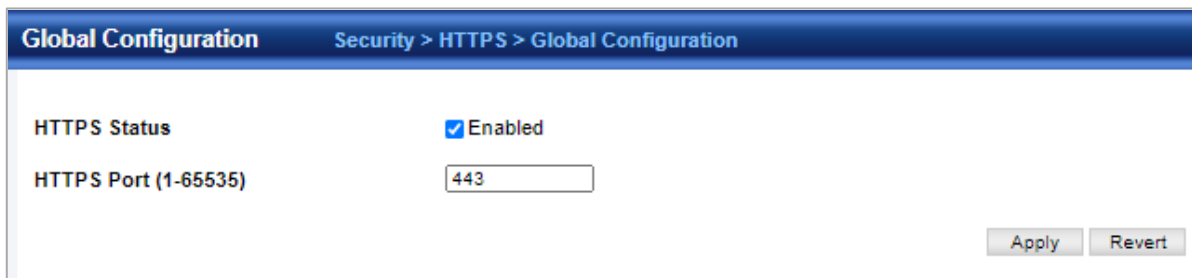


The screenshot shows the 'MAC Authentication Information' page. At the top, there is a breadcrumb trail: 'Security > MAC Authentication > MAC Authentication Information'. Below this, there is a 'Query by:' section with several options: 'Type' (set to 'MAC Address'), 'Interface' (set to '1'), 'Attribute' (set to 'Static'), and 'MAC Address' (with a text input field and a placeholder '(xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)'). A 'Query' button is located below these options. Below the query section, it says 'Authenticated MAC Address List Total: 0'. At the bottom, there is a table header with columns: 'MAC Address', 'Interface', 'RADIUS Server', 'Time', and 'Attribute'.

4.7.5 HTTPS

4.7.5.1 Global Configuration

Security > HTTPS > Global Configuration page is used to enable or disable HTTPS and specify the UDP port used for this service.



The screenshot shows the 'Global Configuration' page for HTTPS. The breadcrumb trail is 'Security > HTTPS > Global Configuration'. There are two main settings: 'HTTPS Status' which is set to 'Enabled' with a checked checkbox, and 'HTTPS Port (1-65535)' which has a text input field containing '443'. At the bottom right, there are 'Apply' and 'Revert' buttons.

- ◆ **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)
- ◆ **HTTPS Port** – Specifies the UDP port number used for HTTPS connection to the switch's web interface. (Default: Port 443)

4.7.5.2 Update Certificate

Security > HTTPS > Copy Certificate page is used to replace the default secure-site certificate.



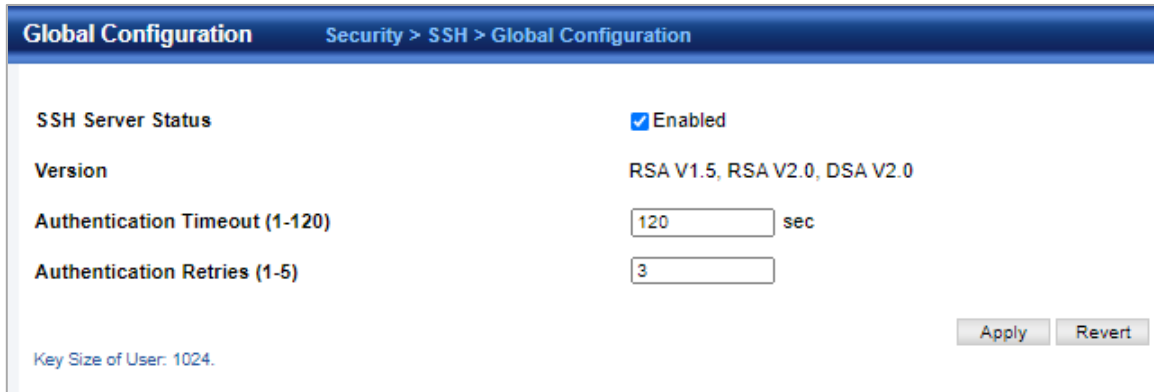
The screenshot shows the 'Update Certificate' page. The breadcrumb trail is 'Security > HTTPS > Update Certificate'. There are five text input fields: 'TFTP Server IP Address', 'Certificate Source File Name', 'Private Key Source File Name', 'Private Password', and 'Confirm Password'. At the bottom right, there are 'Apply' and 'Revert' buttons. At the bottom left, there is a 'Delete' button and a link: 'Click this button to delete current certificate.'

- ◆ **TFTP Server IP Address** – IP address of TFTP server which contains the certificate file.
- ◆ **Certificate Source File Name** – Name of certificate file stored on the TFTP server.
- ◆ **Private Key Source File Name** – Name of private key file stored on the TFTP server.
- ◆ **Private Password** – Password stored in the private key file. This password is used to verify authorization for certificate use, and is verified when downloading the certificate to the switch.
- ◆ **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not download the certificate if these two fields do not match.

4.7.6 SSH

4.7.6.1 Global Configuration

Security > SSH > Global Configuration page is used to enable the SSH server and configure basic settings for authentication.



- ◆ **SSH Server Status** – Allows you to enable/disable the SSH server on the switch. (Default: Disabled)
- ◆ **Version** – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.
- ◆ **Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1-120 seconds; Default: 120 seconds)
- ◆ **Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)
 - The host key is shared with the SSH client, and is fixed at 1024 bits.

4.7.6.2 Key of Switch

Security > SSH > Key of Switch page is used to generate a host public/private key pair used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch.



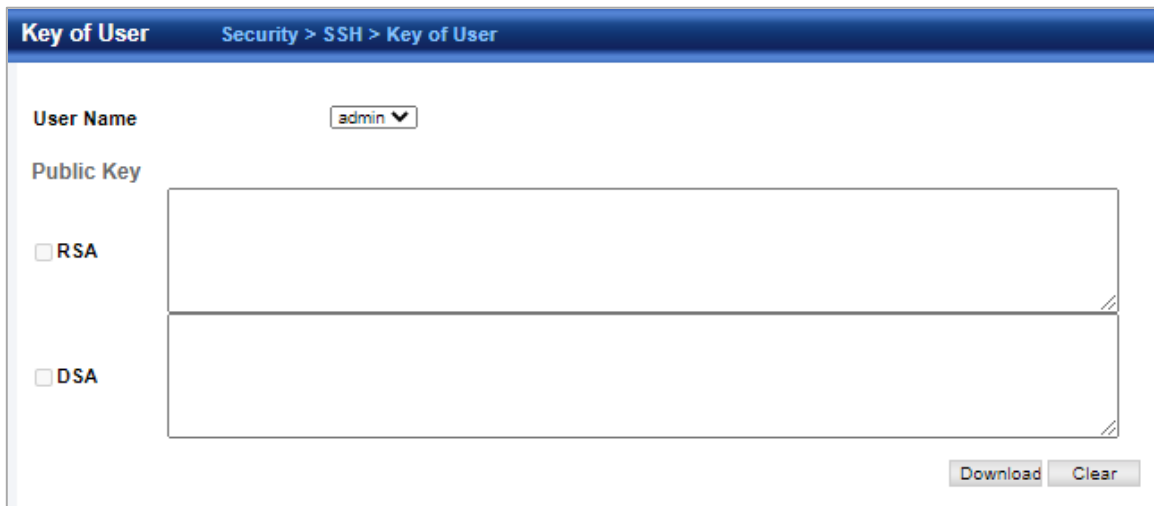
- ◆ **Host-Key Type** – The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA (Version 1), DSA (Version 2), Both; Default: Both)

The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

- ◆ **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory) to flash memory. Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair. (Default: Disabled)

4.7.6.3 Key of User

Security > SSH > Key of User page is used to upload a user's public key to the switch. This public key must be stored on the switch for the user to be able to log in using the public key authentication mechanism. If the user's public key does not exist on the switch, SSH will revert to the interactive password authentication mechanism to complete authentication.



- ◆ **User Name** – This drop-down box selects the user who's public key you wish to manage. Note that you must first create users on the User Accounts page.
- ◆ **User Key Type** – The type of public key to upload.
 - RSA: The switch accepts a RSA version 1 encrypted public key.
 - DSA: The switch accepts a DSA version 2 encrypted public key. The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption. The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.
- ◆ **TFTP Server IP Address** – The IP address of the TFTP server that contains the public key file you wish to import.
- ◆ **Source File Name** – The public key file to upload.

4.7.7 Port Security

Port Security allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Port Security 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 depending on violation mode.

Security > Port Security page is used to configure the maximum number of device MAC addresses that can be learned by a switch port, stored in the address table, and authorized to access the network.

Port Security
Security > Port Security

Port Security List Total: 26

Port	Status	Max MAC Count (0-1024)	Current MAC Count	Action for unthorization address
1	<input type="checkbox"/> Enabled	<input type="text" value="0"/>	0	None ▼
2	<input type="checkbox"/> Enabled	<input type="text" value="0"/>	0	None ▼
3	<input type="checkbox"/> Enabled	<input type="text" value="0"/>	0	None ▼
4	<input type="checkbox"/> Enabled	<input type="text" value="0"/>	0	None ▼
5	<input type="checkbox"/> Enabled	<input type="text" value="0"/>	0	None ▼
6	<input type="checkbox"/> Enabled	<input type="text" value="0"/>	0	None ▼
7	<input type="checkbox"/> Enabled	<input type="text" value="0"/>	0	None ▼
8	<input type="checkbox"/> Enabled	<input type="text" value="0"/>	0	None ▼
9	<input type="checkbox"/> Enabled	<input type="text" value="0"/>	0	None ▼
10	<input type="checkbox"/> Enabled	<input type="text" value="0"/>	0	None ▼

◆ **Port** – Port number.

◆ **Status** – Enables or disables port security on an interface. (Default: Disabled)

◆ **Port Status** – The operational status:

- Secure/Down – Port security is disabled.
- Secure/Up – Port security is enabled.
- Shutdown – Port is shut down due to a response to a port security violation.

◆ **Action for authorization address** – Indicates the action to be taken when a port security violation is detected:

- **None:** No action should be taken. (This is the default.)
- **Trap:** Send an SNMP trap message.
- **Shutdown:** Disable the port.
- **Trap and Shutdown:** Send an SNMP trap message and disable the port.

◆ **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled) The maximum address count is effective when port security is enabled or disabled.

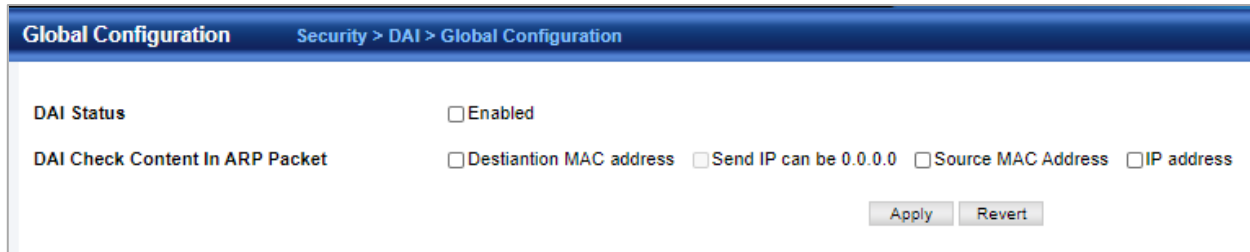
◆ **Current MAC Count** – The number of MAC addresses currently associated with this interface.

4.7.8 DAI – Dynamic ARP Inspection

Dynamic 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.

4.7.8.1 Global Configuration

The Security > DAI > Global Configuration page is used to enable ARP inspection globally for the switch, to validate address information in each packet, and configure logging.



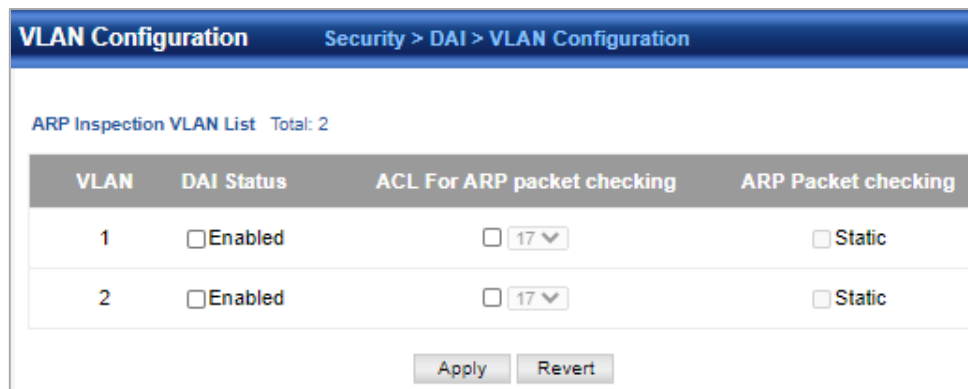
◆ **DAI Status** – Enables ARP Inspection globally. (Default: Disabled)

◆ **DAI Check Content In ARP Packet** – Enables extended ARP Inspection Validation if any of the following options are enabled. (Default: Disabled)

- **Destination MAC address** – Validates the destination MAC address in the Ethernet header against the target MAC address in the body of ARP responses.
- **IP address** – Checks the ARP body for invalid and unexpected IP addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.
- **Source MAC Address** – Validates the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.

4.7.8.2 VLAN Configuration

The Security > DAI > VLAN Configuration page is used to enable ARP inspection for any VLAN and to specify the ARP ACL to use.



VLAN	DAI Status	ACL For ARP packet checking	ARP Packet checking
1	<input type="checkbox"/> Enabled	<input type="checkbox"/> 17	<input type="checkbox"/> Static
2	<input type="checkbox"/> Enabled	<input type="checkbox"/> 17	<input type="checkbox"/> Static

◆ **ARP Inspection VLAN ID** – Selects any configured VLAN. (Default: 1)

◆ **ARP Inspection VLAN Status** – Enables ARP Inspection for the selected VLAN. (Default: Disabled)

◆ **ARP Inspection ACL Name**

- **ARP ACL** – Allows selection of any configured ARP ACLs. (Default: None)
- **Static** – When an ARP ACL is selected, and static mode is also selected, the switch only performs ARP Inspection and bypasses validation against the DHCP Snooping Bindings database. When an ARP ACL is selected, but static mode is not selected, the switch first performs ARP Inspection and then validation against the DHCP Snooping Bindings database. (Default: Disabled)

4.7.8.3 Interface Configuration

The Security > DAI > Interface Configuration page is used to specify the ports that require ARP inspection, and to adjust the packet inspection rate.

Interface Configuration
Security > DAI > Interface Configuration

Interface Port Group

Port Configuration List Total: 26

Port	Mode	Packet Rate Limit for Un-trust Mode (0-2048 pps)
1	Un-trust ▼	<input checked="" type="checkbox"/> 15
2	Un-trust ▼	<input checked="" type="checkbox"/> 15
3	Un-trust ▼	<input checked="" type="checkbox"/> 15
4	Un-trust ▼	<input checked="" type="checkbox"/> 15
5	Un-trust ▼	<input checked="" type="checkbox"/> 15
6	Un-trust ▼	<input checked="" type="checkbox"/> 15
7	Un-trust ▼	<input checked="" type="checkbox"/> 15
8	Un-trust ▼	<input checked="" type="checkbox"/> 15
9	Un-trust ▼	<input checked="" type="checkbox"/> 15
10	Un-trust ▼	<input checked="" type="checkbox"/> 15

- ◆ **Port** – Port or trunk identifier.
- ◆ **Mode** – Configures the port as **trusted** or **untrusted**. (Default: Untrusted)
 By default, all untrusted ports are subject to ARP packet rate limiting, and all trusted ports are exempt from ARP packet rate limiting. Packets arriving on trusted interfaces bypass all ARP Inspection and ARP Inspection Validation checks and will always be forwarded, while those arriving on untrusted interfaces are subject to all configured ARP inspection tests.
- ◆ **Packet Rate Limit for Un-trust Mode (0-2048 pps)** – Sets the maximum number of ARP packets that can be processed by CPU per second on trusted or untrusted ports. (Range: 0-2048; Default: 15)
 Setting the rate limit to “0” means that there is no restriction on the number of ARP packets that can be processed by the CPU. The switch will drop all ARP packets received on a port which exceeds the configured ARP-packets-per-second rate limit.

4.7.8.4 Statistics

The Security > DAI > Statistics page is used to display statistics about the number of ARP packets processed, or dropped for various reasons.

Statistics		Security > DAI > Statistics	
ARP packets dropped by additional validation (Src-MAC)			0
Received ARP packets before ARP inspection rate limit			0
Total ARP packets processed by ARP inspection			0
Dropped ARP packets in processing ARP inspection rate limit			0
ARP packets dropped by ARP ACLs			0
ARP packets dropped by additional validation (IP)			0
ARP packets dropped by DHCP snooping			0
ARP packets dropped by additional validation (Dst-MAC)			0

4.7.8.5 Log

The Security > DAI > Log page is used to show information about entries stored in the log, including the associated VLAN, port, and address components.

Log		Security > DAI > Log				
ARP Inspection Log List Total: 0						
VLAN ID	Port	Src. IP Address	Dst. IP Address	Src. MAC Address	Dst. MAC Address	

4.7.9 Login IP Management

4.7.9.1 Login IP Management

The Security > Login IP Management page is used to create a list of up to 15 IP addresses or IP address groups that are allowed management access to the switch through the web interface, SNMP, or Telnet.



Login IP Management Security > Login IP Management

Login Type Web SNMP Telnet

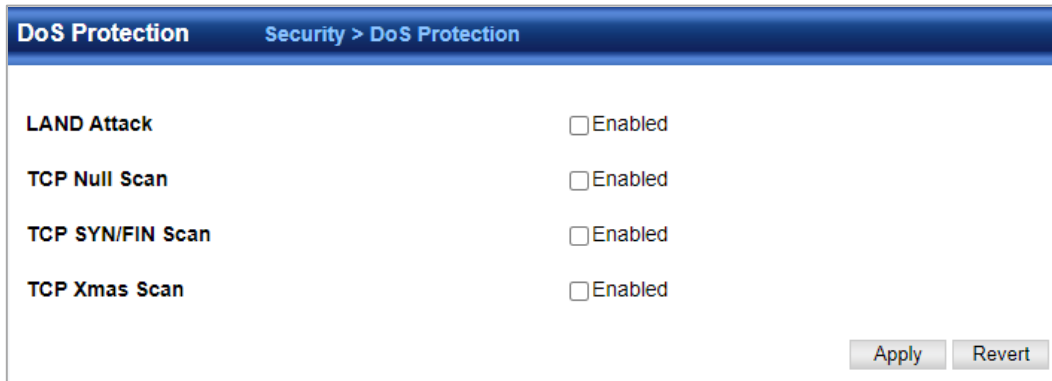
Total: 1

<input type="checkbox"/>	Start IP Address	End IP Address
<input type="checkbox"/>	192.168.1.1	192.168.1.253

- ◆ **Login Type**
 - **Web** – Configures IP address(es) for the web group.
 - **SNMP** – Configures IP address(es) for the SNMP group.
 - **Telnet** – Configures IP address(es) for the Telnet group.
- ◆ **Start IP Address** – A single IP address, or the starting address of a range.
- ◆ **End IP Address** – The end address of a range.

4.7.10 DoS Protection

The Security > DoS Protection page is used to protect against denial-of-service (DoS) attacks. A DoS attack is an attempt to block the services provided by a computer or network resource.



DoS Protection	
Security > DoS Protection	
LAND Attack	<input type="checkbox"/> Enabled
TCP Null Scan	<input type="checkbox"/> Enabled
TCP SYN/FIN Scan	<input type="checkbox"/> Enabled
TCP Xmas Scan	<input type="checkbox"/> Enabled
<input type="button" value="Apply"/> <input type="button" value="Revert"/>	

- ◆ **Echo/Chargen Attack** – Attacks in which the echo service repeats anything sent to it, and the chargen (character generator) service generates a continuous stream of data. When used together, they create an infinite loop and result in a denial-of-service. (Default: Disabled)
- ◆ Echo/Chargen Attack Rate – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)
- ◆ **Smurf Attack** – Attacks in which a perpetrator generates a large amount of spoofed ICMP Echo Request traffic to the broadcast destination IP address (255.255.255.255), all of which uses a spoofed source address of the intended victim. The victim should crash due to the many interrupts required to send ICMP Echo response packets. (Default: Enabled)
- ◆ **TCP Flooding Attack** – Attacks in which a perpetrator sends a succession of TCP SYN requests (with or without a spoofed-Source IP) to a target and never returns ACK packets. These half-open connections will bind resources on the target, and no new connections can be made, resulting in a denial of service. (Default: Disabled)
- ◆ **TCP Flooding Attack Rate** – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)
- ◆ **TCP Null Scan** – A TCP NULL scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and no flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP NULL scan. (Default: Enabled)
- ◆ **TCP-SYN/FIN Scan** – A TCP SYN/FIN scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain SYN (synchronize) and FIN (finish) flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP SYN FIN scan. (Default: Enabled)
- ◆ **TCP Xmas Scan** – A so-called TCP XMAS scan message is used to identify listening TCP ports. This scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and the URG, PSH and FIN flags. If the target's TCP port is closed, the target replies with a TCP RST packet. If the target TCP port is open, it simply discards the TCP XMAS scan. (Default: Enabled)
- ◆ **UDP Flooding Attack** – Attacks in which a perpetrator sends a large number of UDP packets (with or without a spoofed-Source IP) to random ports on a remote host. The target will determine that application is listening at that port, and reply with an ICMP Destination Unreachable packet. It will be forced to send many ICMP packets, eventually leading it to be unreachable by other clients. (Default: Disabled)
- ◆ **UDP Flooding Attack Rate** – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)
- ◆ **WinNuke Attack** – Attacks in which affected the Microsoft Windows 3.1x/95/NT operating systems. In this type of attack, the perpetrator sends the string of OOB out-of-band (OOB) packets contained a TCP URG flag to the target computer on TCP port 139 (NetBIOS), casing it to lock up and display a "Blue Screen of Death." This did not cause any damage to, or change data on, the computer's hard disk, but any unsaved data would be lost. Microsoft made patches to prevent the WinNuke attack, but the OOB packets. (Default: Disabled)
- ◆ **WinNuke Attack Rate** – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)

4.7.11 IPv4 DHCP Snooping

4.7.11.1 Global Configuration

Security > IPv4 DHCP Snooping > Global Configuration page is used to enable DHCP Snooping globally on the switch, or to configure MAC Address Verification.

Global Configuration
Security > IPv4 DHCP Snooping > Global Configuration

DHCP Snooping Status Enabled

DHCP Snooping MAC-Address Checking Enabled

DHCP Snooping Rate Limit (pkt/sec)

Option82 Status Enabled

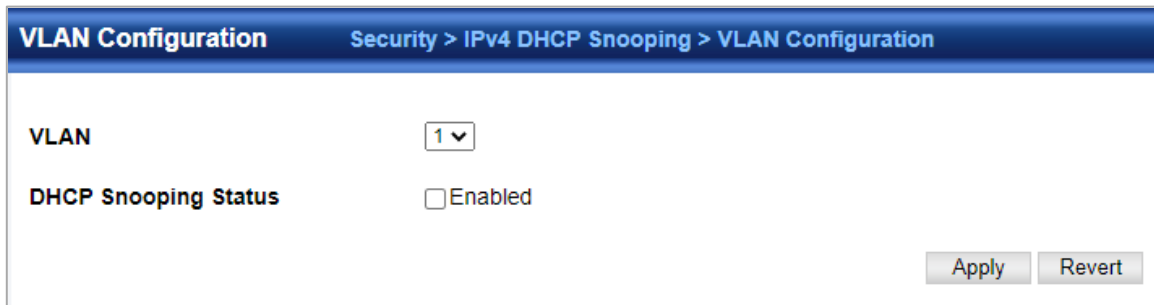
Option82 Remote ID MAC Address (Hex Encoded) ▼

Action for existed Option 82 Entry in DHCP packet Replace ▼

- ◆ **DHCP Snooping Status** – Enables DHCP snooping globally. (Default: Disabled)
- ◆ **DHCP Snooping MAC-Address Verification** – Enables or disables MAC address verification. If the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped. (Default: Enabled)
- ◆ **DHCP Snooping Rate Limit**– Sets the maximum number of DHCP packets that can be trapped by the switch for DHCP snooping. (Range: 1-2048 packets/ second)
- ◆ **DHCP Snooping Information Option Status** – Enables or disables DHCP Option 82 information relay. (Default: Disabled)
- ◆ **DHCP Snooping Information Option Sub-option Format** – Enables or disables use of sub-type and sub-length fields in circuit-ID (CID) and remote-ID (RID) in Option 82 information.
- ◆ **DHCP Snooping Information Option Remote ID** – Specifies the MAC address, IP address, or arbitrary identifier of the requesting device (i.e., the switch in this context).
 - **MAC Address** – Inserts a MAC address in the remote ID sub-option for the DHCP snooping agent (i.e., the MAC address of the switch's CPU). This attribute can be encoded in Hexadecimal or ASCII.
 - **IP Address** – Inserts an IP address in the remote ID sub-option for the DHCP snooping agent (i.e., the IP address of the management interface). This attribute can be encoded in Hexadecimal or ASCII.
 - **string** - An arbitrary string inserted into the remote identifier field. (Range: 1-32 characters)
- ◆ **DHCP Snooping Information Option Remote ID TR101 VLAN Field** – Adds “:VLAN” in TR101 field for untagged packets. The format for TR101 option 82 is: “<IP> eth <SID>/<PORT>[:<VLAN>]”. Note that the SID (Switch ID) is always 0. By default the PVID is added to the end of the TR101 field for untagged packets. For tagged packets, the VLAN ID is always added.
- ◆ **DHCP Snooping Information Option Policy** – Specifies how to handle DHCP client request packets which already contain Option 82 information.
 - **Drop** – Drops the client's request packet instead of relaying it.
 - **Keep** – Retains the Option 82 information in the client request, and forwards the packets to trusted ports.
 - **Replace** – Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information about the relay agent itself, inserts the relay agent's address (when DHCP snooping is enabled), and forwards the packets to trusted ports. (This is the default policy.)

4.7.11.2 VLAN Configuration

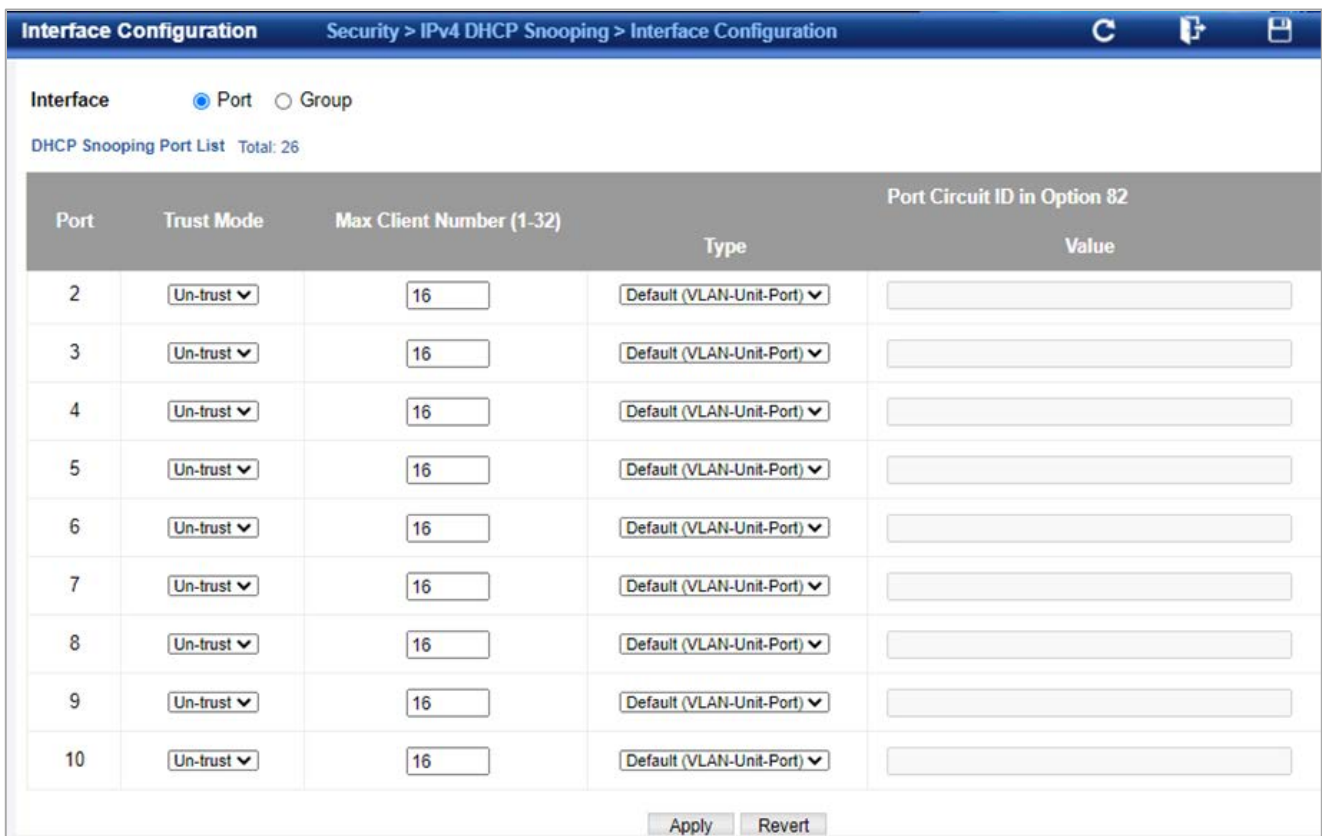
Security > IPv4 DHCP Snooping > VLAN Configuration page is used to enable or disable DHCP snooping on specific VLANs.



- ◆ **VLAN** – ID of a configured VLAN. (Range: 1-4093)
- ◆ **DHCP Snooping Status** – Enables or disables DHCP snooping for the selected VLAN. When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN. (Default: Disabled)

4.7.11.3 Interface Configuration

Security > IPv4 DHCP Snooping > Interface Configuration page is used to configure switch ports as trusted or un-trusted.



Port	Trust Mode	Max Client Number (1-32)	Type	Port Circuit ID in Option 82
2	Un-trust	16	Default (VLAN-Unit-Port)	
3	Un-trust	16	Default (VLAN-Unit-Port)	
4	Un-trust	16	Default (VLAN-Unit-Port)	
5	Un-trust	16	Default (VLAN-Unit-Port)	
6	Un-trust	16	Default (VLAN-Unit-Port)	
7	Un-trust	16	Default (VLAN-Unit-Port)	
8	Un-trust	16	Default (VLAN-Unit-Port)	
9	Un-trust	16	Default (VLAN-Unit-Port)	
10	Un-trust	16	Default (VLAN-Unit-Port)	

- ◆ **Trust Status** – Enables or disables a port as trusted. (Default: Disabled)
- ◆ **Circuit ID** – Specifies DHCP Option 82 circuit ID suboption information.
 - **Mode** – Specifies the default string “VLAN-Unit-Port” or an arbitrary string. (Default: VLAN-Unit-Port)
 - **Value** – An arbitrary string inserted into the circuit identifier field. (Range: 1-32 characters)

4.7.11.4 Legal Client Table

Security > IPv4 DHCP Snooping > Legal Client Table page is used to display entries in the binding table.

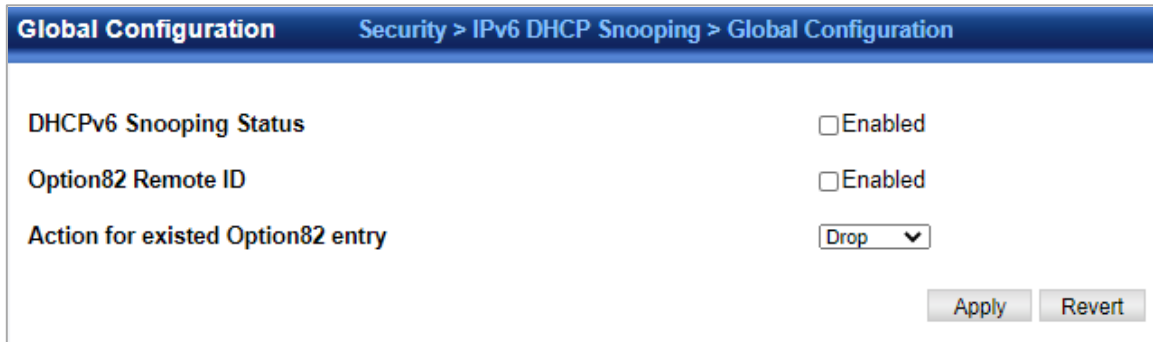
Legal Client Table		Security > IPv4 DHCP Snooping > Legal Client Table			
Legal DHCP Client List Total: 0					
MAC Address	IP Address	Lease Time (seconds)	Type	VLAN	Interface

- ◆ **MAC Address** – Physical address associated with the entry.
- ◆ **IP Address** – IP address corresponding to the client.
- ◆ **Lease Time** – The time for which this IP address is leased to the client.
- ◆ **Type** – Entry types include:
 - **DHCP-Snooping** – Dynamically snooped.
 - **Static-DHCPSNP** – Statically configured.
- ◆ **VLAN** – VLAN to which this entry is bound.
- ◆ **Interface** – Port or group to which this entry is bound.
- ◆ **Store** – Writes all dynamically learned snooping entries to flash memory. This function can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.
- ◆ **Clear** – Removes all dynamically learned snooping entries from flash memory.

4.7.12 IPv6 DHCP Snooping

4.7.12.1 Global Configuration

Security > IPv6 DHCP Snooping > Global Configuration page is used to enable DHCPv6 Snooping globally on the switch, or to configure MAC Address Verification.



◆ **DHCPv6 Snooping Status**—Enables DHCPv6 snooping globally.(Default: Disabled)

◆ **DHCPv6 Snooping Option Remote ID**—Enables the insertion of remote-id option 37 information into DHCPv6 client messages. Remote-id option information such as the port attached to the client, DUID, and VLAN ID is used by the DHCPv6 server to assign pre-assigned configuration data specific to the DHCPv6 client. (Default: Disabled)

- DHCPv6 provides a relay mechanism for sending information about the switch and its DHCPv6 clients to the DHCPv6 server. Known as DHCPv6 Option 37, it allows compatible DHCPv6 servers to use the information when assigning IP addresses, or to set other services or policies for clients.
- When DHCPv6 Snooping Information Option 37 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCPv6 request packets forwarded by the switch and in reply packets sent back from the DHCPv6 server.
- When the DHCPv6 Snooping Option 37 is enabled, clients can be identified by the switch port to which they are connected rather than just their MAC address. DHCPv6 client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.
- DHCPv6 snooping must be enabled for the DHCPv6 Option 37 information to be inserted into packets. When enabled, the switch will either drop, keep or remove option 37 information in incoming DHCPv6 packets. Packets are processed as follows:
 - If an incoming packet is a DHCPv6 request packet with option 37 information, it will modify the option 37 information according to the settings specified.
 - If an incoming packet is a DHCPv6 request packet without option 37 information, enabling the DHCPv6 snooping information option will add option 37 information to the packet.
 - If an incoming packet is a DHCPv6 reply packet with option 37 information, enabling the DHCPv6 snooping information option will remove option 37 information from the packet.
 - When this switch inserts Option 37 information in DHCPv6 client request packets, the switch' s MAC address (hexadecimal) is used for the remote ID.

◆ **DHCPv6 Snooping Option Policy** –Sets the remote-id option policy for DHCPv6 client packets that include Option 37 information. When the switch receives DHCPv6 packets from clients that already include DHCP Option 37 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCPv6 packets, keep the existing information, or replace it with the switch' s relay agent information.

- **Drop** —Drops the client's request packet instead of relaying it (This is the default policy).
 - **Keep** —Retains the Option 82 information in the client request, and forwards the packets to trusted ports.
 - **Replace** —Replaces the Option 37 remote-ID in the client's request with the relay agent's remote-ID (when DHCPv6 snooping is enabled), and forwards the packets to trusted ports.

4.7.12.2 VLAN Configuration

Security > IPv6 DHCP Snooping > VLAN Configuration page is used to enable or disable DHCPv6 snooping on specific VLANs.

VLAN Configuration Security > IPv6 DHCP Snooping > VLAN Configuration

DHCPv6 Snooping VLAN List Total: 6

<input type="checkbox"/>	VLAN
<input type="checkbox"/>	5
<input type="checkbox"/>	6
<input type="checkbox"/>	7
<input type="checkbox"/>	8
<input type="checkbox"/>	9
<input type="checkbox"/>	10

- ◆ **VLAN**—ID of a configured VLAN. (Range: 1-4094)

4.7.12.3 Interface Configuration

Security > IPv6 DHCP Snooping > Interface Configuration page is used to configure switch interfaces as trusted or untrusted, and set the maximum number of entries which can be stored in the binding database for an interface.

Interface Configuration Security > IPv6 DHCP Snooping > Interface Configuration

DHCPv6 Snooping Interface List Total: 26

Interface	Trust Mode	Max Clinet Number (1 - 5)	
Eth 1/1	Un-trust ▼	5	
Eth 1/2	Un-trust ▼	5	
Eth 1/3	Un-trust ▼	5	
Eth 1/4	Un-trust ▼	5	
Eth 1/5	Un-trust ▼	5	
Eth 1/6	Un-trust ▼	5	
Eth 1/7	Un-trust ▼	5	
Eth 1/8	Un-trust ▼	5	
Eth 1/9	Un-trust ▼	5	
Eth 1/10	Un-trust ▼	5	

- ◆ **Interface**—Port or group identifier.
- ◆ **Trust Status** —Enables or disables an interface as trusted. (Default: Disabled)
- ◆ **Max Binding** —Sets the maximum number of entries which can be stored in the binding database for an interface. (Range: 1-5; Default: 5)
- ◆ **Current Binding** —Shows the maximum number of entries which can be stored in the binding database for an interface.

4.7.12.4 Legal Client Table

Security > IPv6 DHCP Snooping > Legal Client Table page is used to display entries in the binding table.

Legal Client Table Security > IPv6 DHCP Snooping > Legal Client Table

Legal Client List Total: 0

Link-layer Address	IPv6 Address	Lifetime	VLAN	Interface	Type

- ◆ **Link-layer Address**—IPv6 link-layer address associated with the entry.
- ◆ **IPv6 Address**—IPv6 address corresponding to the client.
- ◆ **Lifetime**—The time (number of seconds) for which this IPv6 address is leased to the client.
- ◆ **VLAN**—VLAN to which this entry is bound.
- ◆ **Interface**—Port or group to which this entry is bound.
- ◆ **Type**—Entry types include:
 - **NA**—Non-temporary address.
 - **TA**—Temporary address.
- ◆ **Clear**—Removes all dynamically learned snooping entries from RAM.

4.7.13 IPv4 Source Guard

4.7.13.1 Interface Configuration

Security > IP Source Guard > Interface Configuration page is used to set the filtering type based on source IP address, or source IP address and MAC address pairs.

Interface Configuration
Security > IPv4 Source Guard > Interface Configuration

Port Configuration List Total: 26

Port	Chcking Mode	Max Static Table Entry (1-32)
1	Disable ▼	16
2	Disable ▼	16
3	Disable ▼	16
4	Disable ▼	16
5	Disable ▼	16
6	Disable ▼	16
7	Disable ▼	16
8	Disable ▼	16
9	Disable ▼	16
10	Disable ▼	16

◆ **Checking Mode** – Configures the switch to filter inbound traffic based source IP address, or source IP address and corresponding MAC address. (Default: None)

- **None** – Disables IP source guard filtering on the port.
- **Source IP** – Enables traffic filtering based on IP addresses stored in the binding table.
- **Source IP and MAC** – Enables traffic filtering based on IP addresses and corresponding MAC addresses stored in the binding table.

◆ **Max Static Table Entry** – The maximum number of entries that can be bound to an interface. (Range: 1-5; Default: 5) This parameter sets the maximum number of address entries that can be mapped to an interface in the binding table, including both

dynamic entries discovered by DHCP snooping and static entries set by IP source guard.

4.7.13.2 Static Table

Security > IPv4 Source Guard > Static Table page is used to bind a valid static IP source guard entry to a port in ACL mode.

Static Table Security > IPv4 Source Guard > Static Table				
Static IP Source Guard Table Total: 1				
<input type="checkbox"/>	MAC Address	IP Address	VLAN	Interface
<input type="checkbox"/>	00-00-00-00-00-01	10.0.0.1	5 - 10	Unit 1 / Port 24
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>				

- ◆ **Port**—The port to which a static entry is bound.
- ◆ **VLAN**—ID of a configured VLAN (Range: 1-4094)
- ◆ **MAC Address**—A valid unicast MAC address.
- ◆ **IP Address** —A valid unicast IP address, including classful types A, B or C.

4.7.13.3 Dynamic Binding

Security > IPv4 Source Guard > Dynamic Binding page is used to display the source-guard binding table for a selected interface.

Query by

Dynamic Binding Security > IPv4 Source Guard > Dynamic Binding				
Query by:				
<input type="checkbox"/> Port		<input type="text" value="1"/>		
<input type="checkbox"/> VLAN		<input type="text" value="1"/>		
<input type="checkbox"/> MAC Address		<input type="text"/>	(xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)	
<input type="checkbox"/> IP Address		<input type="text"/>		
<input type="button" value="Query"/>				
Dynamic Binding List Total: 0				
VLAN	MAC Address	Interface	IP Address	Type

- ◆ **Port** – A port on this switch.
- ◆ **VLAN** – ID of a configured VLAN (Range: 1-4093)
- ◆ **MAC Address** – A valid unicast MAC address.
- ◆ **IP Address** – A valid unicast IP address, including classful types A, B or C. Dynamic Binding List
- ◆ **VLAN** – VLAN to which this entry is bound.
- ◆ **MAC Address** – Physical address associated with the entry.
- ◆ **Interface** – Port to which this entry is bound.
- ◆ **IP Address** – IP address corresponding to the client.
- ◆ **Lease Time** – The time for which this IP address is leased to the client.

4.7.14 IPv6 Source Guard

4.7.14.1 Interface Configuration

Security > IPv6 Source Guard > Interface Configuration page is used to filter inbound traffic based on the source IPv6 address stored in the binding table.

Interface Configuration
Security > IPv6 Source Guard > Interface Configuration

Port Configuration List Total: 26

Port	Checking Mode	Max Static Table Entry (1-5)
1	Disabled ▼	5
2	Disabled ▼	5
3	Disabled ▼	5
4	Disabled ▼	5
5	Disabled ▼	5
6	Disabled ▼	5
7	Disabled ▼	5
8	Disabled ▼	5
9	Disabled ▼	5
10	Disabled ▼	5

- ◆ **Port**—Port identifier.
- ◆ **Filter Type**—Configures the switch to filter inbound traffic based on the following options. (Default: Disabled)
 - **Disabled**—Disables IPv6 source guard filtering on the port.
 - **Source IP**—Enables traffic filtering based on IPv6 global unicast source IPv6 addresses stored in the binding table.
- ◆ **Max Binding Entry**—The maximum number of entries that can be bound to an interface. (Range: 1-5; Default: 5)
 - This parameter sets the maximum number of IPv6 global unicast source IPv6 address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by ND snooping, DHCPv6 snooping .
 - IPv6 source guard maximum bindings must be set to a value higher than DHCPv6 snooping maximum bindings and ND snooping maximum bindings.
 - If IPv6 source guard, ND snooping, and DHCPv6 snooping are enabled on a port, the dynamic bindings used by ND snooping, DHCPv6 snooping, and IPv6 source guard static bindings cannot exceed the maximum allowed bindings set by this parameter. In other words, no new entries will be added to the IPv6 source guard binding table.
 - If IPv6 source guard is enabled on a port, and the maximum number of allowed bindings is changed to a lower value, precedence is given to deleting entries learned through DHCPv6 snooping, ND snooping, and then manually configured IPv6 source guard static bindings, until the number of entries in the binding table reaches the newly configured maximum number of allowed bindings.

4.7.14.2 Static Table

Use the Security > IPv6 Source Guard > Static Table page to bind a static address to a port. Table entries include a MAC address, IPv6 global unicast address, entry type (Static-IPv6-SG-Binding, Dynamic-ND-Binding, Dynamic-DHCPv6-Binding), VLAN identifier, and port identifier.

Static Table Security > IPv6 Source Guard > Static Table					
Static IPv6 Source Guard Table Total: 1					
<input type="checkbox"/>	VLAN	MAC Address	Interface	IPv6 Address	Type
<input type="checkbox"/>	1	00-00-00-00-00-02	Eth 1/1	2001:db8:2de::e13	Static
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>					

- ◆ **Port**—The port to which a static entry is bound.
- ◆ **VLAN**—ID of a configured VLAN (Range: 1-4094)
- ◆ **MAC Address**—A valid unicast MAC address.
- ◆ **IPv6 Address**—A valid global unicast IPv6 address. This address must be entered according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

4.7.14.3 Dynamic Binding

Security > IPv6 Source Guard > Dynamic Binding page is used to display the source-guard binding table for a selected interface. Query by

Dynamic Binding Security > IPv6 Source Guard > Dynamic Binding					
Query by:					
<input type="checkbox"/>	Port		1	▼	
<input type="checkbox"/>	VLAN		1	▼	
<input type="checkbox"/>	MAC Address	<input type="text"/>	(xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)		
<input type="checkbox"/>	IPv6 Address	<input type="text"/>			
					<input type="button" value="Query"/>
Dynamic Binding List Total: 0					
VLAN	MAC Address	Interface	IPv6 Address	Type	

- ◆ **Port**—A port on this switch.
- ◆ **VLAN**— ID of a configured VLAN (Range: 1-4094)
- ◆ **MAC Address**—A valid unicast MAC address.
- ◆ **IPv6 Address**—A valid global unicast IPv6 address. Dynamic Binding List
- ◆ **VLAN**—VLAN to which this entry is bound.
- ◆ **MAC Address** —Physical address associated with the entry.

- ◆ **Interface**—Port to which this entry is bound.
- ◆ **IPv6 Address**—IPv6 address corresponding to the client.
- ◆ **Type**—Shows the entry type:
 - **DHCP**—Dynamic DHCPv6 binding, stateful address.
 - **ND**—Dynamic Neighbor Discovery binding, stateless address.

4.7.15 Application Filter

Use the Security > Application Filter page to forward CDP or PVST packets.

Application Filter
Security > Application Filter

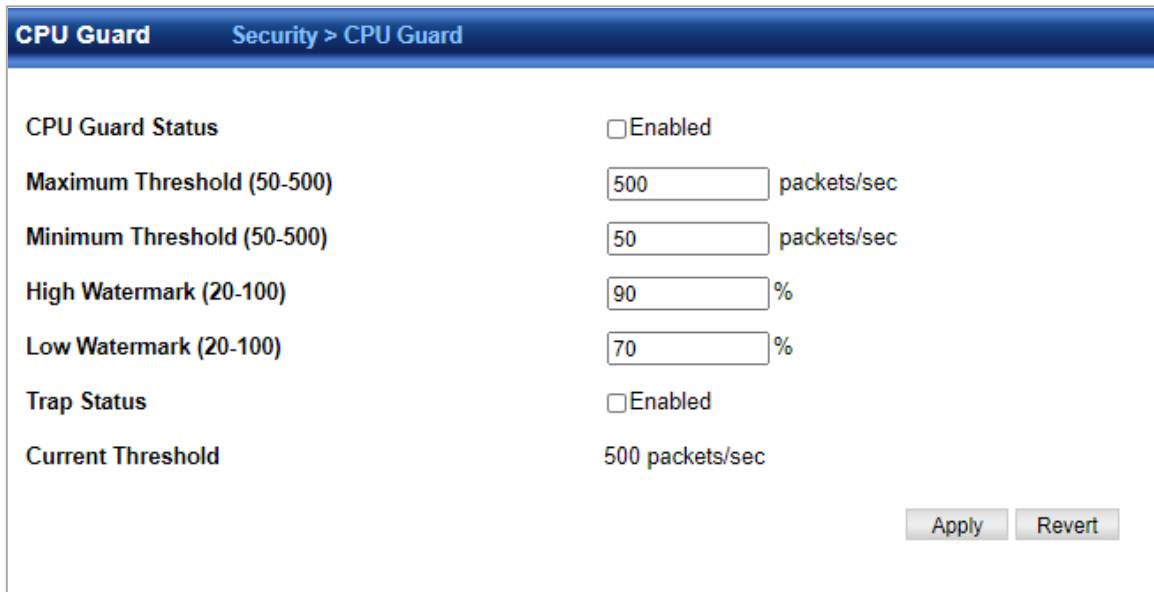
Application Filter List Total: 26

Port	CDP	PVST
1	Default ▼	Default ▼
2	Default ▼	Default ▼
3	Default ▼	Default ▼
4	Default ▼	Default ▼
5	Default ▼	Default ▼
6	Default ▼	Default ▼
7	Default ▼	Default ▼
8	Default ▼	Default ▼
9	Default ▼	Default ▼
10	Default ▼	Default ▼

- ◆ **Port**—Port identifier (Range: 1-26/28/52)
- ◆ **CDP**—Cisco Discovery Protocol
- ◆ **PVST**—Per-VLAN Spanning Tree

4.7.16 CPU Guard

Use the Security > CPU Guard page to set the CPU utilization high and low watermarks in percentage of CPU time utilized and the CPU high and low thresholds in the number of packets being processed per second.



CPU Guard	
Security > CPU Guard	
CPU Guard Status	<input type="checkbox"/> Enabled
Maximum Threshold (50-500)	500 packets/sec
Minimum Threshold (50-500)	50 packets/sec
High Watermark (20-100)	90 %
Low Watermark (20-100)	70 %
Trap Status	<input type="checkbox"/> Enabled
Current Threshold	500 packets/sec
<input type="button" value="Apply"/> <input type="button" value="Revert"/>	

- ◆ **CPU Guard Status**—Enables CPU Guard. (Default: Disabled)
- ◆ **High Watermark** —If the percentage of CPU usage time is higher than the high-watermark, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until usage time falls below the low watermark. (Range: 40-100 %; Default: 90 %)
- ◆ **Low Watermark**—If packet flow has been stopped after exceeding the high watermark, normal flow will be restored after usage falls beneath the low watermark. (Range: 40-100 %; Default: 70 %)
- ◆ **Maximum Threshold** —If the number of packets being processed by the CPU is higher than the maximum threshold, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until the number of packets being processed falls below the minimum threshold. (Range: 50-500 pps; Default: 500 pps)
- ◆ **Minimum Threshold**—If packet flow has been stopped after exceeding the maximum threshold, normal flow will be restored after usage falls beneath the minimum threshold. (Range: 50-500 pps; Default: 50 pps)
- ◆ **Trap Status** —If enabled, an alarm message will be generated when utilization exceeds the high watermark or exceeds the maximum threshold. (Default: Disabled) Once the high watermark is exceeded, utilization must drop beneath the low watermark before the alarm is terminated, and then exceed the high watermark again before another alarm is triggered. Once the maximum threshold is exceeded, utilization must drop beneath the minimum threshold before the alarm is terminated, and then exceed the maximum threshold again before another alarm is triggered.
- ◆ **Current Threshold**—Shows the configured threshold in packets per second.

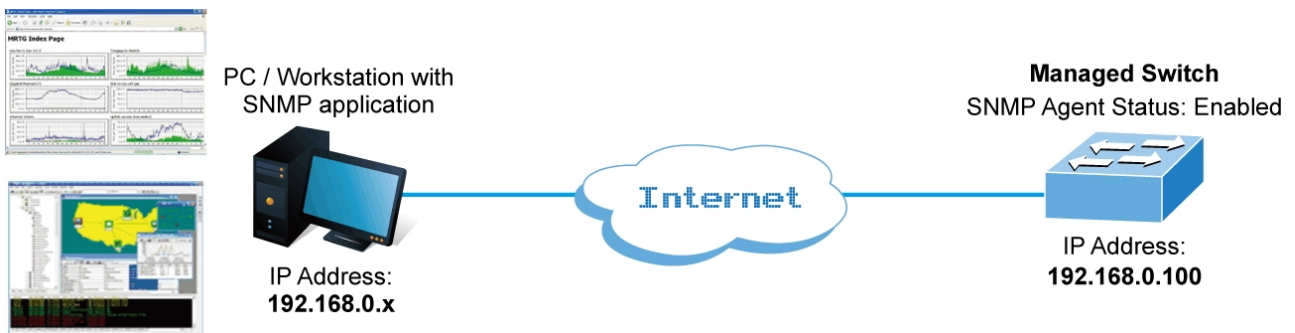
4.8 Device Management

4.8.1 SNMP

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.

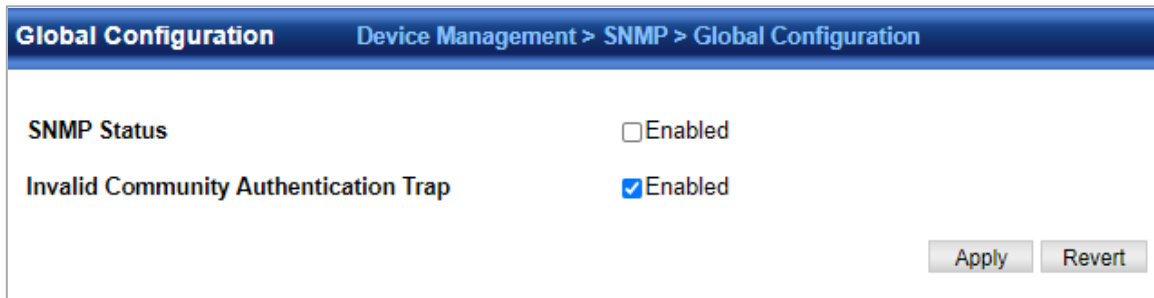
- **Get** -- Allows the NMS to retrieve an object instance from the agent.
- **Set** -- Allows the NMS to set values for object instances within an agent.
- **Trap** -- Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

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. An SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities.

4.8.1.1 Global Configuration

Device Management > SNMP > Global Configuration page is used to enable SNMPv3 service for all management clients (i.e., versions 1, 2c, 3), and to enable trap messages.



The screenshot shows the 'Global Configuration' page under 'Device Management > SNMP > Global Configuration'. It contains two configuration items:

- SNMP Status**: Enabled
- Invalid Community Authentication Trap**: Enabled

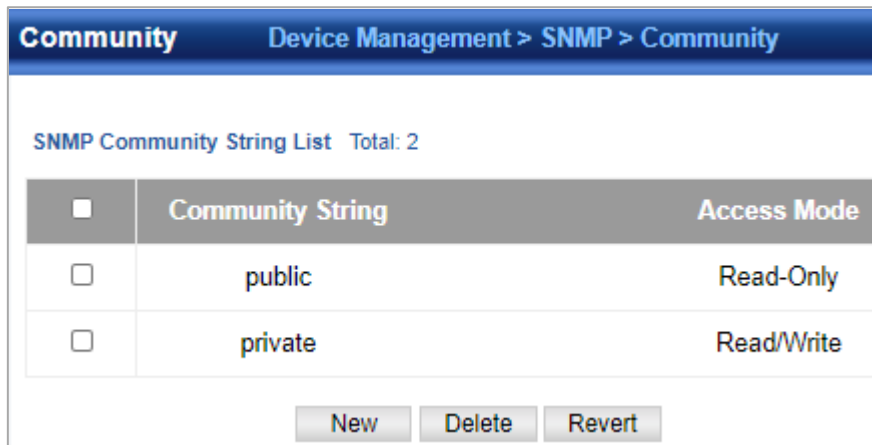
At the bottom right, there are two buttons: 'Apply' and 'Revert'.

◆ **Agent Status** – Enables SNMP on the switch. (Default: Enabled)

◆ **Invalid Community Authentication Trap** – Issues a notification message to specified IP trap managers whenever an invalid community string is submitted during the SNMP access authentication process. (Default: Enabled)

4.8.1.2 Community

Device Management > SNMP > Community page is used to configure up to five community strings authorized for management access by clients using SNMP v1 and v2c. For security reasons, you should consider removing the default strings.



The screenshot shows the 'Community' page under 'Device Management > SNMP > Community'. It displays a table titled 'SNMP Community String List Total: 2'.

<input type="checkbox"/>	Community String	Access Mode
<input type="checkbox"/>	public	Read-Only
<input type="checkbox"/>	private	Read/Write

At the bottom, there are three buttons: 'New', 'Delete', and 'Revert'.

◆ **Community String** – A community string that acts like a password and permits access to the SNMP protocol.

Range: 1-32 characters, case sensitive Default strings: "public" (Read-Only), "private" (Read/Write)

◆ **Access Mode** – Specifies the access rights for the community string:

- **Read-Only** – Authorized management stations are only able to retrieve MIB objects.
- **Read/Write** – Authorized management stations are able to both retrieve and modify MIB objects.

4.8.1.3 View Configuration

Device Management > SNMP > View Configuration page is used to configure SNMPv3 views which are used to restrict user access to specified portions of the MIB tree. The predefined view “defaultview” includes access to the entire MIB tree.

Add View

View Configuration		Device Management > SNMP > View Configuration	
SNMPv3 View OID Subtree List Total: 1			
<input type="checkbox"/>	View Name	Type	OID subtree of View
<input type="checkbox"/>	defaultview	Included	1
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>			

- ◆ **View Name** – The name of the SNMP view. (Range: 1-64 characters)
- ◆ **OID Subtree** – Specifies the initial object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. Use the Add OID Subtree page to configure additional object identifiers.
- ◆ **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view. Add OID Subtree
- ◆ **View Name** – Lists the SNMP views configured in the Add View page.
- ◆ **OID Subtree** – Adds an additional object identifier of a branch within the MIB tree to the selected View. Wild cards can be used to mask a specific portion of the OID string.
- ◆ **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

4.8.1.4 Group Configuration

Device Management > SNMP > Group Configuration page is used to add an SNMPv3 group which can be used to set the access policy for its assigned users, restricting them to specific read, write, and notify views. You can use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views.

Group Configuration		Device Management > SNMP > Group Configuration				
SNMPv3 Group List Total: 4						
<input type="checkbox"/>	Group Name	Model	Level	Read View	Write View	Notify View
<input type="checkbox"/>	public	v1	noAuthNoPriv	defaultview	None	None
<input type="checkbox"/>	public	v2c	noAuthNoPriv	defaultview	None	None
<input type="checkbox"/>	private	v1	noAuthNoPriv	defaultview	defaultview	None
<input type="checkbox"/>	private	v2c	noAuthNoPriv	defaultview	defaultview	None
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>						

- ◆ **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- ◆ **Security Model** – The user security model; SNMP v1, v2c or v3.

◆ **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:

- **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
- **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
- **AuthPriv** – SNMP communications use both authentication and encryption.

◆ **Read View** – The configured view for read access. (Range: 1-32 characters)

◆ **Write View** – The configured view for write access. (Range: 1-32 characters)

◆ **Notify View** – The configured view for notifications. (Range: 1-32 characters)

4.8.1.5 Local User

Device Management > SNMP > Local User page is used to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

Local User						
Device Management > SNMP > Local User						
SNMPv3 Local User List Total: 1						
<input type="checkbox"/>	User Name	Group Name	Model	Level	Authentication	Privacy
<input type="checkbox"/>	test	public	v1	noAuthNoPriv	None	None
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>						

◆ **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)

◆ **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)

◆ **Security Model** – The user security model; SNMP v1, v2c or v3.

◆ **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:

- **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
- **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
- **AuthPriv** – SNMP communications use both authentication and encryption.

◆ **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)

◆ **Authentication Password** – A minimum of eight plain text characters is required.

◆ **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.

◆ **Privacy Password** – A minimum of eight plain text characters is required.

4.8.1.6 Remote User

Device Management > SNMP > Remote User page is used to identify the source of SNMPv3 inform messages sent from the local switch. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

Remote User						
Device Management > SNMP > Remote User						
SNMPv3 Remote User List Total: 0						
User Name	Group Name	Remote Engine ID	Model	Level	Authentication	Privacy
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>						

- ◆ **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- ◆ **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- ◆ **Remote IP** – The Internet address of the remote device where the user resides.
- ◆ **Security Model** – The user security model; SNMP v1, v2c or v3. (Default: v3)
- ◆ **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
 - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
 - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
 - **AuthPriv** – SNMP communications use both authentication and encryption.
- ◆ **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- ◆ **Authentication Password** – A minimum of eight plain text characters is required.
- ◆ **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- ◆ **Privacy Password** – A minimum of eight plain text characters is required.

4.8.1.7 Trap

Device Management > SNMP > Trap is used page to specify the host devices to be sent traps and the types of traps to send. SNMP Version 1

Trap							
Device Management > SNMP > Trap							
SNMP Trap Manager List Total: 0							
IP Address	Version	Type	Community String/User Name	UDP Port	Security Level	Timeout	Retry Times
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>							

- ◆ **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).
- ◆ **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps. (Default: v1)
- ◆ **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive) Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.
- ◆ **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162) SNMP Version 2c
- ◆ **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).
- ◆ **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.
- ◆ Notification Type
 - **Traps** – Notifications are sent as trap messages.

- **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
- **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
- **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. Range: 0-255; Default: 3)

- ◆ **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive) Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.
- ◆ **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162) SNMP Version 3
- ◆ **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).
- ◆ **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.
- ◆ **Notification Type**
 - **Traps** – Notifications are sent as trap messages.
 - **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
 - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
 - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
- ◆ **Local User Name** – The name of a local user which is used to identify the source of SNMPv3 trap messages sent from the local switch. (Range: 1-32 characters) If an account for the specified user has not been created, one will be automatically generated.
- ◆ **Remote User Name** – The name of a remote user which is used to identify the source of SNMPv3 inform messages sent from the local switch. (Range: 1-32 characters) If an account for the specified user has not been created, one will be automatically generated.
- ◆ **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)
- ◆ **Security Level** – When trap version 3 is selected, you must specify one of the following security levels. (Default: noAuthNoPriv)
 - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications.
 - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
 - **AuthPriv** – SNMP communications use both authentication and encryption.

4.8.1.8 Statistics

Device Management > SNMP > Statistics page is used to show counters for SNMP input and output protocol data units.

Statistics			
Device Management > SNMP > Statistics			
SNMP Statistics			
SNMP packets input	0	SNMP packets output	0
Bad SNMP version errors	0	Too big errors	0
Unknown community name	0	No such name errors	0
Illegal operation for community name supplied	0	Bad values errors	0
Encoding errors	0	General errors	0
Number of requested variables	0	Response PDUs	0
Number of altered variables	0	Trap PDUs	0
Get-request PDUs	0		
Get-next PDUs	0		
Set-request PDUs	0		
<input type="button" value="Refresh"/>			

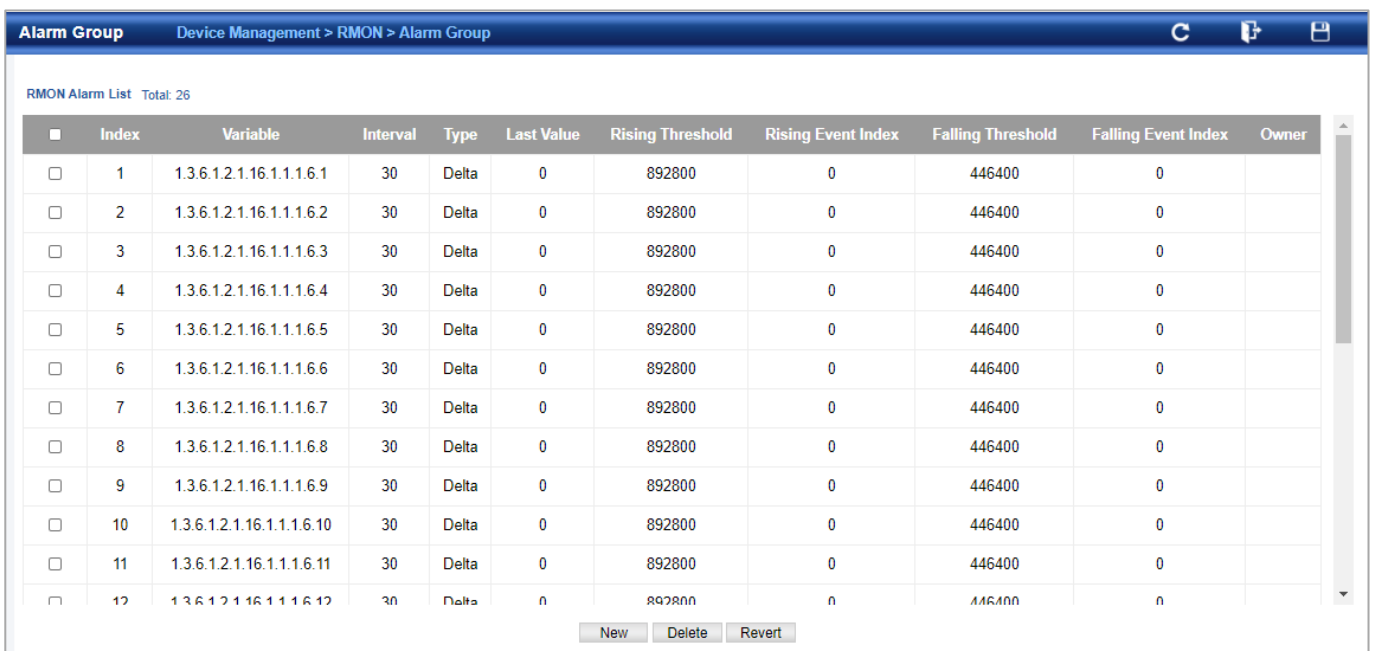
- ◆ **SNMP packets input** – The total number of messages delivered to the SNMP entity from the transport service.
- ◆ **Bad SNMP version errors** – The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.
- ◆ **Unknown community name** – The total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity.
- ◆ **Illegal operation for community name supplied** – The total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.
- ◆ **Encoding errors** – The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
- ◆ **Number of requested variables** – The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
- ◆ **Number of altered variables** – The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
- ◆ **Get-request PDUs** – The total number of SNMP Get-Request PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.
- ◆ **Get-next PDUs** – The total number of SNMP Get-Next PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.
- ◆ **Set-request PDUs** – The total number of SNMP Set-Request PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.
- ◆ **SNMP packets output** – The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
- ◆ **Too big errors** – The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is “tooBig.”

- ◆ **No such name errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is “noSuchName.”
- ◆ **Bad values errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is “badValue.”
- ◆ **General errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is “genErr.”
- ◆ **Response PDUs** – The total number of SNMP Get-Response PDUs which have been accepted and processed by, or generated by, the SNMP protocol entity.
- ◆ **Trap PDUs** – The total number of SNMP Trap PDUs which have been accepted and processed by, or generated by, the SNMP protocol entity.

4.8.2 RMON

4.8.2.1 Alarm Group

Device Management > RMON > Alarm Group page is used to define specific criteria that will generate response events.



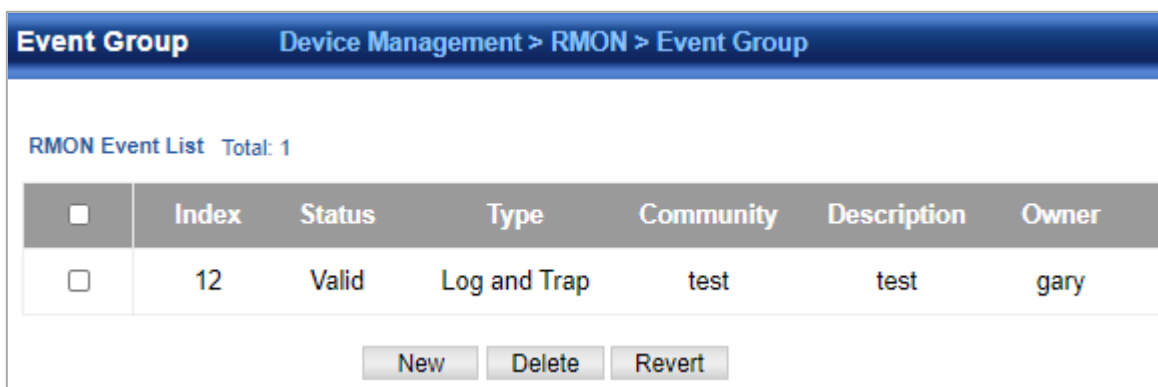
Index	Variable	Interval	Type	Last Value	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner
1	1.3.6.1.2.1.16.1.1.1.6.1	30	Delta	0	892800	0	446400	0	
2	1.3.6.1.2.1.16.1.1.1.6.2	30	Delta	0	892800	0	446400	0	
3	1.3.6.1.2.1.16.1.1.1.6.3	30	Delta	0	892800	0	446400	0	
4	1.3.6.1.2.1.16.1.1.1.6.4	30	Delta	0	892800	0	446400	0	
5	1.3.6.1.2.1.16.1.1.1.6.5	30	Delta	0	892800	0	446400	0	
6	1.3.6.1.2.1.16.1.1.1.6.6	30	Delta	0	892800	0	446400	0	
7	1.3.6.1.2.1.16.1.1.1.6.7	30	Delta	0	892800	0	446400	0	
8	1.3.6.1.2.1.16.1.1.1.6.8	30	Delta	0	892800	0	446400	0	
9	1.3.6.1.2.1.16.1.1.1.6.9	30	Delta	0	892800	0	446400	0	
10	1.3.6.1.2.1.16.1.1.1.6.10	30	Delta	0	892800	0	446400	0	
11	1.3.6.1.2.1.16.1.1.1.6.11	30	Delta	0	892800	0	446400	0	
12	1.3.6.1.2.1.16.1.1.1.6.12	30	Delta	0	892800	0	446400	0	

- ◆ **Index** – Index to this entry. (Range: 1-65535)
- ◆ **Variable** – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled. Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.
- ◆ **Interval** – The polling interval. (Range: 1-31622400 seconds)
- ◆ **Sample Type** – Tests for absolute or relative changes in the specified variable.
 - **Absolute** – The variable is compared directly to the thresholds at the end of the sampling period.
 - **Delta** – The last sample is subtracted from the current value and the difference is then compared to the thresholds.
- ◆ **Rising Threshold** – If the current value is greater than or equal to the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. (Range: 0-2147483647)
- ◆ **Rising Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing above the rising threshold. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 0-65535)

- ◆ **Falling Threshold** – If the current value is less than or equal to the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the falling threshold. (Range: 0-2147483647)
- ◆ **Falling Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing below the falling threshold. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 0-65535)
- ◆ **Owner** – Name of the person who created this entry. (Range: 1-127 characters)

4.8.2.2 Event Group

Device Management > RMON > Event Group page is used to set the action to take when an alarm is triggered. The response can include logging the alarm or sending a message to a trap manager. Alarms and corresponding events provide a way of immediately responding to critical network problems.

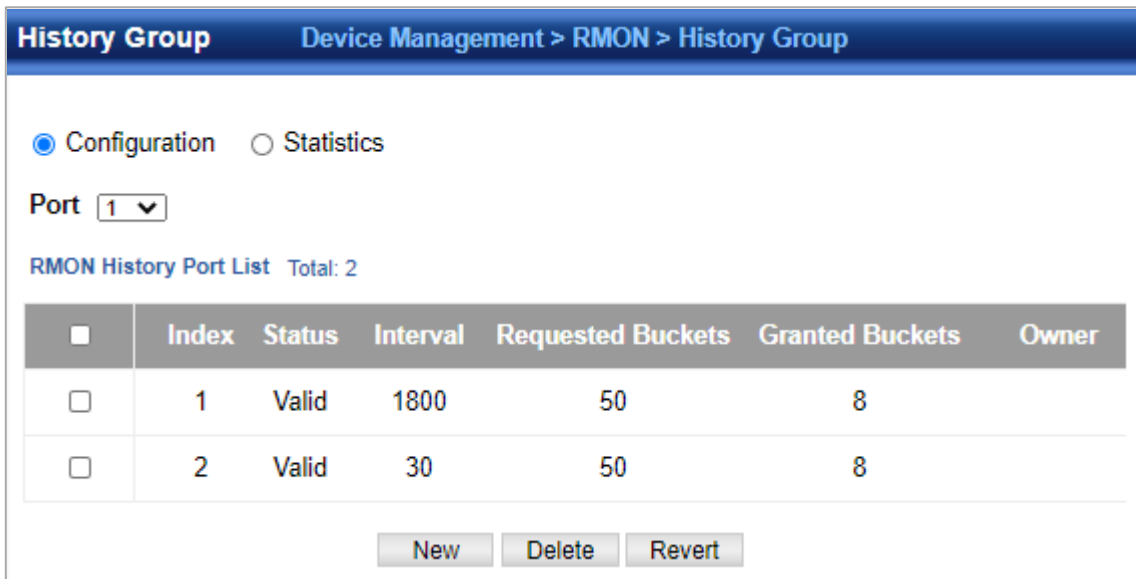


<input type="checkbox"/>	Index	Status	Type	Community	Description	Owner
<input type="checkbox"/>	12	Valid	Log and Trap	test	test	gary

- ◆ **Index** – Index to this entry. (Range: 1-65535)
- ◆ **Type** – Specifies the type of event to initiate:
 - **None** – No event is generated.
 - **Log** – Generates an RMON log entry when the event is triggered. Log messages are processed based on the current configuration settings for event logging.
 - **Trap** – Sends a trap message to all configured trap managers.
 - **Log and Trap** – Logs the event and sends a trap message.
- ◆ **Community** – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts. Although the community string can be set on this configuration page, it is recommended that it be defined on the SNMP trap configuration page prior to configuring it here. (Range: 1-127 characters)
- ◆ **Description** – A comment that describes this event. (Range: 1-127 characters)
- ◆ **Owner** – Name of the person who created this entry. (Range: 1-127 characters)

4.8.2.3 History Group

Device Management > RMON > History Group page is used to collect statistics on a physical interface to monitor network utilization, packet types, and errors. A historical record of activity can be used to track down intermittent problems.



<input type="checkbox"/>	Index	Status	Interval	Requested Buckets	Granted Buckets	Owner
<input type="checkbox"/>	1	Valid	1800	50	8	
<input type="checkbox"/>	2	Valid	30	50	8	

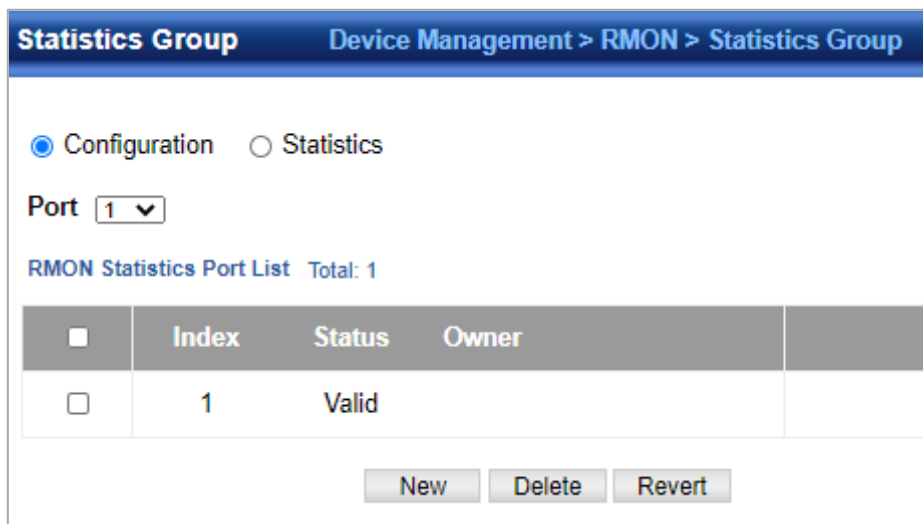
- ◆ **Port** – The port number on the switch.
- ◆ **Index** - Index to this entry. (Range: 1-65535)
- ◆ **Interval** - The polling interval. (Range: 1-3600 seconds; Default: 1800 seconds)
- ◆ **Buckets** - The number of buckets requested for this entry. (Range: 1-65536; Default: 50) The number of buckets granted are displayed on the Show page.
- ◆ **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

4.8.2.4 Statistics Group

Device Management > RMON > Statistics Group page is used to collect statistics on a port, which can subsequently be used to monitor the network for common errors and overall traffic rates. COMMAND USAGE

- ◆ If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made.
- ◆ The information collected for each entry includes: input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, CRC alignment errors, jabbers, fragments, collisions, drop events, and frames of various sizes.

PARAMETERS



<input type="checkbox"/>	Index	Status	Owner
<input type="checkbox"/>	1	Valid	

These parameters are displayed:

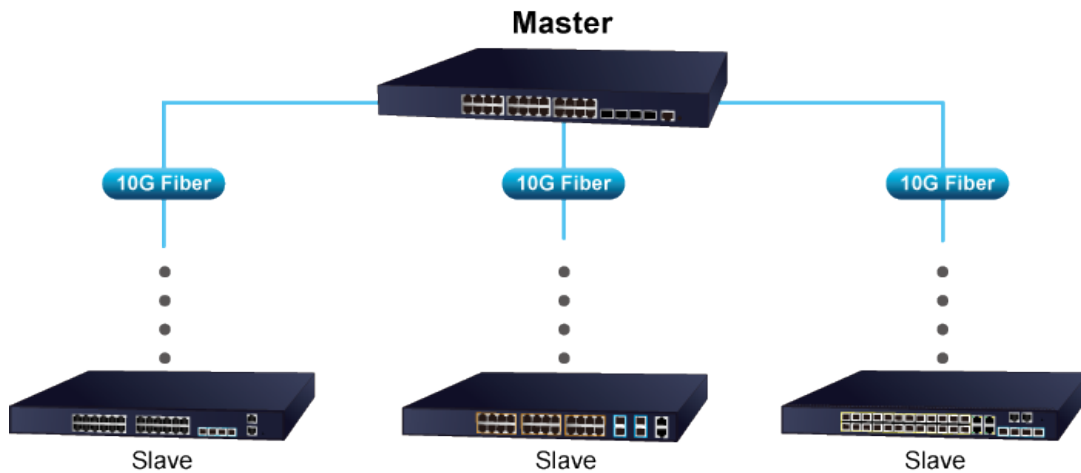
- ◆ **Port** – The port number on the switch.
- ◆ **Index** - Index to this entry. (Range: 1-65535)
- ◆ **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

4.8.3 Cluster

Clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

IP Stacking/Cluster

Up to 16 units with SGS-5240 Series



4.8.3.1 Global Configuration

The Device Management > Cluster > Global Configuration page is used to create a switch cluster.

Global Configuration
Device Management > Cluster > Global Configuration

Cluster Status Enabled

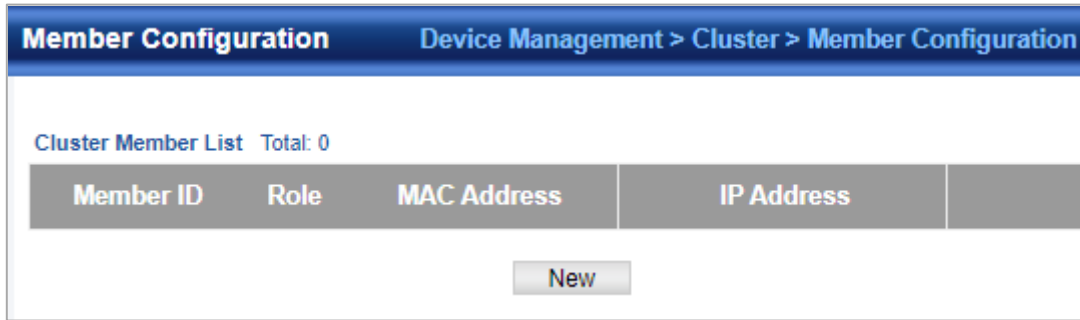
Commander Status Enabled

IP Pool

- ◆ **Cluster Status** – Enables or disables clustering on the switch. (Default: Disabled)
- ◆ **Commander Status** – Enables or disables the switch as a cluster Commander. (Default: Disabled)
- ◆ **IP Pool** – An “internal” IP address pool that is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.x.x.member-ID. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36. Note that you cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled. (Default: 10.254.254.1)

4.8.3.2 Member Configuration

The Device Management > Cluster > Member Configuration page is used to add Candidate switches to the cluster as Members.



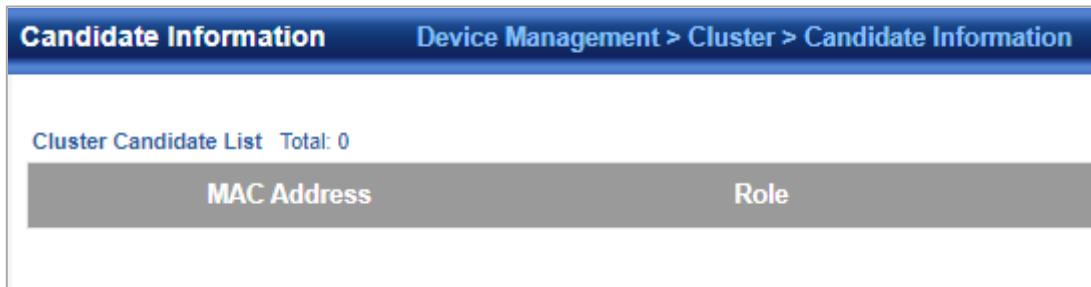
The screenshot shows the 'Member Configuration' page. At the top, there is a breadcrumb trail: 'Device Management > Cluster > Member Configuration'. Below this, the page title 'Member Configuration' is displayed. The main content area shows 'Cluster Member List Total: 0'. Below this, there is a table with the following headers: 'Member ID', 'Role', 'MAC Address', and 'IP Address'. A 'New' button is located below the table.

◆ **Member ID** – Specify a Member ID number for the selected Candidate switch. (Range: 1-36)

◆ **MAC Address** – Select a discovered switch MAC address from the Candidate Table, or enter a specific MAC address of a known switch.

4.8.3.3 Candidate Information

The Device Management > Cluster > Candidate Information page is used to show Candidate.



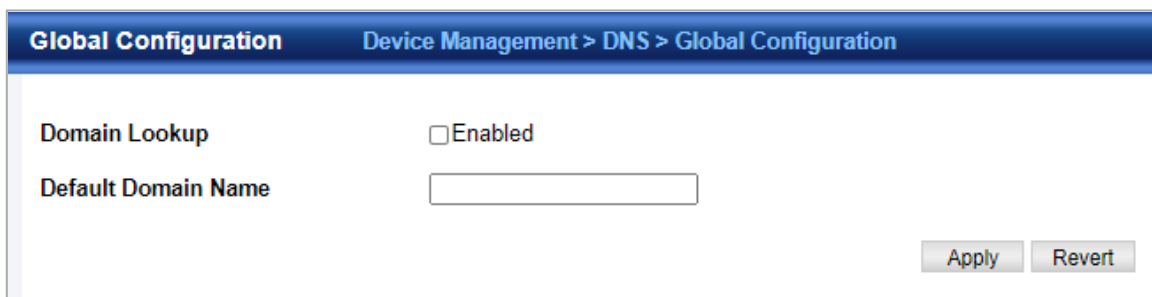
The screenshot shows the 'Candidate Information' page. At the top, there is a breadcrumb trail: 'Device Management > Cluster > Candidate Information'. Below this, the page title 'Candidate Information' is displayed. The main content area shows 'Cluster Candidate List Total: 0'. Below this, there is a table with the following headers: 'MAC Address' and 'Role'.

4.8.4 DNS

DNS service on this switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response. You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

4.8.4.1 Global Configuration

Device Management > DNS > Global Configuration page is used to enable domain lookup and set the default domain name.



The screenshot shows the 'Global Configuration' page. At the top, there is a breadcrumb trail: 'Device Management > DNS > Global Configuration'. Below this, the page title 'Global Configuration' is displayed. The main content area has two settings: 'Domain Lookup' with a checkbox labeled 'Enabled' (which is unchecked), and 'Default Domain Name' with an empty text input field. At the bottom right, there are 'Apply' and 'Revert' buttons.

◆ **Domain Lookup** – Enables DNS host name-to-address translation. (Default: Disabled)

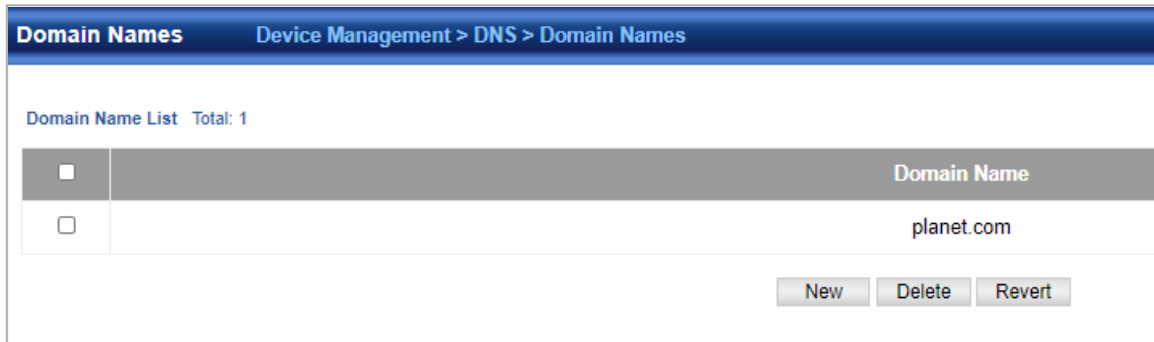
◆ **Default Domain Name** – Defines the default domain name appended to incomplete host names. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 alphanumeric characters)

4.8.4.2 Domain Names

Device Management > DNS > Domain Names page is used to configure a list of name servers to be tried in sequential order.

Name Server IP Address – Specifies the IPv4 or IPv6 address of a domain name server to use for name-to-address resolution.

Up to six IP addresses can be added to the name server list.



Domain Names		Device Management > DNS > Domain Names	
Domain Name List Total: 1			
<input type="checkbox"/>	Domain Name		
<input type="checkbox"/>	planet.com		
		<input type="button" value="New"/>	<input type="button" value="Delete"/>
		<input type="button" value="Revert"/>	

4.8.4.3 Name Servers

Device Management > DNS > Name Servers is used page to configure a list of name servers to be tried in sequential order.

Name Server IP Address – Specifies the IPv4 or IPv6 address of a domain name server to use for name-to-address resolution.

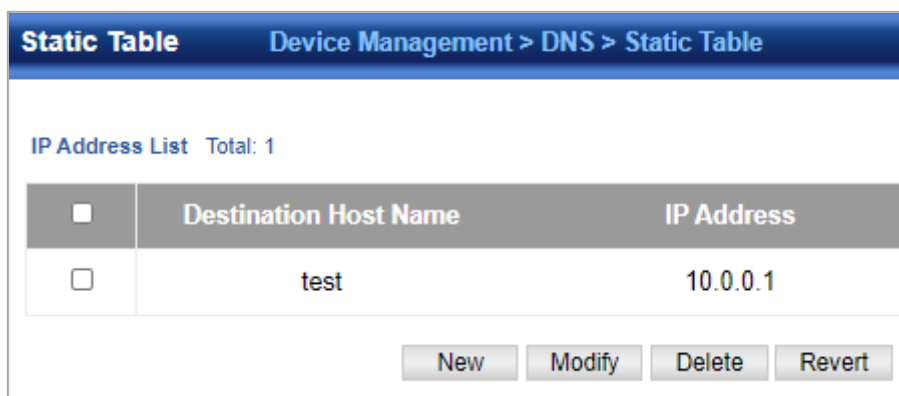
Up to six IP addresses can be added to the name server list.



Name Servers		Device Management > DNS > Name Servers	
Name Server IP Address List Total: 1			
<input type="checkbox"/>	Name Server IP Address		
<input type="checkbox"/>	10.1.1.10		
		<input type="button" value="New"/>	<input type="button" value="Delete"/>
		<input type="button" value="Revert"/>	

4.8.4.4 Static Table

Device Management > DNS > Static Table page is used to manually configure static entries in the DNS table that are used to map domain names to IP addresses.



Static Table			Device Management > DNS > Static Table		
IP Address List Total: 1					
<input type="checkbox"/>	Destination Host Name	IP Address			
<input type="checkbox"/>	test	10.0.0.1			
		<input type="button" value="New"/>	<input type="button" value="Modify"/>	<input type="button" value="Delete"/>	<input type="button" value="Revert"/>

◆ **Host Name** – Name of a host device that is mapped to one or more IP addresses. (Range: 1-127 characters)

◆ **IP Address** – Internet address(es) associated with a host name.

4.8.4.5 Current DNS Information

Device Management > DNS > Current DNS Information page is used to display entries in the DNS cache that have been learned via the designated name servers.

Current DNS Information		Device Management > DNS > Current DNS Information		
Cache Information Total: 0				
ID	Destination Host Name	Type	IP address	TTL

- ◆ **ID.** – The entry number for each resource record.
- ◆ **Type** – This field includes CNAME which specifies the host address for the owner, and ALIAS which specifies an alias.
- ◆ **IP address**– The IP address associated with this record.
- ◆ **TTL** – The time to live reported by the name server.
- ◆ **Host** – The host name associated with this record.

4.8.5 DHCP

4.8.5.1 DHCP Options

Device Management > DHCP > DHCP Options page is used to specify the DHCP client identifier for a VLAN interface.

DHCP Options		Device Management > DHCP > DHCP Options	
L3 Interface VLAN	<input type="text" value="1"/>		
Option 60(Vendor Class Identifier)	<input checked="" type="checkbox"/> Default	<input type="text" value="SGS-5240-24T4X"/>	
		<input type="button" value="Apply"/>	<input type="button" value="Revert"/>

- ◆ **L3 Interface VLAN** – ID of configured VLAN.
- ◆ **Vendor Class ID** – The following options are supported when the check box is marked to enable this feature:
 - **Default** – The default string is ECS4510-28T.
 - **Text** – A text string. (Range: 1-32 characters)
 - **Hex** – A hexadecimal value. (Range: 1-64 characters)

4.8.5.2 Relay

Relay
Device Management > DHCP > Relay

DHCP Server by VLAN List Total: 1

L3 Interface VLAN	L3 Interface IP address				
	Server 1	Server 2	Server 3	Server 4	Server 5
1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Click this button to restart DHCP Relay service.

Note: DHCP relay configuration will be disabled if an active DHCP server is detected on the same network segment.

◆ **L3 Interface VLAN ID**—ID of configured VLAN.

◆ **Server IP Address**—Addresses of DHCP servers or relay servers to be used by the switch's DHCP relay agent in order of preference.

◆ **Restart DHCP Relay**—Use this button to re-initialize DHCP relay service.

4.8.5.3 Relay Option82

◆ **Insertion of Relay Information**—Enable DHCP Option 82 information relay. (Default: Disabled)

◆ **DHCP Option Policy**—Specifies how to handle client requests which already contain DHCP Option 82 information:

- **Drop**- Floods the original request packet onto the VLAN that received it instead of relaying it. (This is the default.)
- **Keep**- Retains the Option 82 information in the client request, inserts the relay agent's address, and unicasts the packet to the DHCP server.
- **Replace**- Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information provided by the relay agent itself, inserts the relay agent's address, and unicasts the packet to the DHCP server.

◆ **DHCP Sub-option Format**—Specifies whether or not to use the sub-type and sub-length fields in the circuit-ID (CID) and remote-ID (RID) in Option 82 information. (Default: Included)

◆ **Server IP Address**—Addresses of DHCP servers or relay servers to be used by the switch's DHCP relay agent in order of preference.

4.8.5.4 Dynamic Provision

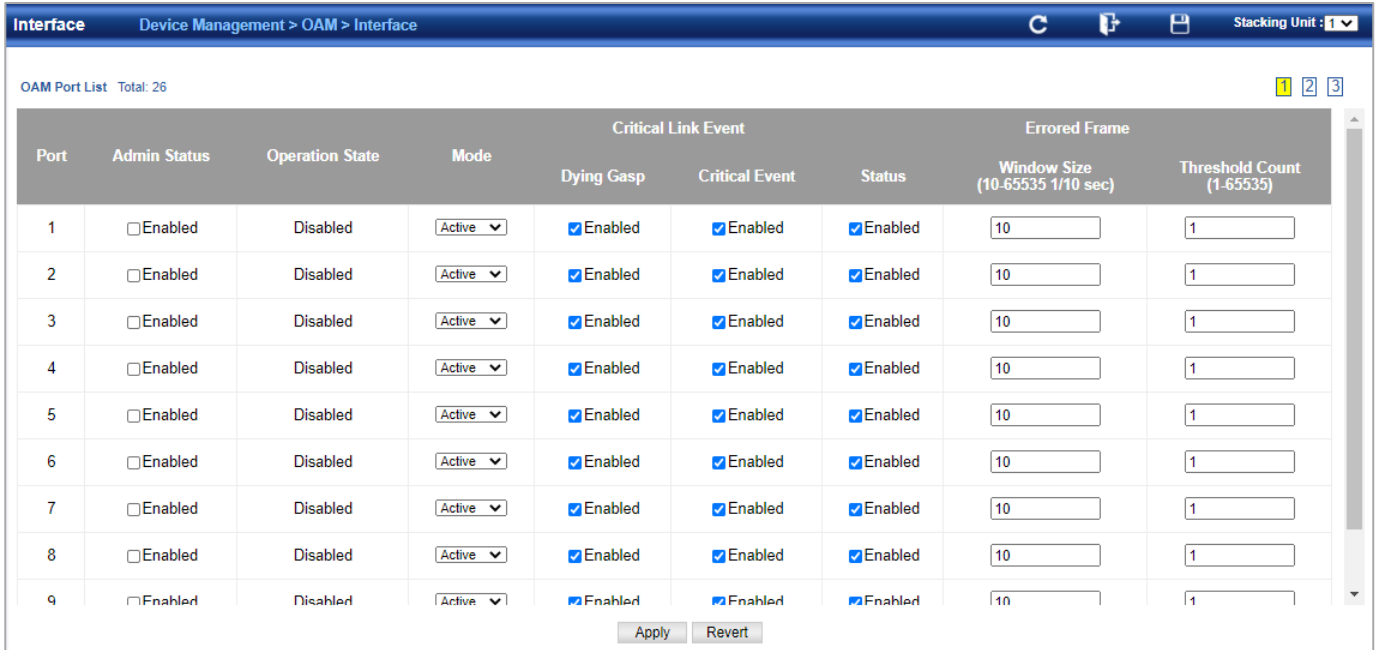
Device Management > DHCP > Dynamic Provision is used to enable dynamic provisioning via DHCP.

◆ **Dynamic Provision via DHCP Status** — Enables dynamic provisioning via DHCP. (Default: Disabled)

4.8.6 OAM

4.8.6.1 Interface

The Device Management > OAM > Interface page is used to enable OAM functionality on the selected port. Not all CPEs support operation and maintenance functions, so OAM is therefore disabled by default. If a CPE supports OAM, this functionality must first be enabled on the connected port to gain access to the configuration functions provided under the OAM menu.

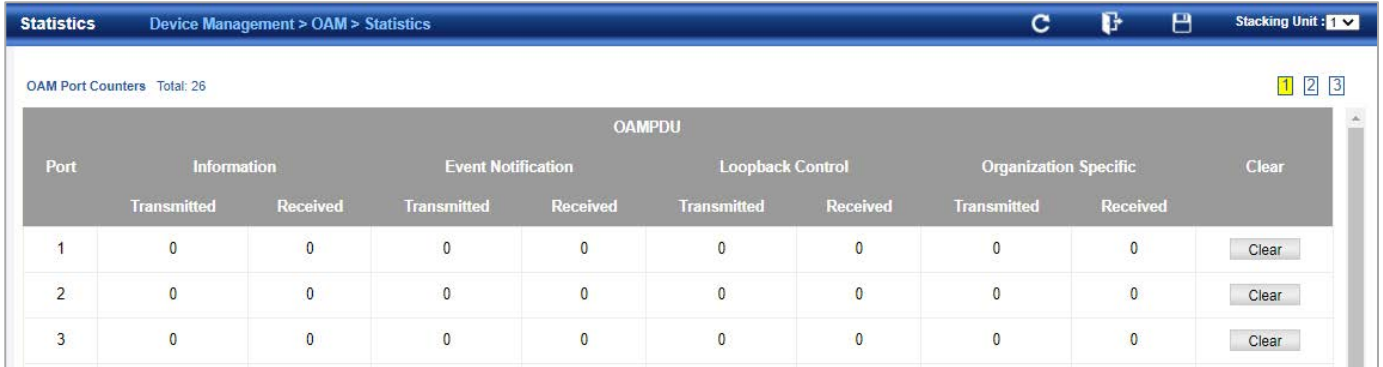


Port	Admin Status	Operation State	Mode	Critical Link Event			Errored Frame	
				Dying Gasp	Critical Event	Status	Window Size (10-65535 1/10 sec)	Threshold Count (1-65535)
1	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
2	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
3	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
4	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
5	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
6	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
7	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
8	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
9	<input type="checkbox"/> Enabled	Disabled	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1

- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Admin Status** – Enables or disables OAM functions. (Default: Disabled)
- ◆ **Operation State** – Shows the operational state between the local and remote OAM devices. This value is always “disabled” if OAM is disabled on the local interface. OAM Operation State
- ◆ **Mode** – Sets the OAM operation mode. (Default: Active)
 - **Active** – All OAM functions are enabled.
 - **Passive** – All OAM functions are enabled, except for OAM discovery, sending variable request OAMPDUs, and sending loopback control OAMPDUs.
- ◆ **Critical Link Event** – Controls reporting of critical link events to its OAM peer.
 - **Dying Gasp** – If an unrecoverable condition occurs, the local OAM entity (i.e., this switch) indicates this by immediately sending a trap message. (Default: Enabled) Dying gasp events are caused by an unrecoverable failure, such as a power failure or device reset.
 - **Critical Event** – If a critical event occurs, the local OAM entity indicates this to its peer by setting the appropriate flag in the next OAMPDU to be sent and stores this information in its OAM event log. (Default: Enabled) Critical events include various failures, such as abnormal voltage fluctuations, out-of-range temperature detected, fan failure, CRC error in flash memory, insufficient memory, or other hardware faults.
- ◆ **Errored Frame** – Controls reporting of errored frame link events. An errored frame is a frame in which one or more bits are errored. An errored frame link event occurs if the threshold is reached or exceeded within the specified period. If reporting is enabled and an errored frame link event occurs, the local OAM entity (this switch) sends an Event Notification OAMPDU to the remote OAM entity. The Errored Frame Event TLV includes the number of errored frames detected during the specified period.
 - **Status** – Enables reporting of errored frame link events. (Default: Enabled)
 - **Window Size** – The period of time in which to check the reporting threshold for errored frame link events. (Range: 10-65535 in units of 10 milliseconds; Default: 10 units of 10 milliseconds, or the equivalent of 1 second)
 - **Threshold Count** – The threshold for errored frame link events. (Range: 1-65535; Default: 1)

4.8.6.2 Statistics

The Device Management > OAM > Statistics page is used to display statistics for the various types of OAM messages passed across each port.

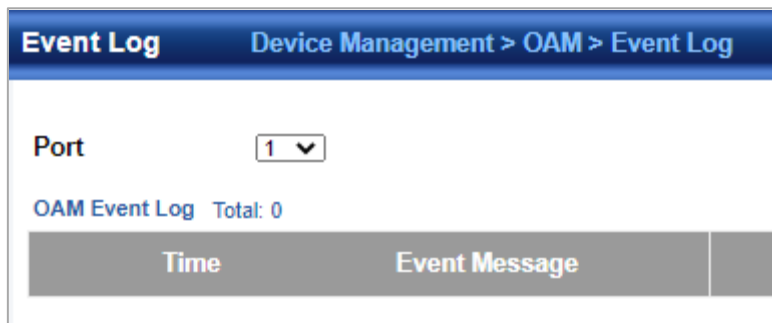


Port	OAMPDU								Clear	
	Information		Event Notification		Loopback Control		Organization Specific			
	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received		
1	0	0	0	0	0	0	0	0	0	Clear
2	0	0	0	0	0	0	0	0	0	Clear
3	0	0	0	0	0	0	0	0	0	Clear

- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Clear** – Clears statistical counters for the selected ports.
- ◆ **OAMPDU** – Message types transmitted and received by the OAM protocol, including Information OAMPDUs, unique Event OAMPDUs, Loopback Control OAMPDUs, and Organization Specific OAMPDUs.

4.8.6.3 Event Log

The Device Management > OAM > Event Log page is used to display link events for the selected port. To display link events for the selected port:



Event Log Device Management > OAM > Event Log

Port:

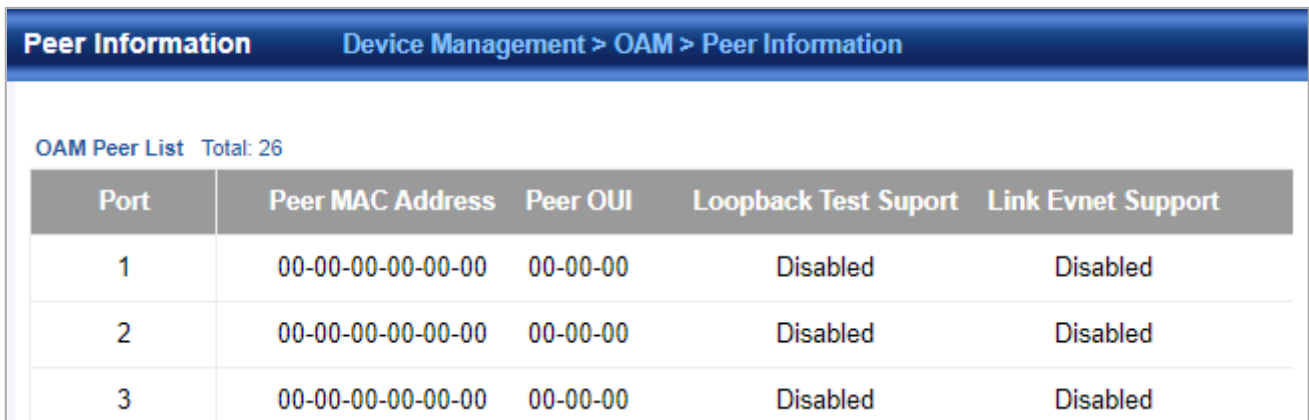
OAM Event Log Total: 0

Time	Event Message

1. Click Device Management, OAM, Event Log.
2. Select a port from the drop-down list.

4.8.6.4 Peer Information

The Device Management > OAM > Peer Information page is used to display information about attached OAM-enabled devices.



Port	Peer MAC Address	Peer OUI	Loopback Test Suport	Link Evnet Support
1	00-00-00-00-00-00	00-00-00	Disabled	Disabled
2	00-00-00-00-00-00	00-00-00	Disabled	Disabled
3	00-00-00-00-00-00	00-00-00	Disabled	Disabled

- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **MAC Address** – MAC address of the OAM peer.
- ◆ **OUI** – Organizational Unit Identifier of the OAM peer.
- ◆ **Remote Loopback** – Shows if remote loopback is supported by the OAM peer.
- ◆ **Unidirectional Function** – Shows if this function is supported by the OAM peer. If supported, this indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (where traffic flows in one direction only). Some newer physical layer devices support the optional ability to encode and transmit data while one direction of the link is non-operational. This function allows OAM remote fault indication during fault conditions. This switch does not support the unidirectional function, but can parse error messages sent from a peer with unidirectional capability.
- ◆ **Link Monitor** – Shows if the OAM entity can send and receive Event Notification OAMPDUs.
- ◆ **MIB Variable Retrieval** – Shows if the OAM entity can send and receive Variable Request and Response OAMPDUs.

4.8.6.5 Loopback Result

Use the Device Management > OAM > Loopback Result page is used to display the results of remote loop back testing for each port for which this information is available.

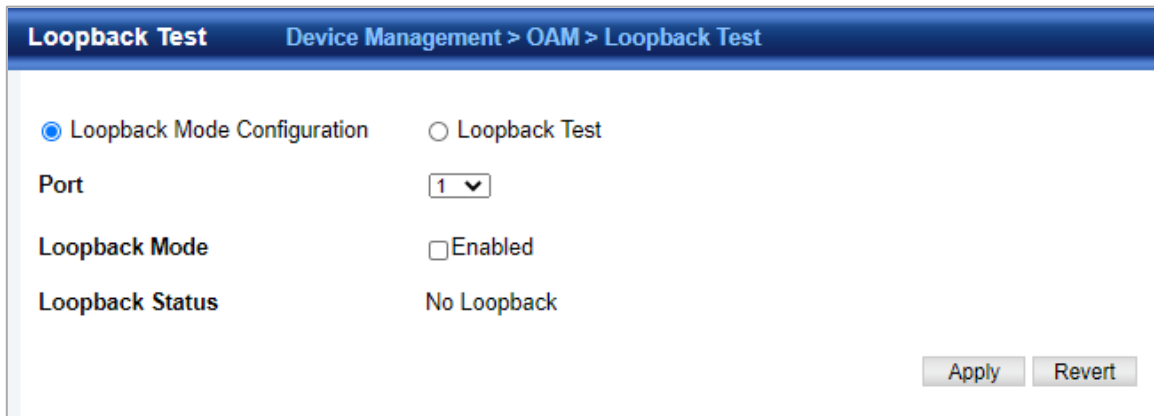
Loopback Result		Device Management > OAM > Loopback Result		
Port Remote Test Result List Total: 26				
Port	Packets Transmitted	Packets Received	Loss Rate	
1	0	0	0.00 %	
2	0	0	0.00 %	
3	0	0	0.00 %	

- ◆ **Port** – Port identifier. (Range: 1-12/26)
- ◆ **Packets Transmitted** – The number of loop back frames transmitted during the last loop back test on this interface.
- ◆ **Packets Received** – The number of loop back frames received during the last loop back test on this interface.
- ◆ **Loss Rate** – The percentage of packets transmitted for which there was no response.

4.8.6.6 Loopback Test

The Device Management > OAM > Loopback Test page is used to initiate a loop back test to the peer device attached to the selected port.

Loopback Mode of Remote Device



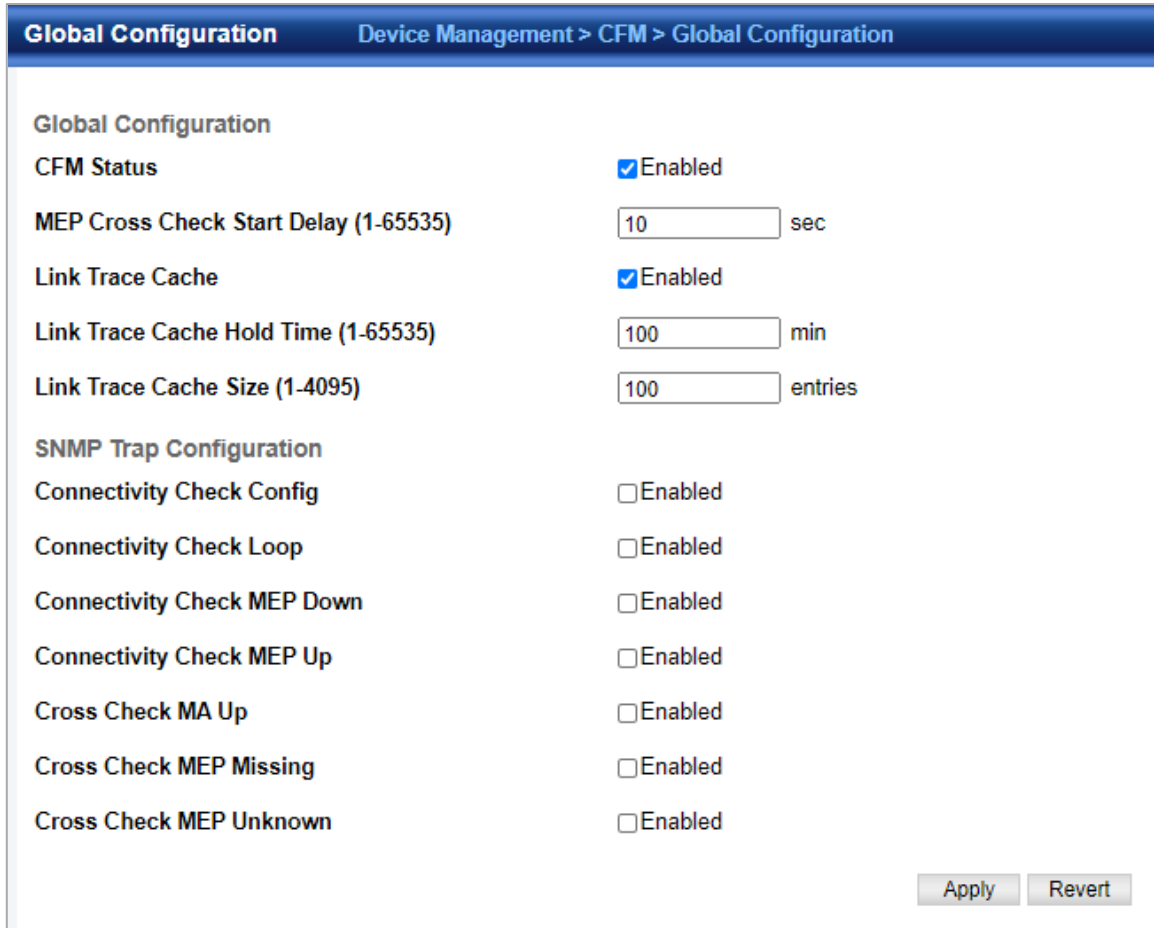
- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Loopback Mode** – Shows if loop back mode is enabled on the peer. This attribute must be enabled before starting the loopback test.
- ◆ **Loopback Status** – Shows if loopback testing is currently running. Loopback Test Parameters
- ◆ **Packets Number** – Number of packets to send. (Range: 1-99999999; Default: 10000)
- ◆ **Packet Size** – Size of packets to send. (Range: 64-1518 bytes; Default: 64 bytes)
- ◆ **Test** – Starts the loop back test.
- ◆ **End** – Stops the loop back test. Loop Back Status of Remote Device
- ◆ **Result** – Shows the loop back status on the peer. The loop back states shown in this field are described below. OAM Operation State
- ◆ **Packets Transmitted** – The number of loop back frames transmitted during the last loopback test on this interface.
- ◆ **Packets Received** – The number of loop back frames received during the last loopback test on this interface.
- ◆ **Loss Rate** – The percentage of packets for which there was no response.

4.8.7 CFM

4.8.7.1 Global Configuration

Device Management > CFM > Global Configuration page is used to configure global settings for CFM, such as enabling the CFM process on the switch, setting the start-up delay for cross-check operations, configuring parameters for the link trace cache, and enabling traps for events discovered by continuity check messages or cross-check messages.

Global Configuration



Global Configuration	
CFM Status	<input checked="" type="checkbox"/> Enabled
MEP Cross Check Start Delay (1-65535)	<input type="text" value="10"/> sec
Link Trace Cache	<input checked="" type="checkbox"/> Enabled
Link Trace Cache Hold Time (1-65535)	<input type="text" value="100"/> min
Link Trace Cache Size (1-4095)	<input type="text" value="100"/> entries
SNMP Trap Configuration	
Connectivity Check Config	<input type="checkbox"/> Enabled
Connectivity Check Loop	<input type="checkbox"/> Enabled
Connectivity Check MEP Down	<input type="checkbox"/> Enabled
Connectivity Check MEP Up	<input type="checkbox"/> Enabled
Cross Check MA Up	<input type="checkbox"/> Enabled
Cross Check MEP Missing	<input type="checkbox"/> Enabled
Cross Check MEP Unknown	<input type="checkbox"/> Enabled

- ◆ **CFM Status** – Enables CFM processing globally on the switch.

(Default: Enabled)

To avoid generating an excessive number of traps, the complete CFM maintenance structure and process parameters should be configured prior to enabling CFM processing globally on the switch. Specifically, the maintenance domains, maintenance associations, and **maintenance end-points (MEPs)** should be configured on each participating bridge using the Configure MD page, Configure MA page, and the Configure MEP page. When CFM is enabled, hardware resources are allocated for CFM processing.

- ◆ **MEP Cross Check Start Delay** – Sets the maximum delay that a device waits for remote MEPs to come up before starting the crosscheck operation. (Range: 1-65535 seconds; Default: 10 seconds)

This parameter sets the time to wait for a remote MEP to come up, and the switch starts cross-checking the list of statically configured remote MEPs in the local maintenance domain against the MEPs learned through continuity check messages (CCMs). The cross-check start delay should be configured to a value greater than or equal to the continuity check message interval to avoid generating unnecessary traps. Link Trace Cache Settings

- ◆ **Link Trace Cache** – Enables caching of CFM data learned through link trace messages. (Default: Enabled)

A linktrace message is a multicast CFM frame initiated by a MEP, and forwarded from MIP to MIP, with each MIP generating a linktrace reply, up to the point at which the linktrace message reaches its destination or can no longer be forwarded. Use this command attribute to enable the link trace cache to store the results of link trace operations initiated on this device. Use the CFM Transmit Link Trace page to transmit a linktrace message. Linktrace responses are returned

from each MIP along the path and from the target MEP. Information stored in the cache includes the maintenance domain name, MA name, MEPID, sequence number, and TTL value.

- ◆ **Link Trace Cache Hold Time** – The hold time for CFM link trace cache entries. (Range: 1-65535 minutes; Default: 100 minutes)

Before setting the aging time for cache entries, the cache must first be enabled in the Linktrace Cache attribute field.

- ◆ **Link Trace Cache Size** – The maximum size for the link trace cache. (Range: 1-4095 entries; Default: 100 entries)
If the cache reaches the maximum number of specified entries, or the size is set to a value less than the current number of stored entries, no new entries are added. To add additional entries, the cache size must first be increased, or purged.

Continuity Check Errors

- ◆ **Connectivity Check Config** – Sends a trap if this device receives a continuity check message (CCM) with the same maintenance end point identifier (MPID) as its own but with a different source MAC address, indicating that a CFM configuration error exists.
- ◆ **Connectivity Check Loop** – Sends a trap if this device receives a CCM with the same source MAC address and MPID as its own, indicating that a forwarding loop exists.
- ◆ **Connectivity Check MEP Down** – Sends a trap if this device loses connectivity with a remote maintenance end point (MEP), or connectivity has been restored to a remote MEP which has recovered from an error condition.
- ◆ **Connectivity Check MEP Up** – Sends a trap if a remote MEP is discovered and added to the local database, the port state of a previously discovered remote MEP changes, or a CCM is received from a remote MEP which as an expired entry in the archived database. MEP Up traps are suppressed when cross-checking of MEPs is enabled¹¹ because cross-check traps include more detailed status information. Cross-check Errors
- ◆ **Cross Check MA Up** – Sends a trap when all remote MEPs in an MA come up. An MA Up trap is sent if cross-checking is enabled, and a CCM is received from all remote MEPs configured in the static list for this maintenance association
- ◆ **Cross Check MEP Missing** – Sends a trap if the cross-check timer expires and no CCMs have been received from a remote MEP configured in the static list. A MEP Missing trap is sent if cross-checking is enabled¹¹, and no CCM is received for a remote MEP configured in the static list¹².
- ◆ **Cross Check MEP Unknown** – Sends a trap if an unconfigured MEP comes up. A MEP Unknown trap is sent if cross-checking is enabled¹¹, and a CCM is received from a remote MEP that is not configured in the static list¹².

4.8.7.2 Interface Configuration

CFM processes are enabled by default for all physical interfaces, both ports and trunks. You can use the Device Management > CFM > Interface Configuration page to change these settings.

Interface Configuration
Device Management > CFM > Interface Configuration

Interface Port Group

Port List Total: 26

Port	CFM Status
1	<input checked="" type="checkbox"/> Enabled
2	<input checked="" type="checkbox"/> Enabled
3	<input checked="" type="checkbox"/> Enabled
4	<input checked="" type="checkbox"/> Enabled
5	<input checked="" type="checkbox"/> Enabled
6	<input checked="" type="checkbox"/> Enabled
7	<input checked="" type="checkbox"/> Enabled
8	<input checked="" type="checkbox"/> Enabled
9	<input checked="" type="checkbox"/> Enabled
10	<input checked="" type="checkbox"/> Enabled

4.8.7.3 MD Management

Device Management > CFM > MD Management pages is used to create and configure a **Maintenance Domain (MD)** which defines a portion of the network for which connectivity faults can be managed. Domain access points are set up on the boundary of a domain to provide end-to-end connectivity fault detection, analysis, and recovery. Domains can be configured in a hierarchy to provide management access to the same basic network resources for different user levels.

Creating a Maintenance Domain

MD Management
Device Management > CFM > MD Management

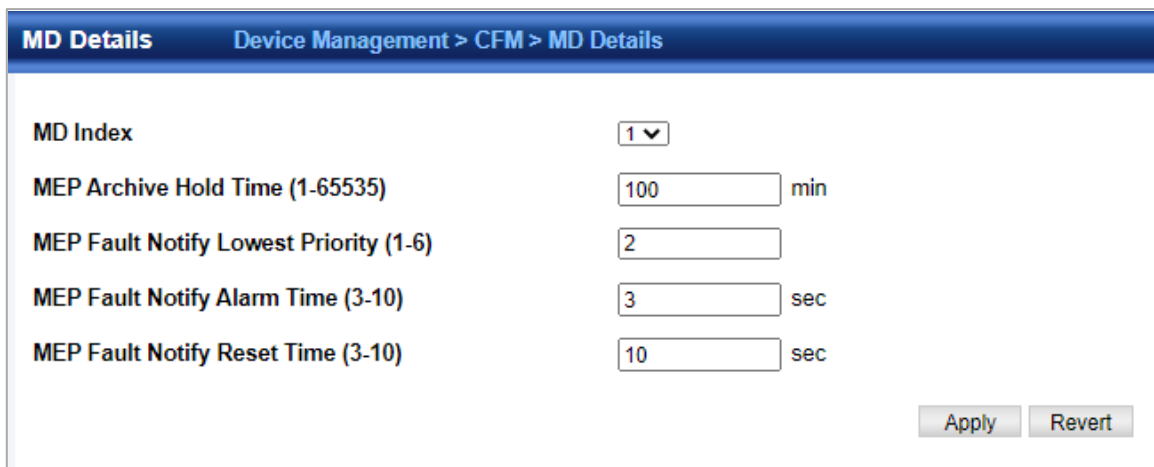
CFM MD List Total: 1

☐	MD Index	MD Name	MD Level	MIP Creation Type
<input type="checkbox"/>	1	test	3	Default

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MD Name** – Maintenance domain name. (Range: 1-43 alphanumeric characters)
- ◆ **MD Level** – Authorized maintenance level for this domain. (Range: 0-7)
- ◆ **MIP Creation Type** – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this domain:
 - **Default** – MIPs can be created for any **maintenance association (MA)** configured in this domain on any bridge port through which the MA's VID can pass.
 - **Explicit** – MIPs can be created for any MA configured in this domain only on bridge ports through which the MA's VID can pass, and only if a **maintenance end point (MEP)** is created at some lower MA Level.
 - **None** – No MIP can be created for any MA configured in this domain.

4.8.7.4 MD Details

Device Management > CFM > MD Details page is used to configure details of specify MD.

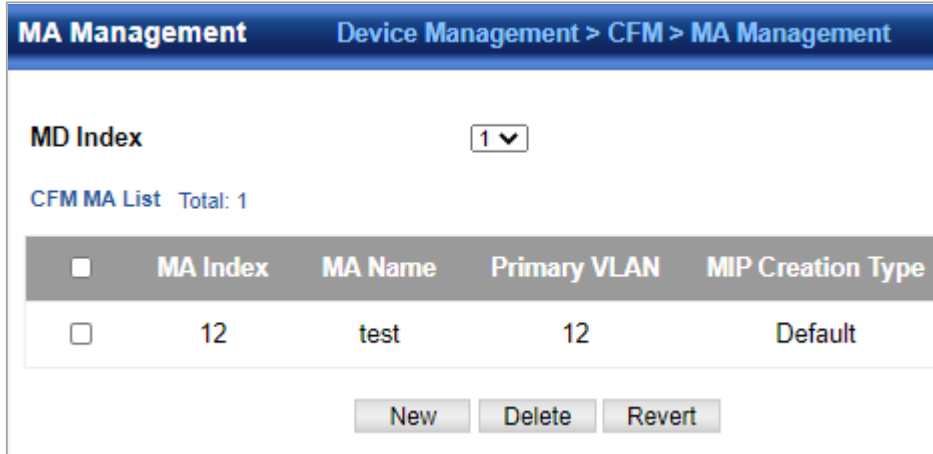


- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MEP Archive Hold Time** – The time that data from a missing MEP is retained in the **continuity check message (CCM)** database before being purged. (Range: 1-65535 minutes; Default: 100 minutes) A change to the hold time only applies to entries stored in the database after this attribute is changed.
- ◆ **MEP Fault Notify Lowest Priority** – The lowest priority defect that is allowed to generate a fault alarm. (Range: 1-6, Default: 2)
- ◆ **MEP Fault Notify Alarm Time** – The time that one or more defects must be present before a fault alarm is issued. (Range: 3-10 seconds; Default: 3 seconds)
- ◆ **MEP Fault Notify Reset Time** – The time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued. (Range: 3-10 seconds; Default: 10 seconds)

4.8.7.5 MA Management

Device Management > CFM > MA Management pages is used to create and configure the **Maintenance Associations (MA)** which define a unique CFM service instance. Each MA can be identified by its parent MD, the MD's maintenance level, the VLAN assigned to the MA, and the set of **maintenance end points (MEPs)** assigned to it.

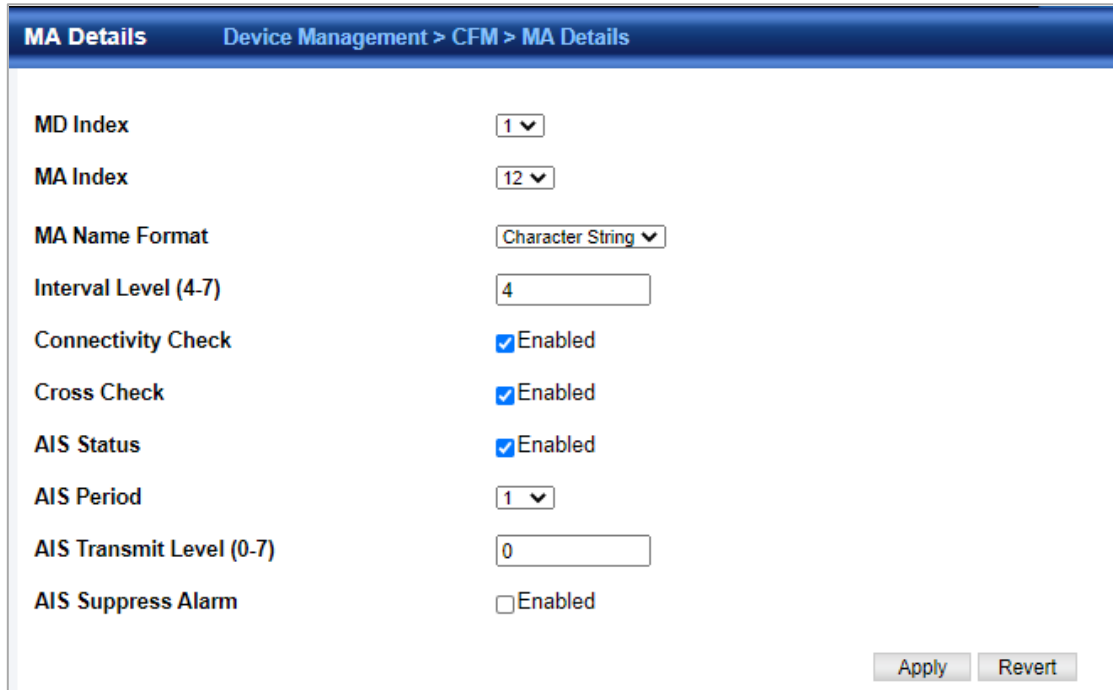
Creating a Maintenance Association



- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MA Name** – MA name. (Range: 1-43 alphanumeric characters)
Each MA name must be unique within the CFM domain.
- ◆ **Primary VLAN** – Service VLAN ID. (Range: 1-4093)
This is the VLAN through which all CFM functions are executed for this MA.
- ◆ **MIP Creation Type** – Specifies the CFM protocol's creation method for **maintenance intermediate points (MIPs)** in this MA:
 - **Default** – MIPs can be created for this MA on any bridge port through which the MA's VID can pass.
 - **Explicit** – MIPs can be created for this MA only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.
 - **None** – No MIP can be created for this MA.

4.8.7.6 MA Details

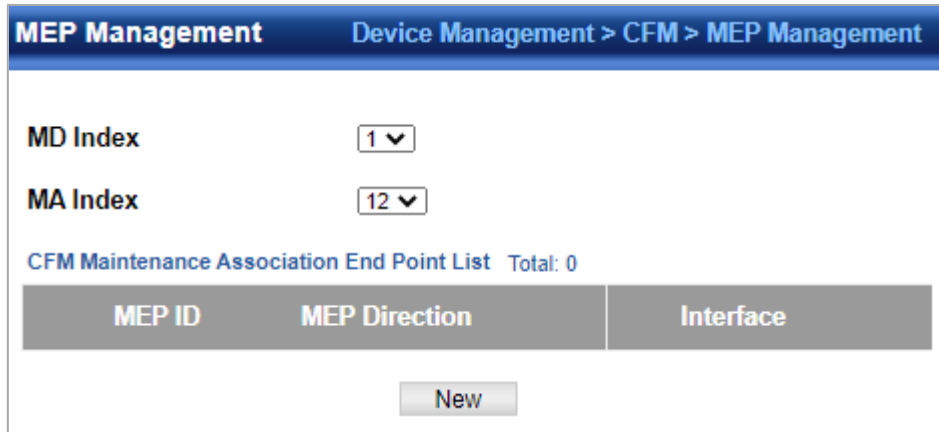
Device Management > CFM > MA Details page is used to configure details of specify MA. Configuring Detailed Settings for a Maintenance Association



- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MA Name Format** – Specifies the name format for the maintenance association as IEEE 802.1ag character based, or ITU-T SG13/SG15 Y.1731 defined ICC-based format.
 - **Character String** – IEEE 802.1ag defined character string format. This is an IETF RFC 2579 DisplayString.
 - **ICC Based** – ITU-T SG13/SG15 Y.1731 defined ICC based format.
- ◆ **Interval Level** – The delay between sending CCMs. The setting for this parameter is expressed as levels 4 through 7, which in turn map to specific intervals of time. (Options: 4 - 100 ms, 5 - 1 sec, 6 - 10 sec, 7 - 60 sec)
- ◆ **Connectivity Check** – Enables transmission of CCMs. (Default: Disabled)
- ◆ **Cross Check** – Enables cross-checking between a static list of MEPs assigned to other devices within the same maintenance association and the MEPs learned through CCMs. Before starting the cross-check process, first configure the remote MEPs that exist on other devices inside the maintenance association using the Remote MEP List. These remote MEPs are used in the cross-check operation to verify that all endpoints in the specified MA are operational. The cross-check start delay, which sets the maximum delay this device waits for a remote MEP to come up before starting the cross-check operation, is a domain-level parameter. To set this parameter, use the CFM MD Configuration screen.
- ◆ **AIS Status** – Enables/disables suppression of the **Alarm Indication Signal (AIS)**. (Default: Disabled)
- ◆ **AIS Period** – Configures the period at which AIS is sent in an MA. (Range: 1 or 60 seconds; Default: 1 second)
- ◆ **AIS Transmit Level** – Configure the AIS maintenance level in an MA. (Range: 0-7; Default is 0) AIS Level must follow this rule: AIS Level >= Domain Level
- ◆ **AIS Suppress Alarm** – Enables/disables suppression of the AIS. (Default: Disabled)

4.8.7.7 MEP Management

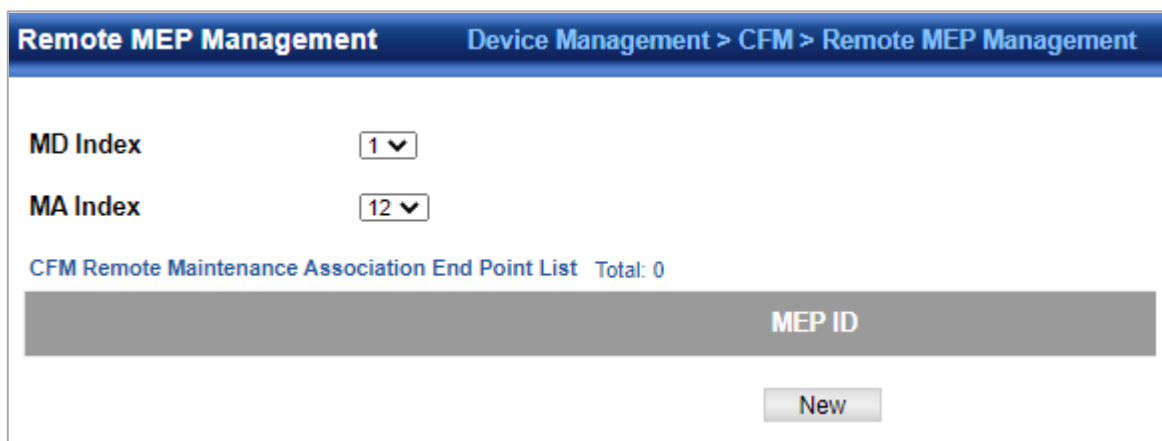
Device Management > CFM > MEP Management page is used to configure Maintenance End Points (MEPs). MEPs, also called **Domain Service Access Points (DSAPs)**, must be configured at the domain boundary to provide management access for each maintenance association.



- ◆ **MD Index** – Domain index.
(Range: 1-65535)
- ◆ **MA Index** – MA identifier.
(Range: 1-2147483647)
- ◆ **MEP ID** – Maintenance end point identifier.
(Range: 1-8191)
- ◆ **MEP Direction** – Up indicates that the MEP faces inward toward the switch cross-connect matrix, and transmits CFM messages towards, and receives them from, the direction of the internal bridge relay mechanism.
If the **Up** option is not selected, then the MEP is facing away from the switch, and transmits CFM messages towards, and receives them from, the direction of the physical medium.
- ◆ **Interface** – Indicates a port or trunk.

4.8.7.8 Remote MEP Management

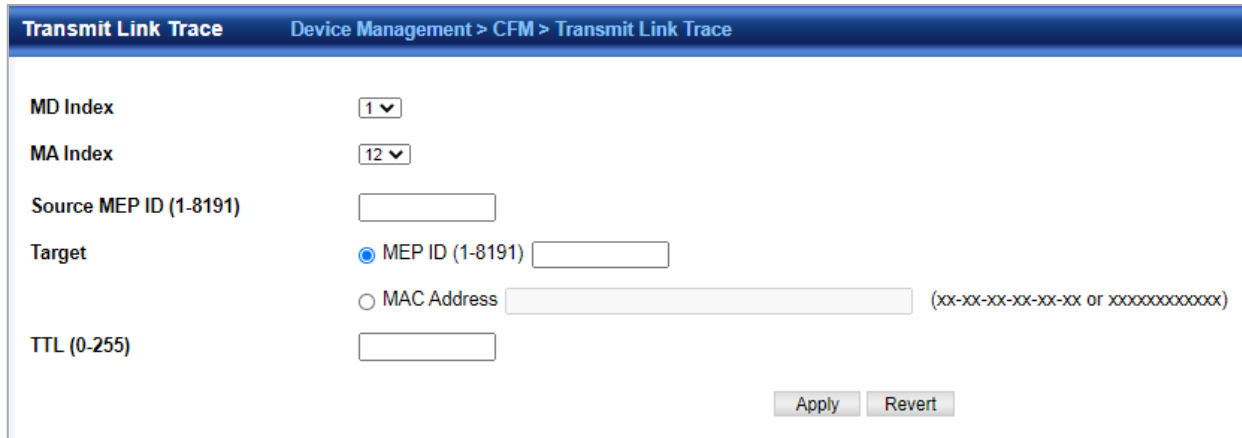
Device Management > CFM > Remote MEP Management page is used to specify remote **maintenance end points (MEPs)** set on other CFM-enabled devices within a common MA.



- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MEP ID** – Identifier for a maintenance end point which exists on another CFM-enabled device within the same MA.
(Range: 1-8191)

4.8.7.9 Transmit Link Trace

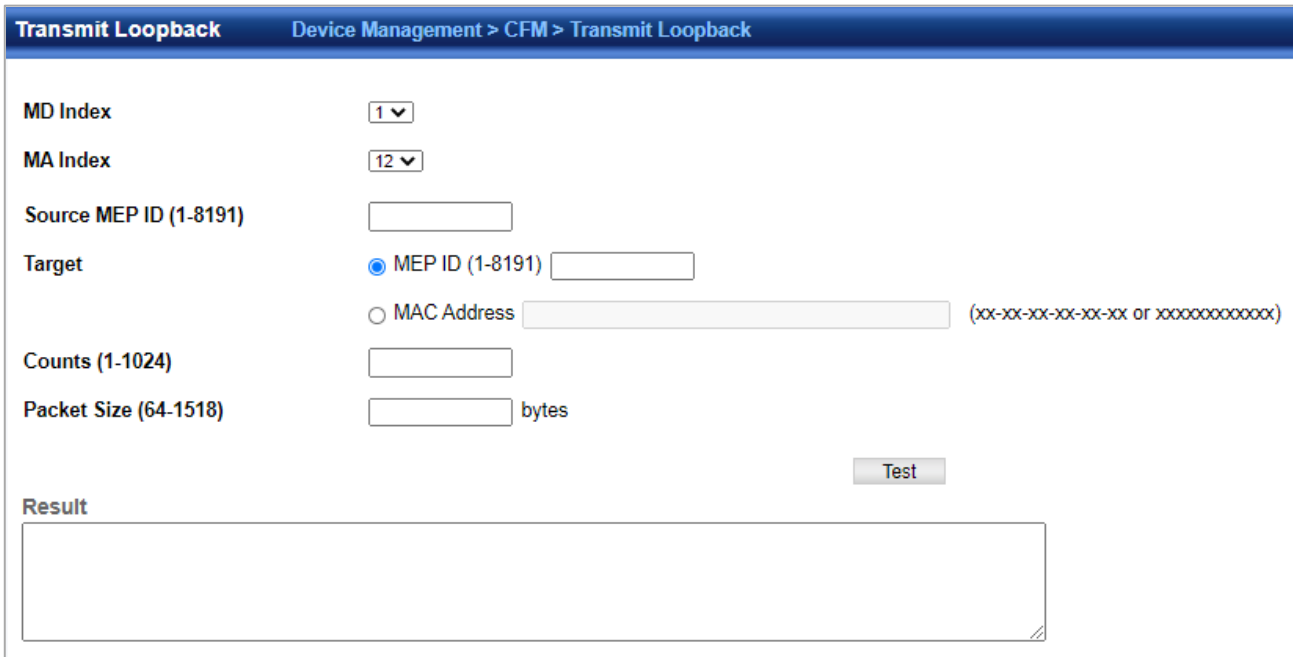
Device Management > CFM > Transmit Link Trace page is used to **transmit link trace messages (LTMs)**. These messages can isolate connectivity faults by tracing the path through a network to the designated target node (i.e., a remote maintenance end point).



- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **Source MEP ID** – The identifier of a source MEP that will send the link trace message. (Range: 1-8191)
- ◆ **Target**
 - **MEP ID** – The identifier of a remote MEP that is the target of a link trace message. (Range: 1-8191)
 - **MAC Address** – MAC address of a remote MEP that is the target of a link trace message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx
- ◆ **TTL** – The time to live of the link trace message. (Range: 0-255 hops)

4.8.7.10 Transmit Loopback

Device Management > CFM > Transmit Loopback page is used to transmit **Loopback Messages (LBMs)**. These messages can be used to isolate or verify connectivity faults by submitting a request to a target node (i.e., a remote MEP or MIP) to echo the message back to the source.



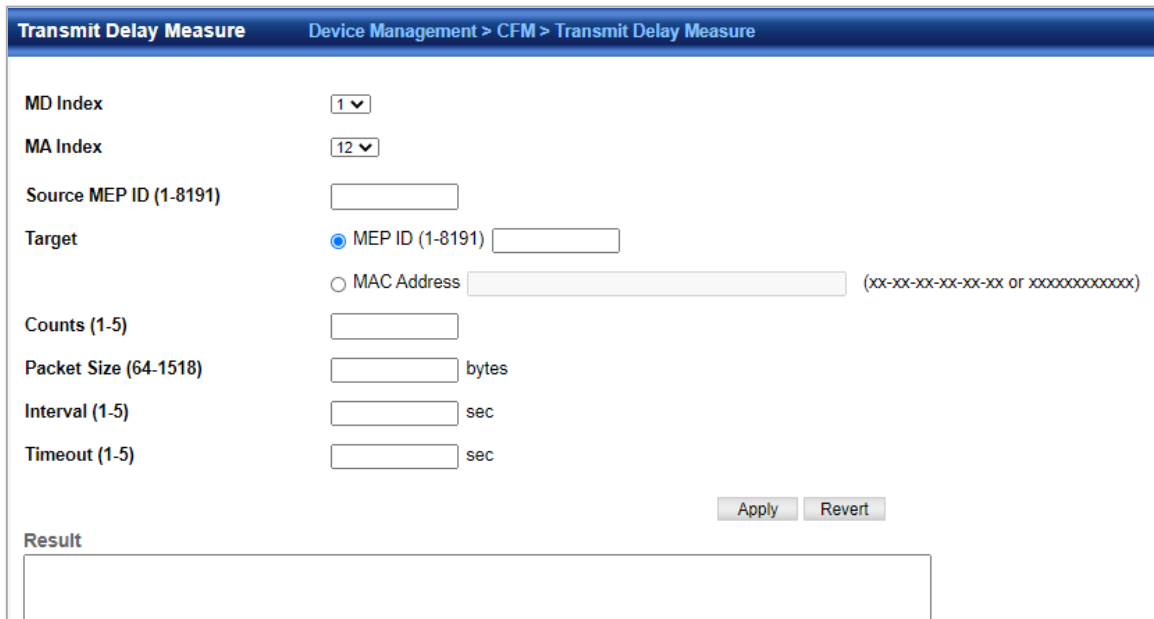
The screenshot shows the 'Transmit Loopback' configuration page. The breadcrumb navigation is 'Device Management > CFM > Transmit Loopback'. The page contains several input fields and a 'Test' button:

- MD Index:** A dropdown menu with '1' selected.
- MA Index:** A dropdown menu with '12' selected.
- Source MEP ID (1-8191):** An empty text input field.
- Target:** Two radio button options:
 - MEP ID (1-8191)** with an empty text input field.
 - MAC Address** with an empty text input field and a hint '(xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)'.
- Counts (1-1024):** An empty text input field.
- Packet Size (64-1518):** An empty text input field followed by the text 'bytes'.
- Test:** A button located to the right of the Packet Size field.
- Result:** A large empty text area at the bottom of the page.

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **Source MEP ID** – The identifier of a source MEP that will send the loopback message. (Range: 1-8191)
- ◆ **Target**
 - **MEP ID** – The identifier of a remote MEP that is the target of a loopback message. (Range: 1-8191)
 - **MAC Address** – MAC address of a remote MEP that is the target of a loopback message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx
- ◆ **Count** – The number of times the loopback message is sent. (Range: 1-1024)
- ◆ **Packet Size** – The size of the loopback message. (Range: 64-1518 bytes; Default: 64 bytes)

4.8.7.11 Transmit Delay Measure

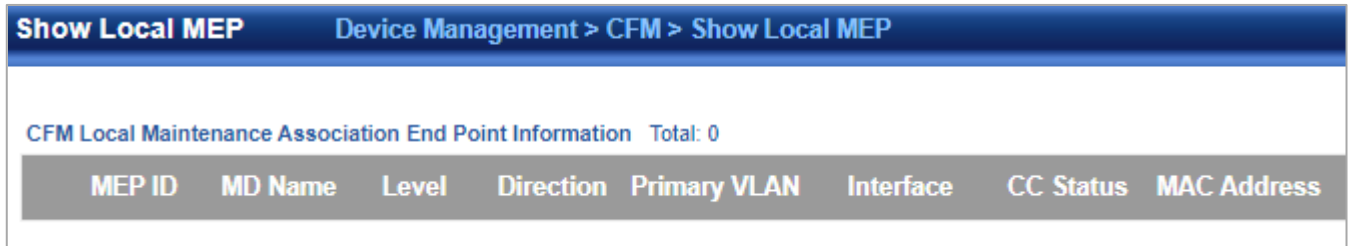
Device Management > CFM > Transmit Delay Measure page is used to send periodic delay-measure requests to a specified MEP within a maintenance association.



- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **Source MEP ID** – The identifier of a source MEP that will send the delay-measure message. (Range: 1-8191)
- ◆ **Target**
 - **MEP ID** – The identifier of a remote MEP that is the target of a delay-measure message. (Range: 1-8191)
 - **MAC Address** – MAC address of a remote MEP that is the target of a delay-measure message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx
- ◆ **Count** – The number of times to retry sending the message if no response is received before the specified timeout. (Range: 1-5; Default: 5)
- ◆ **Packet Size** – The size of the delay-measure message. (Range: 64-1518 bytes; Default: 64 bytes)
- ◆ **Interval** – The transmission delay between delay-measure messages. (Range: 1-5 seconds; Default: 1 second)
- ◆ **Timeout** – The timeout to wait for a response. (Range: 1-5 seconds; Default: 5 seconds)

4.8.7.12 Show Local MEP

Device Management > CFM > Show Local MEP page is used to show information for the MEPs configured on this device.



- ◆ **MEP ID** – Maintenance end point identifier.
- ◆ **MD Name** – Maintenance domain name.
- ◆ **Level** – Authorized maintenance level for this domain.
- ◆ **Direction** – Direction in which the MEP communicates CFM messages:
 - Down indicates that the MEP is facing away from the switch, and transmits CFM messages towards, and receives them from, the direction of the physical medium.
 - Up indicates that the MEP faces inward toward the switch cross connect matrix, and transmits CFM messages towards, and receives them from, the direction of the internal bridge relay mechanism.
- ◆ **Primary VLAN** – Service VLAN ID.
- ◆ **Interface** – Physical interface of this entry (either a port or trunk).
- ◆ **CC Status** – Shows administrative status of CCMs.
- ◆ **MAC Address** – MAC address of this MEP entry.

4.8.7.13 Show Local MEP Details

Device Management > CFM > Show Local MEP Details page is used to show detailed CFM information about a local MEP in the continuity check database.



- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MEP ID** – Maintenance end point identifier. (Range: 1-8191)
- ◆ **MD Name** – The maintenance domain for this entry.
- ◆ **MA Name** – Maintenance association to which this remote MEP belongs.
- ◆ **MA Name Format** – The format of the Maintenance Association name, including primary VID, character string, unsigned Integer 16, or RFC 2865 VPN ID.
- ◆ **Level** – Maintenance level of the local maintenance point.
- ◆ **Direction** – The direction in which the MEP faces on the Bridge port (up or down).
- ◆ **Interface** – The port to which this MEP is attached.
- ◆ **CC Status** – Shows if the MEP will generate CCM messages.
- ◆ **MAC Address** – MAC address of the local maintenance point. (If a CCM for the specified remote MEP has never been

received or the local MEP record times out, the address will be set to the initial value of all Fs.)

- ◆ **Defect Condition** – Shows the defect detected on the MEP.
- ◆ **Received RDI** – Receive status of **remote defect indication (RDI)** messages on the MEP.
- ◆ **AIS Status** – Shows if MEPs within the specified MA are enabled to send frames with AIS information following detection of defect conditions.
- ◆ **AIS Period** – The interval at which AIS information is sent.
- ◆ **AIS Transmit Level** – The maintenance level at which AIS information will be sent for the specified MEP.
- ◆ **Suppress Alarm** – Shows if the specified MEP is configured to suppress sending frames containing AIS information following the detection of defect conditions.
- ◆ **Suppressing Alarms** – Shows if the specified MEP is currently suppressing sending frames containing AIS information following the detection of defect conditions.

4.8.7.14 Show Local MIP

Device Management > CFM > Show Local MIP page is used to show the MIPs on this device discovered by the CFM protocol.

Show Local MIP		Device Management > CFM > Show Local MIP		
CFM Local Maintenance Association Intermediate Point Information Total: 0				
MD Name	Level	MA Name	Primary VLAN	Interface

- ◆ **MD Name** – Maintenance domain name.
- ◆ **Level** – Authorized maintenance level for this domain.
- ◆ **MA Name** – Maintenance association name.
- ◆ **Primary VLAN** – Service VLAN ID.
- ◆ **Interface** – Physical interface of this entry (either a port or trunk).

4.8.7.15 Show Remote MEP

Device Management > CFM > Show Remote MEP page is used to show MEPs located on other devices which have been discovered through continuity check messages, or statically configured in the MEP database and verified through cross-check messages.

Show Remote MEP		Device Management > CFM > Show Remote MEP			
CFM Remote Maintenance Association End Point Information Total: 0					
MEP ID	MA Name	Level	Primary VLAN	MEP Up	Remote MAC Address

- ◆ **MEP ID** – Maintenance end point identifier.
- ◆ **MA Name** – Maintenance association name.
- ◆ **Level** – Authorized maintenance level for this domain.
- ◆ **Primary VLAN** – Service VLAN ID.
- ◆ **MEP Up** – Indicates whether or not this MEP is functioning normally.
- ◆ **Remote MAC Address** – MAC address of the remote maintenance point. (If a CCM for the specified remote MEP has never been received or the remote MEP record times out, the address will be set to the initial value of all Fs.)

4.8.7.16 Show Remote MEP Details

Device Management > CFM > Show Remote MEP Details is used page to show detailed information for MEPs located on other devices which have been discovered through continuity check messages, or statically configured in the MEP database and verified through cross-check messages.



- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MEP ID** – Maintenance end point identifier. (Range: 1-8191)
- ◆ **MD Name** – Maintenance domain name.
- ◆ **MA Name** – Maintenance association name.
- ◆ **Level** – Authorized maintenance level for this domain.
- ◆ **MAC Address** – MAC address of this MEP entry.
- ◆ **Primary VLAN** – Service VLAN ID.
- ◆ **Incoming Port** – Port to which this remote MEP is attached.
- ◆ **CC Lifetime** – Length of time to hold messages about this MEP in the CCM database.
 - ◆ **Age of Last CC Message** – Length of time the last CCM message about this MEP has been in the CCM database.
 - ◆ **Frame Loss** – Percentage of transmitted frames lost.
 - ◆ **CC Packet Statistics** – The number of CCM packets received successfully and those with errors.
- ◆ **Port State** – Port states include:
 - Up – The port is functioning normally.
 - Blocked – The port has been blocked by the Spanning Tree Protocol.
 - No port state – Either no CCM has been received, or nor port status TLV was received in the last CCM.
- ◆ **Interface State** – Interface states include:
 - No Status – Either no CCM has been received, or no interface status TLV was received in the last CCM.
 - Up – The interface is ready to pass packets.
 - Down – The interface cannot pass packets.
 - Testing – The interface is in some test mode.
 - Unknown – The interface status cannot be determined for some reason.
 - Dormant – The interface is not in a state to pass packets but is in a pending state, waiting for some external event.
 - Not Present – Some component of the interface is missing.
 - isLowerLayerDown – The interface is down due to state of the lower layer interfaces.
- ◆ **Crosscheck Status** – Shows if crosscheck function has been enabled.

4.8.7.17 Show Link Trace Cache

Device Management > CFM > Show Link Trace Cache page is used to show information about link trace operations launched from this device.

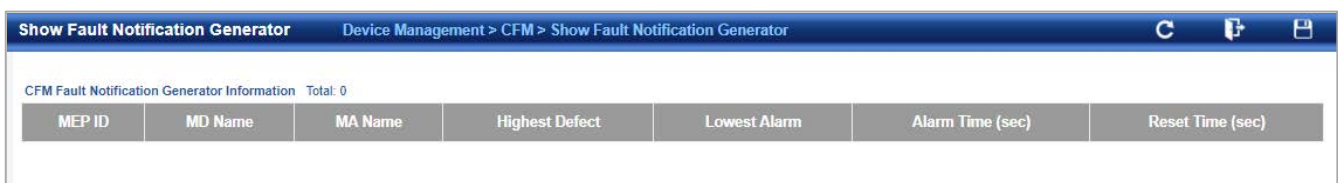


Hops	MA	IP Address/Alias	Forwarded	Ingress MAC Address	Egress MAC Address	Ingress Action	Egress Action	Reply

- ◆ **Hops** – The number hops taken to reach the target MEP.
- ◆ **MA** – Maintenance association name.
- ◆ **IP/Alias** – IP address or DNS alias of the target device's CPU.
- ◆ **Forwarded** – Shows whether or not this link trace message was forwarded. A message is not forwarded if received by the target MEP.
- ◆ **Ingress MAC Address** – MAC address of the ingress port on the target device.
- ◆ **Egress MAC Address** – MAC address of the egress port on the target device.
- ◆ **Ingress Action** – Action taken on the ingress port:
 - **IngOk** – The target data frame passed through to the MAC Relay Entity.
 - **IngDown** – The bridge port's MAC_Operational parameter is false. This value could be returned, for example, by an operationally Down MEP that has another Down MEP at a higher MD level on the same bridge port that is causing the bridge port's MAC_Operational parameter to be false.
 - **IngBlocked** – The ingress port can be identified, but the target data frame was not forwarded when received on this port due to active topology management, i.e., the bridge port is not in the forwarding state.
 - **IngVid** – The ingress port is not in the member set of the LTM's VIDs, and ingress filtering is enabled, so the target data frame was filtered by ingress filtering.
- ◆ **Egress Action** – Action taken on the egress port:
 - **EgrOk** – The targeted data frame was forwarded.
 - **EgrDown** – The Egress Port can be identified, but that bridge port's MAC_Operational parameter is false.
 - **EgrBlocked** – The egress port can be identified, but the data frame was not passed through the egress port due to active topology management, i.e., the bridge port is not in the forwarding state.
 - **EgrVid** – The Egress Port can be identified, but the bridge port is not in the LTM's VID member set, and was therefore filtered by egress filtering.
- ◆ **Reply** – Reply action:
 - **FDB** – Target address found in forwarding database.
 - **MPDB** – Target address found in the maintenance point database.
 - **HIT** – Target located on this device.

4.8.7.18 Show Fault Notification Generator

Device Management > CFM > Show Fault Notification Generator page is used to display configuration settings for the fault notification generator.



MEP ID	MD Name	MA Name	Highest Defect	Lowest Alarm	Alarm Time (sec)	Reset Time (sec)

- ◆ **MEP ID** – Maintenance end point identifier.
- ◆ **MD Name** – Maintenance domain name.
- ◆ **MA Name** – Maintenance association name.
- ◆ **Highest Defect** – The highest defect that will generate a fault alarm. (This is disabled by default.)
- ◆ **Lowest Alarm** – The lowest defect that will generate a fault alarm.
- ◆ **Alarm Time** – The time a defect must exist before a fault alarm is issued.
- ◆ **Reset Time** – The time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued.

4.8.7.19 Show Continuity Check Error

Device Management > CFM > Show Continuity Check Error page is used to display the CFM continuity check errors logged on this device.

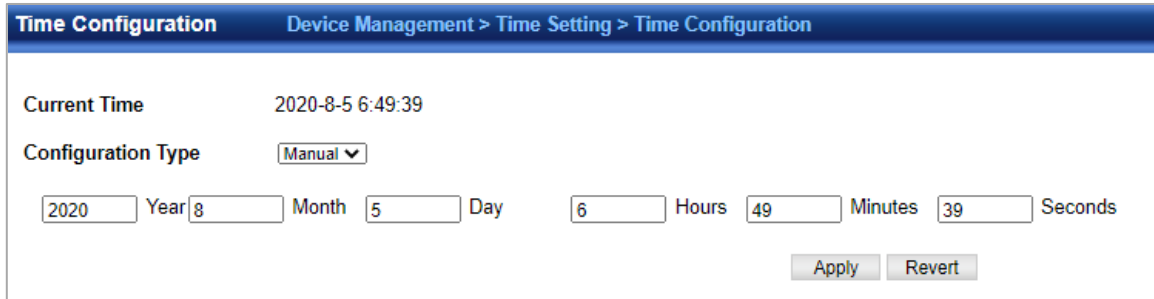
Show Continuity Check Error		Device Management > CFM > Show Continuity Check Error				
CFM Continuity Check Error Information Total: 0						
Level	Primary VLAN	MEP ID	Interface	Remote MAC	Reason	MA Name

- ◆ **Level** – Maintenance level associated with this entry.
- ◆ **Primary VLAN** – VLAN in which this error occurred.
- ◆ **MEP ID** – Identifier of remote MEP.
- ◆ **Interface** – Port at which the error was recorded.
- ◆ **Remote MAC** – MAC address of remote MEP.
- ◆ **Reason** – Error types include:
 - **LEAK** – MA x is associated with a specific VID list¹⁴, one or more of the VIDs in this MA can pass through the bridge port, no MEP is configured facing outward (down) on any bridge port for this MA, and some other MA y, at a higher maintenance level, and associated with at least one of the VID(s) also in MA x, does have a MEP configured on the bridge port.
 - **VIDS** – MA x is associated with a specific VID list¹⁴, an MEP is configured facing inward (up) on this MA on the bridge port, and some other MA y, associated with at least one of the VID(s) also in MA x, also has an Up MEP configured facing inward (up) on some bridge port.
 - **EXCESS_LEV** – The number of different MD levels at which MIPs are to be created on this port exceeds the bridge's capabilities.
 - **OVERLAP_LEV** – A MEP is created for one VID at one maintenance level, but a MEP is configured on another VID at an equivalent or higher level, exceeding the bridge's capabilities.
- ◆ **MA Name** – The maintenance association for this entry.

4.8.8 Time Setting

4.8.8.1 Time Configuration

The Device Management > Time Setting > Time Configuration page is used to set the system time on the switch manually without using SNTP.



Time Configuration Device Management > Time Setting > Time Configuration

Current Time 2020-8-5 6:49:39

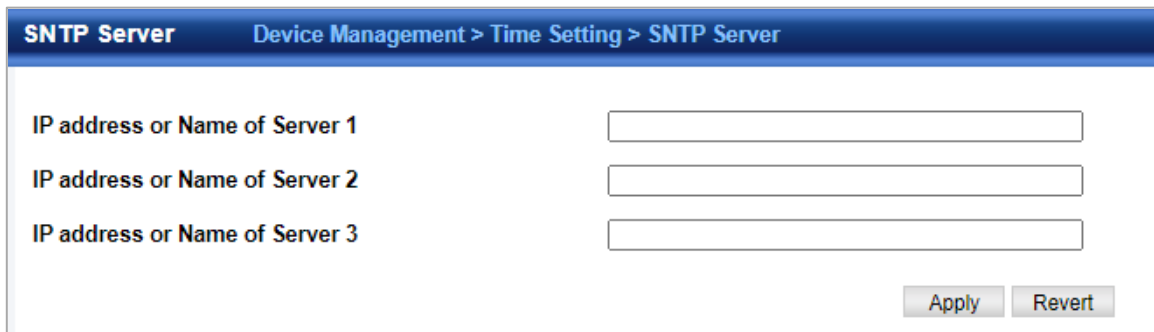
Configuration Type

Year Month Day Hours Minutes Seconds

- ◆ **Current Time** – Shows the current time set on the switch.
- ◆ **Hours** – Sets the hour. (Range: 0-23)
- ◆ **Minutes** – Sets the minute value. (Range: 0-59)
- ◆ **Seconds** – Sets the second value. (Range: 0-59)
- ◆ **Month** – Sets the month. (Range: 1-12)
- ◆ **Day** – Sets the day of the month. (Range: 1-31)
- ◆ **Year** – Sets the year. (Range: 1970-2037)

4.8.8.2 SNTP Server

The Device Management > Time Setting > SNTP Server page is used to specify the IP address for up to three SNTP time servers.



SNTP Server Device Management > Time Setting > SNTP Server

IP address or Name of Server 1

IP address or Name of Server 2

IP address or Name of Server 3

- ◆ **SNTP Server IP Address** – Sets the IPv4 or IPv6 address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

4.8.8.3 NTP Server

The Device Management > Time Setting > NTP Server page is used to add the IP address for up to 50 NTP time servers.

NTP Server		Device Management > Time Setting > NTP Server	
NTP Server List Total: 1			
<input type="checkbox"/>	Server Address	Authentication Key	Version
<input type="checkbox"/>	10.1.1.12		3
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>			

- ◆ **NTP Server IP Address** – Adds the IPv4 or IPv6 address for up to 50 time servers. The switch will poll the specified time servers for updates when the clock maintenance type is set to NTP on the System > Time (Configure General) page. It issues time synchronization requests at a fixed interval of 1024 seconds. The switch will poll all the time servers configured, the responses received are filtered and compared to determine the most reliable and accurate time update for the switch.
- ◆ **Version** – Specifies the NTP version supported by the server. (Fixed: Version 3)
- ◆ **Authentication Key** – Specifies the number of the key in the NTP Authentication Key List to use for authentication with the configured server. NTP authentication is optional. If enabled on the System > Time (Configure General) page, you must also configure at least one key on the System > Time (Add NTP Authentication Key) page. (Range: 1-65535)

4.8.8.4 NTP authentication Key

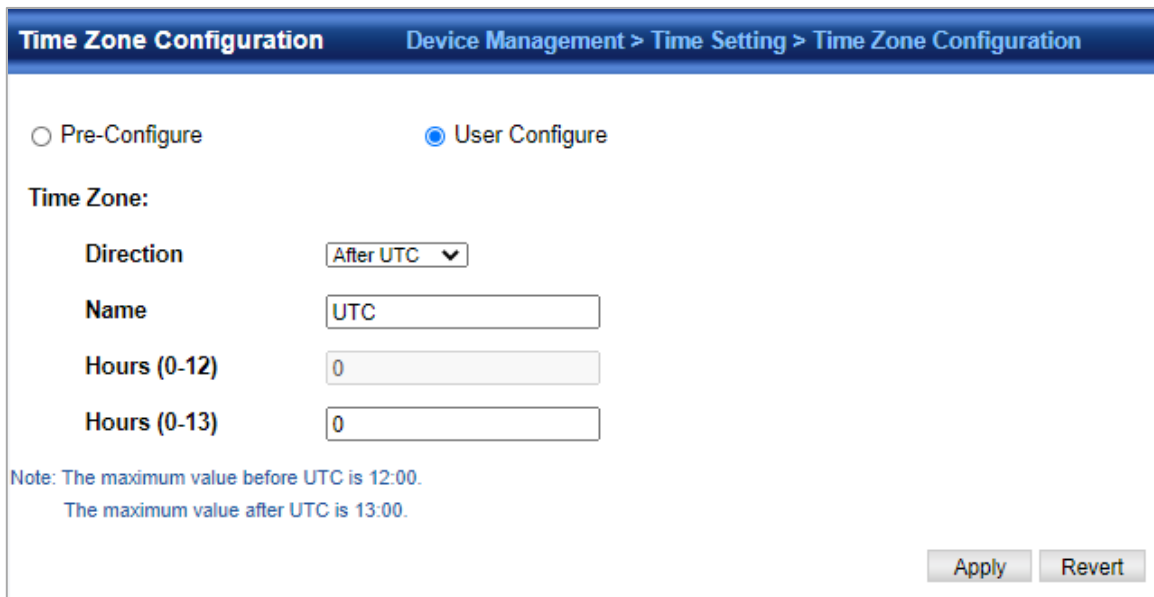
The Device Management > Time Setting > NTP Authentication Key page is used to add an entry to the authentication key list.

NTP Authentication Key		Device Management > Time Setting > NTP Authentication Key	
NTP Authentication Key List Total: 1			
<input type="checkbox"/>	Authentication Key	Key Context	
<input type="checkbox"/>	12	3L6497	
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>			

- ◆ **Authentication Key** – Specifies the number of the key in the NTP Authentication Key List to use for authentication with a configured server. NTP authentication is optional. When enabled on the System > Time (Configure General) page, you must also configure at least one key on this page. Up to 255 keys can be configured on the switch. (Range: 1-65535)
- ◆ **Key Context** – An MD5 authentication key string. The key string can be up to 32 case-sensitive printable ASCII characters (no spaces). NTP authentication key numbers and values must match on both the server and client.

4.8.8.5 Time Zone Configuration

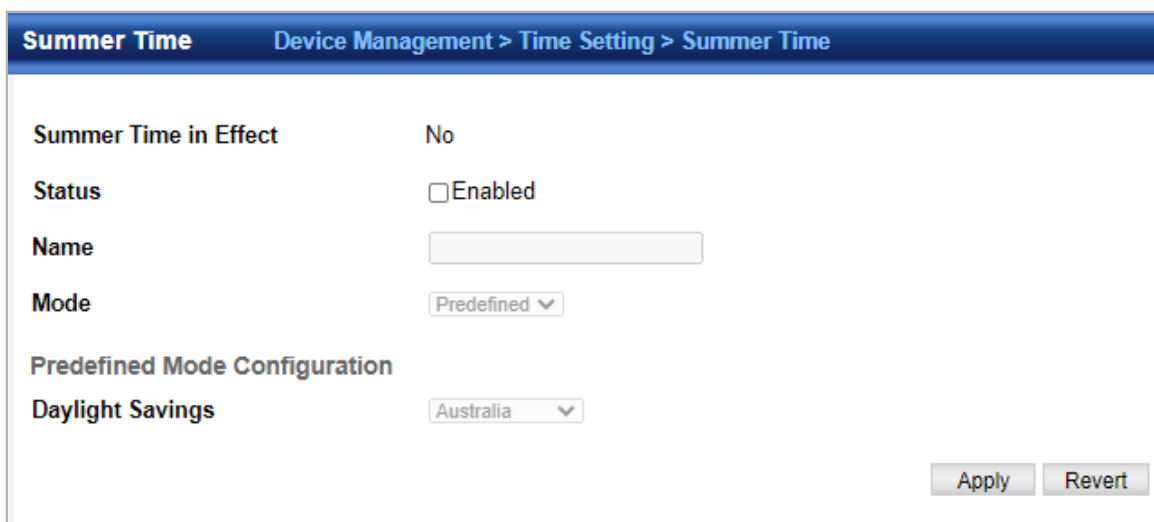
The Device Management > Time Setting > Time Zone Configuration page is used to set the time zone.



- ◆ **Direction:** Configures the time zone to be before (east of) or after (west of) UTC.
- ◆ **Name** – Assigns a name to the time zone. (Range: 1-30 characters)
- ◆ **Hours (0-13)** – The number of hours before/after UTC. The maximum value before UTC is 12. The maximum value after UTC is 13.
- ◆ **Minutes (0-59)** – The number of minutes before/after UTC.

4.8.8.6 Summer Time

The Device Management > Time Setting > Summer Time page is used to set the system clock forward during the summer months (also known as daylight savings time). In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.



- ◆ **Summer Time in Effect** – Shows if the system time has been adjusted.
- ◆ **Status** – Shows if summer time is set to take effect during the specified period.
- ◆ **Name** – Name of the time zone while summer time is in effect, usually an acronym. (Range: 1-30 characters)
- ◆ **Mode** – Selects one of the following configuration modes. (The Mode option can only be managed when the Summer Time

Status option has been set to enabled for the switch.)

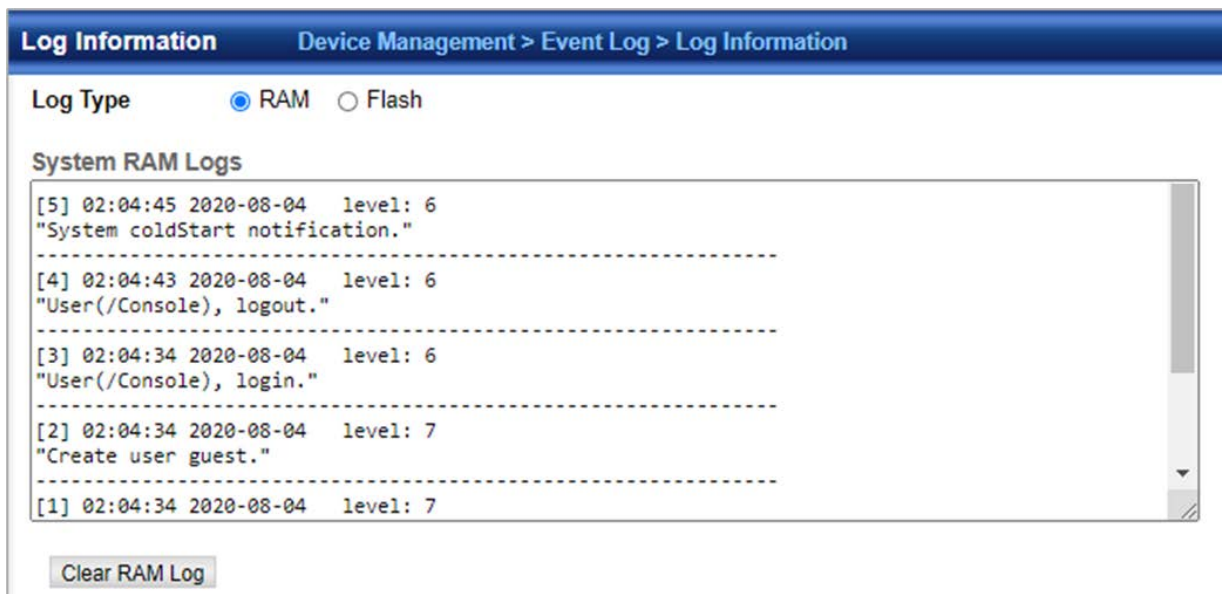
- **Predefined Mode** – Configures the summer time status and settings for the switch using predefined configurations for several major regions of the world. To specify the time corresponding to your local time when summer time is in effect, select the predefined summer-time zone appropriate for your location.
 - **Date Mode** – Sets the start, end, and offset times of summer time for the switch on a one-time basis. This mode sets the summer-time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summertime zone deviates from your regular time zone.
 - ◆ **Offset** – Summer-time offset from the regular time zone, in minutes. (Range: 1-120 minutes)
 - ◆ **From** – Start time for summer-time offset.
 - ◆ **To** – End time for summer-time offset.
- Recurring Mode** – Sets the start, end, and offset times of summer time for the switch on a recurring basis. This mode sets the summer-time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summertime zone deviates from your regular time zone.
- ◆ **Offset** – Summer-time offset from the regular time zone, in minutes. (Range: 1-120 minutes)
 - ◆ **From** – Start time for summer-time offset.
 - ◆ **To** – End time for summer-time offset.

4.8.9 Event Log

4.8.9.1 Log Information

The Device Management > Event Log > Log Information page is used to display System Logs

This page allows you to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset) and up to 4096 entries in permanent flash memory.



4.8.9.2 Global Configuration

The Device Management > Event Log > Global Configuration page is used to enable or disable event logging, and specify which levels are logged to RAM or flash memory. Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory. The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

Global Configuration
Device Management > Event Log > Global Configuration

Status Enabled

Min Log Level of Flash 3 - Error ▼

Min Log Level of RAM 7 - Debugging ▼

Note: The log level of flash must be equal to or less than the log level of RAM.

- ◆ **Status** – Enables/disables the logging of debug or error messages to the logging process. (Default: Enabled)
- ◆ **History Flash Level** – Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. (Range: 0-7, Default: 3)
- ◆ **History RAM Level** – Limits log messages saved to the switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7)

4.8.9.3 Remote Log Server

The Device Management > Event Log > Remote Log Server page is used to send log messages to syslog servers or other management stations.

Remote Log Server
Device Management > Event Log > Remote Log Server

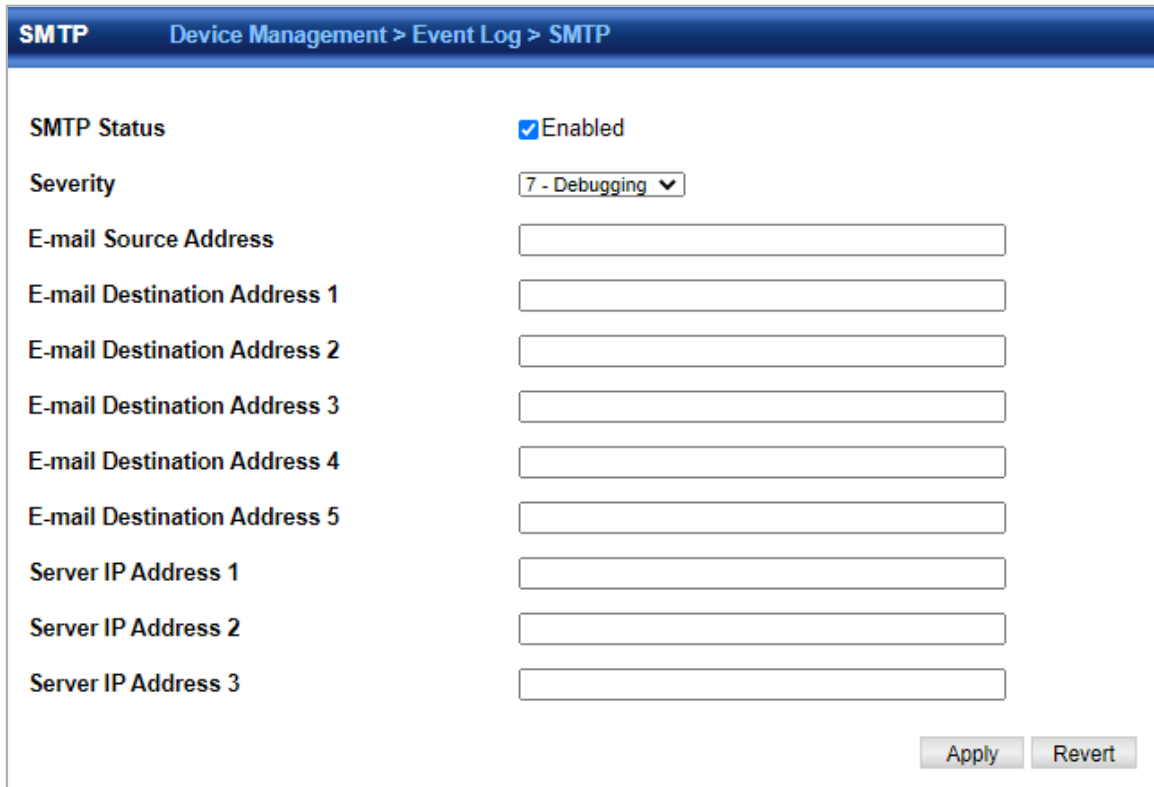
Min Log Level of Remote Server 7 - Debugging messages ▼

Server IP Address 1	<input type="text"/>	Port	<input type="text"/>
Server IP Address 2	<input type="text"/>	Port	<input type="text"/>
Server IP Address 3	<input type="text"/>	Port	<input type="text"/>
Server IP Address 4	<input type="text"/>	Port	<input type="text"/>
Server IP Address 5	<input type="text"/>	Port	<input type="text"/>

- ◆ **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- ◆ **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service.
- ◆ The attribute specifies the facility type tag sent in syslog messages (see RFC 3164). This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)
- ◆ **Logging Trap Level** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)
- ◆ **Server IP Address** – Specifies the IPv4 or IPv6 address of a remote server which will be sent syslog messages.

4.8.9.4 SMTP

The Device Management > Event Log > SMTP page is used to alert system administrators of problems by sending SMTP (Simple Mail Transfer Protocol) email messages when triggered by logging events of a specified level. The messages are sent to specified SMTP servers on the network and can be retrieved using POP or IMAP clients.



The screenshot shows the configuration interface for SMTP. At the top, the breadcrumb path is 'Device Management > Event Log > SMTP'. The main configuration area contains the following elements:

- SMTP Status:** A checkbox labeled 'Enabled' which is checked.
- Severity:** A dropdown menu currently set to '7 - Debugging'.
- E-mail Source Address:** A single-line text input field.
- E-mail Destination Address 1 through 5:** Five separate single-line text input fields for specifying email recipients.
- Server IP Address 1 through 3:** Three separate single-line text input fields for specifying SMTP server addresses.
- Buttons:** 'Apply' and 'Revert' buttons located at the bottom right of the configuration area.

- ◆ **SMTP Status** – Enables/disables the SMTP function. (Default: Enabled)
- ◆ **Severity** – Sets the syslog severity threshold level used to trigger alert messages. All events at this level or higher will be sent to the configured email recipients. For example, using Level 7 will report all events from level 7 to level 0. (Default: Level 7)
- ◆ **Email Source Address** – Sets the email address used for the “From” field in alert messages. You may use a symbolic email address that identifies the switch, or the address of an administrator responsible for the switch. (Range: 1-41 characters)
- ◆ **Email Destination Address** – Specifies the email recipients of alert messages. You can specify up to five recipients.
- ◆ **Server IP Address** – Specifies a list of up to three recipient SMTP servers. IPv4 or IPv6 addresses may be specified. The switch attempts to connect to the listed servers in sequential order if the first server fails to respond. For host name-to-IP address translation to function properly, host name lookup must be enabled, and one or more DNS servers specified.

4.8.10 File Management

Device Management> File Management page is used to manage the file in device.

User can upload configuration file to PC, download runtime file to device. Copy a configuration file to another configuration file.

File Management					
Device Management > File Management					
File List Total: 3					
<input type="checkbox"/>	File Name	File Type	Status	Modify Time	Size (bytes)
<input type="checkbox"/>	SGS-5240-24T4X_0804	Image	Active	2020-08-04 07:28:29	20179348
<input type="checkbox"/>	Factory_Default_Config.cfg	Config File	Inactive	2020-07-23 09:14:34	672
<input type="checkbox"/>	startup1.cfg	Config File	Active	2020-08-04 02:07:22	1876
<input type="button" value="Boot"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>					

4.8.10.1 File download

In the Device Management> File Management page, click copy button to download firmware or configuration settings using FTP, TFTP or HTTP.

Copy Type HTTP Download ▼

File Type Config File ▼

Source File Name startup1.cfg ▼

- ◆ **Copy Type** – The firmware copy operation includes these options:
 - FTP Upload – Copies a file from an FTP server to the switch.
 - HTTP Upload– Copies a file from a management station to the switch.
 - TFTP Upload – Copies a file from a TFTP server to the switch.
- ◆ **FTP/TFTP Server IP Address** – The IP address of an FTP/TFTP server.
- ◆ **User Name** – The user name for FTP server access.
- ◆ **Password** – The password for FTP server access.
- ◆ **File Type** – Specify Operation Code to copy firmware.

4.8.10.2 Saving Configuration

In the Device Management> File Management page, click copy button to save the current configuration settings to a local file on the switch. The configuration settings are not automatically saved by the system for subsequent use when the switch is rebooted. You must save these settings to the current startup file, or to another file which can be subsequently set as the startup file.

Copy Type

Destination File Name startup1.cfg

4.8.10.3 Setting The BOOT File

In the Device Management> File Management page, click Boot button to set the firmware or configuration file used for system initialization.

Copy Type

File Type

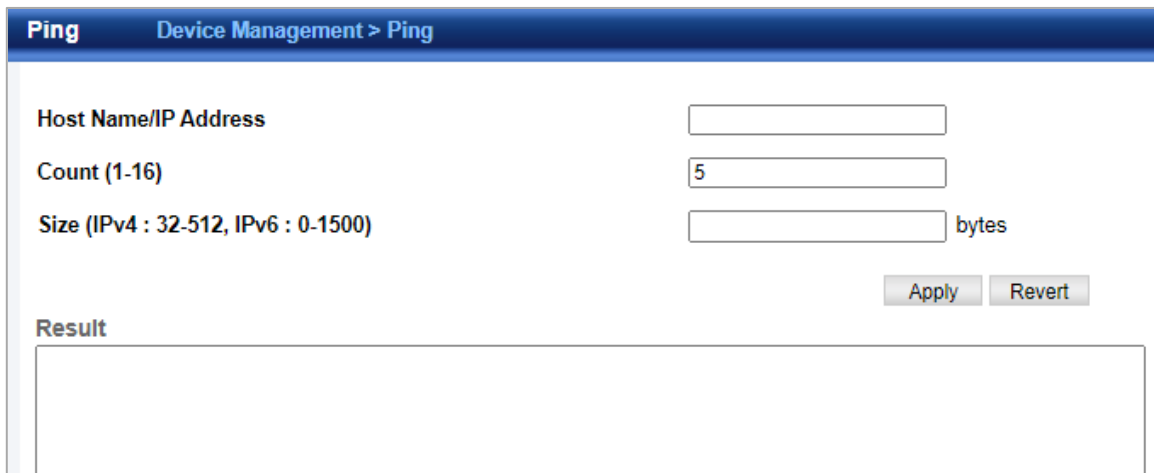
Source File Name 未選擇任何檔案

Destination File Name SGS-5240-24T4X_0804

Note: During firmware upload, the switch may not respond to commands for a couple of minutes.

4.8.11 Ping

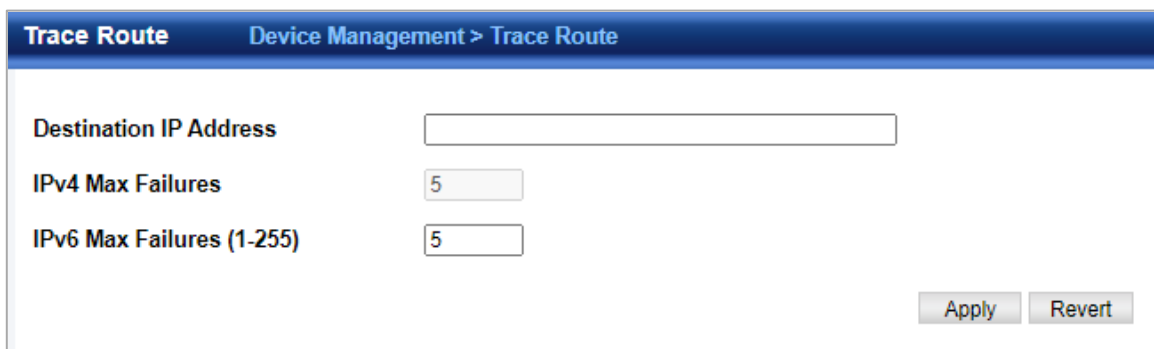
The Device Management > Ping page is used to send ICMP echo request packets to another node on the network.



- ◆ **Host Name/IP Address** – IP address or alias of the host.
- ◆ **Probe Count** – Number of packets to send. (Range: 1-16)
- ◆ **Packet Size** – Number of bytes in a packet. (Range: 32-512 bytes) The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

4.8.12 Trace Route

The Device Management > Trace Route page is used to show the route packets take to the specified destination.



- ◆ **Destination IP Address** – Alias or IPv4/IPv6 address of the host.
- ◆ **IPv4 Max Failures** – The maximum number of failures before which the trace route is terminated. (Fixed: 5)
- ◆ **IPv6 Max Failures** – The maximum number of failures before which the trace route is terminated. (Range: 1-255; Default: 5)

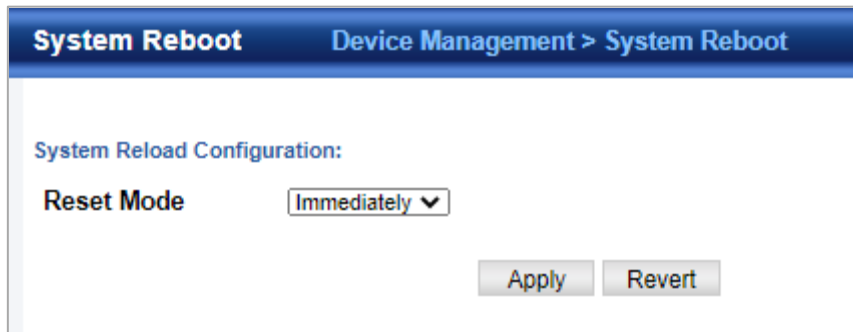
Command Usage

- ◆ Use the trace route function to determine the path taken to reach a specified destination.
- ◆ A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.
- ◆ The trace route function first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an “ICMP port unreachable” message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the “Request Timed Out” message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example,

FE80::7272%1 identifies VLAN 1 as the interface from which the trace route is sent.

4.8.13 System Reboot

The Device Management > System Reboot page is used to restart the switch immediately, at a specified time, after a specified delay, or at a periodic interval.



The screenshot shows the 'System Reboot' configuration page. The page title is 'System Reboot' and the breadcrumb is 'Device Management > System Reboot'. Under the heading 'System Reload Configuration:', there is a 'Reset Mode' label and a dropdown menu currently set to 'Immediately'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

5. SWITCH OPERATION

5.1 Address Table

The SGS-5240 series 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 SGS-5240 Series switch.

5.2 Learning

When one packet comes in from any port, the SGS-5240 series 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 SGS-5240 Series Switch, it will also check the destination address besides the source address learning. The SGS-5240 series 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 SGS-5240 series 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 SGS-5240 series 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 SGS-5240 series 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 SGS-5240 Series 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 SGS-5240 series performs "**Store and Forward**"; therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

5.5 Auto-Negotiation

The STP ports on the 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 SGS-5240 series is not functioning properly, make sure the SGS-5240 series 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 SGS-5240 Series PoE **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 SGS-5240 Series PoE **Switch**. If the SGS-5240 series 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.

■ 100BASE-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. DC wire or AC power cord is not inserted or faulty.
2. Check that the DC wire/AC power cord is inserted correctly.
3. Replace the DC wire/AC power cord if the cord is inserted correctly; check that the DC/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 DC/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-

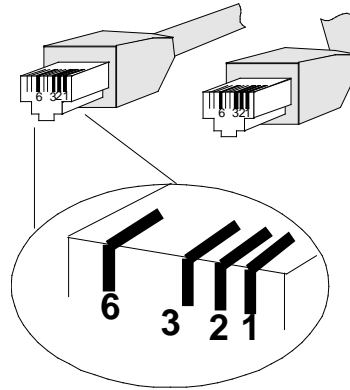
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

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	MDI-X
	Media Dependent Interface	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																																
<table border="0"> <tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr> </table>	1	2	3	4	5	6	7	8									1	2	3	4	5	6	7	8	SIDE 1	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown								
1	2	3	4	5	6	7	8																												
1	2	3	4	5	6	7	8																												
	SIDE 2																																		
Crossover Cable		SIDE 1	SIDE 2																																
<table border="0"> <tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr> </table>	1	2	3	4	5	6	7	8																	1	2	3	4	5	6	7	8	SIDE 1	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Green 2 = Green 3 = White / Orange 4 = Blue 5 = White / Blue 6 = Orange 7 = White / Brown 8 = Brown
1	2	3	4	5	6	7	8																												
1	2	3	4	5	6	7	8																												
	SIDE 2																																		

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 **C**ontinuity **C**heck. 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 **C**ontinuity **C**heck **M**essage. 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 **C**isco **D**iscovery **P**rotocol.

D

DEI

DEI is an acronym for **D**rop **E**ligible **I**ndicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for **D**ata **E**ncryption **S**tandard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for **D**ynamic **H**ost **C**onfiguration **P**rotocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

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

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID. 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 **I**nternet **M**essage **A**ccess **P**rotocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, 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 **I**nternet **P**rotocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over 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 **I**P **M**ulticast.

IP Source Guard

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

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol allows bundling several physical ports together to form a single logical port.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The **L**ink **L**ayer **D**iscovery **P**rotocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management 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 **L**oss **O**f **C**onnectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M**MAC Table**

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

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for **M**aintenance **E**ntity **E**ndpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for **M**essage-**D**igest 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 implement the Ethernet physical layer (IEEE-802.3).

PING

Ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

Ping uses Internet Control Message Protocol (ICMP) packets. The Ping Request is the packet from the origin computer, and the Ping Reply is the packet response from the target.

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.

Pepo

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**u's **C**ontrol **E**ntry. It describes Qu's 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 Qu's classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

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

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific Qu's 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.

Qu's

Qu's 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 Qu's becomes the secret to a successful end-to-end business solution. Therefore, Qu's is the set of techniques to manage network resources.

Qu's 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 Qu's class. There is a one to one mapping between Qu's class, queue and priority. A Qu's 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 login, 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**ivial **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.