



Questo manuale d'istruzione è fornito da trovaprezzi.it. Scopri tutte le offerte per [Planet GS-4210-24P2S](#) o cerca il tuo prodotto tra le [migliori offerte di Switch](#)



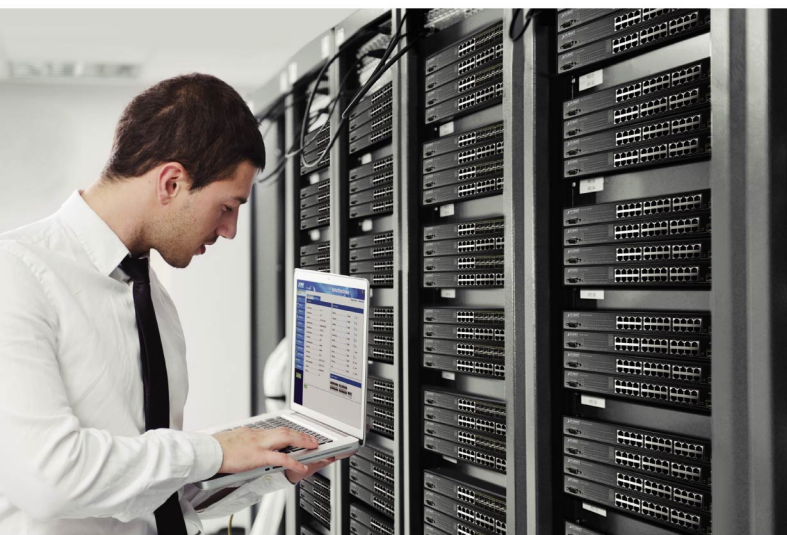
Questo manuale d'istruzione è fornito da trovaprezzi.it. Scopri tutte le offerte per [Planet GS-4210-24P2S](#) o cerca il tuo prodotto tra le [migliori offerte di Switch](#)



User's Manual

**16/24-Port 10/100/1000T +
2-Port 100/1000X SFP
Managed Switch**

▶ **GS-4210-16T2S/GS-4210-24T2S/
GS-4210-24P2S**



Trademarks

Copyright © PLANET Technology Corp. 2015.

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 is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

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 16/24-Port 10/100/1000T + 2-Port 100/1000X SFP Managed Switch User's Manual

FOR MODELS: GS-4210-16T2S / GS-4210-24T2S / GS-4210-24P2S

REVISION: 1.0 (MARCH 2015)

Part No: EM-GS-4210-16T2S_24T2S_24P2S_v1.0

TABLE OF CONTENTS

1. INTRODUCTION	12
1.1 Package Contents	12
1.2 Product Description	13
1.3 How to Use This Manual	15
1.4 Product Features	16
1.5 Product Specifications	19
2. INSTALLATION	25
2.1 Hardware Description	25
2.1.1 Switch Front Panel	25
2.1.2 LED Indications	26
2.1.3 Switch Rear Panel	29
2.2 Installing the Switch.....	30
2.2.1 Desktop Installation	30
2.2.2 Rack Mounting.....	31
2.2.3 Installing the 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	40
4. WEB CONFIGURATION	42
4.1 Main Web Page	45
4.1.1 Save Button	47
4.1.2 Configuration Manager	47
4.1.2.1 Saving Configuration	48
4.2 System.....	50

4.2.1 System Information.....	50
4.2.2 IP Configuration.....	51
4.2.3 IPv6 Configuration.....	53
4.2.4 User Configuration.....	55
4.2.5 Time Settings.....	56
4.2.5.1 System Time.....	56
4.2.5.2 SNTP Configuration.....	59
4.2.6 Log Management.....	60
4.2.6.1 Logging Service.....	60
4.2.6.2 Local Logging.....	61
4.2.6.3 Remote Syslog.....	62
4.2.6.4 Logging Message.....	64
4.2.7 SNMP Management.....	66
4.2.7.1 SNMP Overview.....	66
4.2.7.2 SNMP Setting.....	67
4.2.7.3 SNMP View.....	68
4.2.7.4 SNMP Access Group.....	69
4.2.7.5 SNMP Community.....	71
4.2.7.6 SNMP User.....	72
4.2.7.7 SNMPv1, 2 Notification Recipients.....	74
4.2.7.8 SNMPv3 Notification Recipients.....	75
4.2.7.9 SNMP Engine ID.....	77
4.2.7.10 SNMP Remote Engine ID.....	78
4.3 Port Management.....	79
4.3.1 Port Configuration.....	79
4.3.2 Port Counters.....	82
4.3.3 Bandwidth Utilization.....	87
4.3.4 Port Mirroring.....	88
4.3.5 Jumbo Frame.....	90
4.3.6 Port Error Disabled Configuration.....	91
4.3.7 Port Error Disabled Status.....	93
4.3.8 Protected Ports.....	94
4.3.9 EEE.....	96
4.4 Link Aggregation.....	98
4.4.1 LAG Setting.....	100
4.4.2 LAG Management.....	101
4.4.3 LAG Port Setting.....	102
4.4.4 LACP Setting.....	104
4.4.5 LACP Port Setting.....	105

4.4.6 LAG Status	106
4.5 VLAN.....	109
4.5.1 VLAN Overview	109
4.5.2 IEEE 802.1Q VLAN	110
4.5.3 Management VLAN	113
4.5.4 Create VLAN	114
4.5.5 Interface Settings.....	115
4.5.6 Port to VLAN.....	119
4.5.7 Port VLAN Membership.....	121
4.5.8 Protocol VLAN Group Setting	122
4.5.9 Protocol VLAN Port Setting	123
4.5.10 GVRP Setting	125
4.5.11 GVRP Port Setting	126
4.5.12 GVRP VLAN	128
4.5.13 GVRP Statistics	128
4.5.14 VLAN setting example:	130
4.5.14.1 Two separate 802.1Q VLANs	130
4.5.14.2 VLAN Trunking between two 802.1Q aware switch	133
4.6 Spanning Tree Protocol	136
4.6.1 Theory	136
4.6.2 STP Global Settings	142
4.6.3 STP Port Setting	144
4.6.4 CIST Instance Setting	147
4.6.5 CIST Port Setting	150
4.6.6 MST Instance Configuration	153
4.6.7 MST Port Setting	155
4.6.8 STP Statistics	158
4.7 Multicast.....	160
4.7.1 Properties	160
4.7.2 IGMP Snooping	162
4.7.2.1 IGMP Setting	166
4.7.2.2 IGMP Querier Setting	168
4.7.2.3 IGMP Static Group.....	169
4.7.2.4 IGMP Group Table	170
4.7.2.5 IGMP Router Setting	171
4.7.2.6 IGMP Router Table	172
4.7.2.7 IGMP Forward All	174
4.7.3 IGMP Snooping Statics.....	175
4.7.4 MLD Snooping.....	177

4.7.4.1 MLD Setting.....	177
4.7.4.2 MLD Static Group	179
4.7.4.3 MLD Group Table	180
4.7.4.4 MLD Router Setting.....	180
4.7.4.5 MLD Router Table.....	182
4.7.4.6 MLD Forward All	183
4.7.5 MLD Snooping Statics	184
4.7.6 Multicast Throttling Setting	186
4.7.7 Multicast Filter	188
4.7.7.1 Multicast Profile Setting.....	188
4.7.7.2 IGMP Filter Setting	190
4.7.7.3 MLD Filtering	191
4.8 Quality of Service	192
4.8.1 Understand QoS.....	192
4.8.2 General.....	193
4.8.2.1 QoS Properties	193
4.8.2.2 QoS Port Settings.....	194
4.8.2.3 Queue Settings.....	196
4.8.2.4 CoS Mapping.....	197
4.8.2.5 DSCP Mapping.....	198
4.8.2.6 IP Precedence Mapping	201
4.8.3 QoS Basic Mode.....	203
4.8.3.1 Global Settings	203
4.8.3.2 Port Settings	204
4.8.4 QoS Advanced Mode.....	206
4.8.4.1 Global Settings	206
4.8.4.2 Class Mapping.....	207
4.8.4.3 Aggregate Police	208
4.8.4.4 Policy Table	209
4.8.4.5 Policy Class Maps	210
4.8.4.6 Policy Binding	212
4.8.5 Rate Limit	214
4.8.5.1 Ingress Bandwidth Control	214
4.8.5.2 Ingress VLAN Settings	216
4.8.5.3 Egress Bandwidth Control	217
4.8.5.4 Egress Queue Settings.....	219
4.8.6 Voice VLAN	221
4.8.6.1 Introduction to Voice VLAN.....	221
4.8.6.2 Properties	221
4.8.6.3 Telephony OUI MAC Setting.....	223

4.8.6.4 Telephony OUI Port Setting	225
4.9 Security	227
4.9.1 Storm Control.....	227
4.9.1.1 Global Setting	227
4.9.1.2 Port Setting.....	228
4.9.2 802.1X	230
4.9.2.1 Understanding IEEE 802.1X Port-based Authentication	231
4.9.2.2 802.1X Setting	234
4.9.2.3 802.1X Port Setting	235
4.9.2.4 Guest VLAN Setting	237
4.9.2.5 Authenticated Host	240
4.9.3 DHCP Snooping	241
4.9.3.1 DHCP Snooping Overview	241
4.9.3.2 Global Setting	242
4.9.3.3 VLAN Setting	243
4.9.3.4 Port Setting.....	245
4.9.3.5 Statistics	247
4.9.3.6 Rate Limit	248
4.9.3.7 Option82 Global Setting	250
4.9.3.8 Option82 Port Setting	251
4.9.3.9 Option82 Circuit-ID Setting.....	253
4.9.4 Dynamic ARP Inspection	254
4.9.4.1 Global Setting	254
4.9.4.2 VLAN Setting	255
4.9.4.3 Port Setting.....	256
4.9.4.4 Statistics	258
4.9.4.5 Rate Limit	259
4.9.5 IP Source Guard	260
4.9.5.1 Port Settings	261
4.9.5.2 Binding Table	263
4.9.6 Port Security	264
4.9.7 DoS	267
4.9.7.1 Global DoS Setting	267
4.9.7.2 DoS Port Setting.....	270
4.9.8 AAA	272
4.9.8.1 Login List	273
4.9.8.2 Enable List.....	274
4.9.8.3 Accounting List	275
4.9.8.4 Accounting Update	276
4.9.9 TACACS+ Server.....	277

4.9.10 RADIUS Server	279
4.9.11 Access	282
4.9.11.1 Console	282
4.9.11.2 Telnet	284
4.9.11.3 HTTP	286
4.9.11.4 HTTPs	287
4.10 ACL	288
4.10.1 MAC-based ACL	288
4.10.2 MAC-based ACE	289
4.10.3 IPv4-based ACL	293
4.10.4 IPv4-based ACE	294
4.10.5 IPv6-based ACL	299
4.10.6 IPv6-based ACE	300
4.10.7 ACL Binding	305
4.11 MAC Address Table	306
4.11.1 Static MAC Setting	306
4.11.2 MAC Filtering	307
4.11.3 Dynamic Address Setting	308
4.11.4 Dynamic Learned	309
4.11.5 RMA Setting	310
4.12 LLDP	312
4.12.1 Link Layer Discovery Protocol	312
4.12.2 LLDP Global Setting	312
4.12.3 LLDP Port Setting	315
4.12.4 LLDP Local Device	319
4.12.5 LLDP Remote Device	325
4.12.6 MED Network Policy	326
4.12.7 MED Port Setting	330
4.12.8 LLDP Overloading	334
4.12.9 LLDP Statistics	335
4.13 Diagnostics	338
4.13.1 Cable Diagnostics	338
4.13.2 System Status	340
4.13.3 Ping Test	341
4.13.4 IPv6 Ping Test	342
4.13.5 Trace Router	343
4.14 Power over Ethernet (GS-4210-24P2S only)	344
4.14.1 PoE Global Setting	344

4.14.2 PoE Port Setting	345
4.14.3 PoE Delay Setting	347
4.14.4 Power over Ethernet Powered Device	349
4.15 RMON.....	350
4.15.1 RMON Statistics	350
4.15.2 RMON Event	352
4.15.3 RMON Event Log	353
4.15.4 RMON Alarm	354
4.15.5 RMON History	357
4.15.6 RMON History Log	359
4.16 Maintenance.....	360
4.16.1 Factory Default	360
4.16.2 Reboot Switch	361
4.16.3 Backup Manager	362
4.16.4 Upgrade Manager.....	363
4.16.5 Configuration Manager	364
4.16.6 Enable Password.....	365
5. COMMAND LINE INTERFACE.....	366
5.1 Accessing the CLI	366
Logon to the Console	366
Configure IP address.....	367
5.2 Telnet Login	368
6. Command Line Mode	369
6.1 User Mode Commands	370
6.1.1 enable command	370
6.1.2 exit command	371
6.1.3 ping command	371
6.1.4 Show Command	372
6.1.5 traceroute command.....	374
6.2 Privileged Mode Commands	374
6.2.1 clear command	374
6.2.2 clock command.....	378
6.2.3 configure command	379
6.2.4 copy command	379
6.2.5 debug command.....	379

6.2.6 delete command	380
6.2.7 disable command	380
6.2.8 end command	380
6.2.9 exit command	381
6.2.10 no command	381
6.2.11 ping command	382
6.2.12 reboot command	382
6.2.13 renew command	382
6.2.14 restore-defaults command	383
6.2.15 save command	383
6.2.16 show command	383
6.2.17 ssl command	384
6.2.18 traceroute command	384
6.2.19 udld command	385
6.3 Global Config Mode Commands	386
6.3.1 aaa Command	386
6.3.2 boot Command	386
6.3.3 bridge Command	386
6.3.4 class-map Command	386
6.3.5 clock Command	387
6.3.6 dos Command	387
6.3.7 dot1x Command	388
6.3.8 do Command	388
6.3.9 enable Command	388
6.3.10 end Command	388
6.3.11 errdisable Command	388
6.3.12 exit Command	389
6.3.13 gvrp Command	389
6.3.14 hostname Command	389
6.3.15 interface Command	389
6.3.16 ip Command	390
6.3.17 ipv6 Command	390
6.3.18 jumbo-frame Command	391
6.3.19 l2 Command	391
6.3.20 lacp Command	391
6.3.21 lag Command	391
6.3.22 line Command	391
6.3.23 lldp Command	392
6.3.24 logging Command	392
6.3.25 mac Command	392

6.3.26 management-vlan Command	392
6.3.27 mirror Command.....	393
6.3.28 no Command	393
6.3.29 policy-map Command.....	393
6.3.30 port-security Command	393
6.3.31 qos Command	394
6.3.32 radius Command	394
6.3.33 rate-limit Command	394
6.3.34 rmon Command.....	394
6.3.35 Snmp Command.....	395
6.3.36 snmp Command	395
6.3.37 spanning-tree Command	395
6.3.38 storm-control Command	396
6.3.39 system Command.....	396
6.3.40 tacacs Command.....	396
6.3.41 udld Command	396
6.3.42 username Command	397
6.3.43 vlan Command	397
6.3.44 voice-vlan Command	397

7. SWITCH OPERATION 398

7.1 Address Table.....	398
------------------------	-----

7.2 Learning	398
--------------------	-----

7.3 Forwarding & Filtering	398
----------------------------------	-----

7.4 Store-and-Forward	398
-----------------------------	-----

7.5 Auto-Negotiation	400
----------------------------	-----

8. POWER OVER ETHERNET OVERVIEW 401

9. TROUBLESHOOTING 403

APPENDIX A 404

A.1 Switch's RJ45 Pin Assignments 1000Mbps, 1000BASE-T.....	404
---	-----

A.2 10/100Mbps, 10/100BASE-TX.....	404
------------------------------------	-----

1. INTRODUCTION

Thank you for purchasing PLANET 16/24-Port 10/100/1000T + 2-Port 100/1000X SFP Managed Switch, GS-4210-16T2S, GS-4210-24T2S and GS-4210-24P2S. The description of this model is shown below:

GS-4210-16T2S	16-Port 10/100/1000T + 2-Port 100/1000X SFP Managed Switch
GS-4210-24T2S	24-Port 10/100/1000T + 2-Port 100/1000X SFP Managed Switch
GS-4210-24P2S	24-Port 10/100/1000T 802.3at PoE + 2-Port 100/1000X SFP Managed Switch

“Managed Switch” mentioned in this Guide refers to the GS-4210-16T2S, GS-4210-24T2S and GS-4210-24P2S.

1.1 Package Contents

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**
- ◆ **Rubber Feet x 4**
- ◆ **Power Cord x 1**
- ◆ **RS-232 to RJ45 Console Cable x 1**
- ◆ **SFP Dust Cap x 2**
- ◆ **Rack-mount Accessory Kit x 1**

If any item is found missing or damaged, please contact your local reseller for replacement.

1.2 Product Description



Cost-Optimized Managed Switch for Small and Medium Businesses

PLANET Managed Switch is an ideal Gigabit Switch which provides cost-effective advantage to local area network and is widely accepted in the SMB office network. It offers **intelligent Layer 2 data packet switching and management functions, friendly web user interface** and **stable operation**. Besides the hot IPv6 / IPv4 management and abundant L2 / L4 switching functions, the GS-4210-16T2S / GS-4210-24T2S comes with fanless feature and green technology to provide a quiet, energy-saving, high-speed and reliable office network environment, the GS-4210-24P2S complies with **IEEE 802.3at Power over Ethernet Plus (PoE+)** at an affordable price, its **24** Gigabit Ethernet ports are integrated with 802.3at PoE+ injector function on all ports. The Managed Switch is equipped with **16/24 10/100/1000BASE-T** Gigabit Ethernet ports and **2** additional **100/1000BASE-X** SFP interfaces with inner power system. It offers a rack-mountable, affordable, safe and reliable Gigabit network switch solution for SMBs deploying networks, or requiring enhanced data security and network traffic management.

IEEE 802.3at/af Compliant Power Source Switch (GS-4210-24P2S)

The PoE in-line power following the **IEEE 802.3at/af standard** makes the GS-4210-24P2S able to deliver Gigabit speed data and up to **30 watts** of power per port to 24 PoE compliant powered devices (PDs) with a combined power output budget of up to 300 watts. The GS-4210-24P2S provides more flexibility in power requirement for all kinds of PDs with affordable installation costs.

High-performance Switch Architecture

The Managed Switch provides **16/24 10/100/1000Mbps** Gigabit Ethernet ports and **2 100/1000BASE-X SFP** slots. It boasts a high-performance switch architecture capable of providing the non-blocking switch fabric and wire-speed throughput as high as 36/52Gbps, which greatly simplifies the tasks of upgrading the LAN for catering to increasing bandwidth demands.

Robust Layer 2 Features

The Managed Switch can be programmed for advanced switch management functions such as dynamic port link aggregation, 802.1Q VLAN and Q-in-Q VLAN, Multiple Spanning Tree protocol (MSTP), Loop and BPDU Guard, IGMP Snooping, and MLD Snooping. Via the link aggregation, the Managed Switch allows the operation of a high-speed trunk to combine with multiple ports such as a 32Gbps fat pipe, and supports fail-over as well. Also, the Link Layer Discovery Protocol (LLDP) is the Layer 2 protocol included to help discover basic information about neighboring devices on the local broadcast domain.

Efficient Traffic Control

The Managed Switch is loaded with robust QoS features and powerful traffic management to enhance services to business-class data, voice, and video solutions. The functionality includes broadcast / multicast / unicast **storm control**, per port **bandwidth control**, 802.1p / CoS / IP DSCP QoS priority and remarking. It guarantees the best performance at VoIP and video stream transmission, and empowers the enterprises to take full advantage of the limited network resources.

Enhanced and Secure Management

For efficient management, the Managed Switch is equipped with console, Web, Telnet and SNMP management interfaces. With the built-in Web-based management interface, the Managed Switch offers an easy-to-use, platform-independent management and configuration facility. By supporting standard Simple Network Management Protocol (SNMP), the switch can be managed via any standard management software. For text-based management, the switch can be accessed via Telnet and the console port. Moreover, the Managed Switch offers secure remote management by supporting HTTPS and SNMPv3 connections which encrypt the packet content at each session.

Powerful Security

PLANET Managed Switch offer comprehensive **IPv4 / IPv6** 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** authentication, which can be deployed with RADIUS to ensure the port level security and block illegal users. With the **protected port** function, communication between edge ports can be prevented to guarantee user privacy. Furthermore, **port security** function allows limiting the number of network devices on a given port.

Advanced Network Security

The Managed Switch also provides **DHCP snooping**, **IP source guard** and **dynamic ARP inspection** functions to prevent IP snooping from attack and discard ARP packets with invalid MAC address. The network administrators can now construct highly-secured corporate networks with considerably less time and effort than before.

Flexible Extension Solution

The two mini-GBIC slots built in the Managed Switch are compatible with the **100BASE-FX / 1000BASE-SX/LX** SFP (Small Form-factor Pluggable) fiber transceiver to uplink to backbone switch and monitor center in long distance. The distance can be extended from 550 meters to 2km (multi-mode fiber) up to above 10/20/30/40/50/60/70/120 kilometers (single-mode fiber or WDM fiber). They are well suited for applications within the enterprise data centers and distributions.

Fanless Design (GS-4210-16T2S / GS-4210-24T2S)

Adopting the latest chip process and green technology, the GS-4210-16T2S / GS-4210-24T2S successfully reduces substantial power consumption with the fanless and noiseless design collocating with the effective cooler. Therefore, the GS-4210-16T2S / GS-4210-24T2S are able to operate stably and quietly in any environment without affecting its performance.

1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2, INSTALLATION

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

Section 3, SWITCH MANAGEMENT

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

Section 4, WEB CONFIGURATION

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

Section 5, COMMAND LINE INTERFACE

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

Section 6, CLI CONFIGURATION

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

Section 7 SWITCH OPERATION

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

Section 8 POWER OVER ETHERNET OVERVIEW

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

Section 9 TROUBLESHOOTING

The chapter explains how to troubleshoot the Managed Switch.

Appendix A

The section contains cable information of the Managed Switch.

1.4 Product Features

Physical Port

- 16/24-port 10/100/1000BASE-T Gigabit RJ45 copper
- 2 100/1000BASE-X mini-GBIC/SFP slots
- RJ45 console interface for switch basic management and setup
- Reset button for system factory default and reboot

Switching

- Hardware based 10/100Mbps, half / full duplex and 1000Mbps full duplex mode, flow control and auto-negotiation and auto MDI/MDI-X
- Features Store-and-Forward mode with wire-speed filtering and forwarding rates
- IEEE 802.3x flow control for full duplex operation and back pressure for half duplex operation
- 9K Jumbo frame
- Automatic address learning and address aging
- Supports CSMA/CD protocol

Power over Ethernet (GS-4210-24P2S)

- Complies with IEEE 802.3at High Power over Ethernet
- Complies with IEEE 802.3af Power over Ethernet
- Up to 24 ports of IEEE 802.3af / 802.3at devices powered
- Supports PoE Power up to 30.8 watts for each PoE port
- 300-watt PoE budget
- Auto detects powered device (PD)
- Circuit protection prevents power interference between ports
- Remote power feeding up to 100m
- PoE Management
 - Total PoE power budget control
 - Per port PoE function enable/disable
 - PoE Port Power feeding priority
 - Per PoE port power limitation
 - PoE delay
 - PD classification detection

Layer 2 Features

- Supports VLAN
 - IEEE 802.1Q tagged VLAN
 - Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
 - Protocol VLAN
 - Voice VLAN
 - Private VLAN (Protected port)

- Management VLAN
- GVRP
- Supports **Spanning Tree Protocol**
 - STP (Spanning Tree Protocol)
 - RSTP (Rapid Spanning Tree Protocol)
 - MSTP (Multiple Spanning Tree Protocol)
 - STP BPDU Guard, BPDU Filtering and BPDU Forwarding
- Supports **Link Aggregation**
 - IEEE 802.3ad Link Aggregation Control Protocol (LACP)
 - Cisco ether-channel (Static Trunk)
 - Maximum 8 trunk groups, up to 8 ports per trunk group
- Provides port mirror (many-to-1)
- Loop protection to avoid broadcast loops

Quality of Service

- Ingress / Egress Rate Limit per port bandwidth control
- Traffic classification
- IEEE 802.1p CoS
- DSCP / IP Precedence of IPv4 / IPv6 packets
- Strict priority and Weighted Round Robin (WRR) CoS policies

Multicast

- Supports IPv4 IGMP snooping v2 and v3
- Supports IPv6 MLD snooping v1, v2
- IGMP querier mode support
- IGMP snooping port filtering
- MLD snooping port filtering

Security

- Storm Control support
 - Broadcast / Unknown-Unicast / Unknown-Multicast
- Authentication
 - IEEE 802.1X port-based network access authentication
 - Built-in RADIUS client to co-operate with the RADIUS servers
 - DHCP Option 82
 - RADIUS / TACACS+ authentication
- Access Control List
 - IPv4 / IPv6 IP-based ACL
 - IPv4 / IPv6 IP-based ACE
 - MAC-based ACL
 - MAC-based ACE
- MAC Security

- Static MAC
- MAC Filtering
- Port security for source MAC address entries filtering
- 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
- DoS attack prevention

Management

- IPv4 and IPv6 dual stack management
- Switch Management Interface
 - Local Command Line Interface
 - IPv4 / IPv6 Web switch management
 - Telnet Command Line Interface
 - SNMP v1, v2c and v3
 - HTTPs secure access
- Built-in Trivial File Transfer Protocol (TFTP) client
- Static and DHCP for IP address assignment
- System Maintenance
 - Firmware upload / download via HTTP / TFTP
 - Configuration upload / download through HTTP / TFTP
 - Hardware reset button for system reset to factory default
- SNTP Network Time Protocol
- Cable diagnostics
- Link Layer Discovery Protocol (LLDP) Protocol and LLDP-MED
- SNMP trap for interface Link Up and Link Down notification
- Event message logging to remote Syslog server
- Four RMON groups (history, statistics, alarms and events)
- PLANET Smart Discovery Utility

1.5 Product Specifications

Product	GS-4210-16T2S	GS-4210-24T2S
Hardware Specifications		
10/100/1000T Copper Ports	16 x RJ45 auto-MDI/MDI-X ports	24 x RJ45 auto-MDI/MDI-X ports
SFP/mini-GBIC Slots	2 100/1000BASE-X SFP interfaces, supporting 100/1000Mbps dual mode	
Console	1 x RS-232-to-RJ45 serial port (115200, 8, N, 1)	
Reset Button	System factory default	
Switch Architecture	Store-and-Forward	
Switch Fabric	36Gbps / non-blocking	52Gbps / non-blocking
Switch Throughput@64 bytes	26.7Mpps @64 bytes	38.6Mpps @64 bytes
MAC Address Table	8K entries	
Shared Data Buffer	4.1 megabits	
Flow Control	IEEE 802.3x pause frame for full-duplex Back pressure for half-duplex	
Jumbo Frame	9216 bytes	
Reset Button	> 5 sec: Factory default	
LED	System: Power (Green) 10/100/1000T RJ45 Interfaces (Port 1 to Port 16): 1000 LNK / ACT (Green), 10/100 LNK/ACT (Orange) 100/1000Mbps SFP Interfaces (Port 17 to Port 18): 1000 LNK / ACT (Green), 100 LNK/ACT (Orange)	System: Power (Green) 10/100/1000T RJ45 Interfaces (Port 1 to Port 24): 1000 LNK / ACT (Green), 10/100 LNK/ACT (Orange) 100/1000Mbps SFP Interfaces (Port 25 to Port 26): 1000 LNK / ACT (Green), 100 LNK/ACT (Orange)
Power Requirements	100~240V AC, 50/60Hz, 0.8A (max.)	
Power Consumption / Dissipation	Max. 10.4 watts / 35 BTU	Max. 14 watts / 47 BTU
Dimensions (W x D x H)	445 x 207 x 45 mm (1U height)	
Weight	2kg	2.1kg
ESD Protection	Yes	
Enclosure	Metal	
Layer 2 Functions		
Port Mirroring	TX / RX / Both Many-to-1 monitor	
VLAN	802.1Q tagged-based VLAN Up to 256 VLAN groups, out of 4094 VLAN IDs 802.1ad Q-in-Q tunneling (VLAN stacking) Voice VLAN	

	<p>Protocol VLAN</p> <p>Private VLAN (Protected port)</p> <p>GVRP</p> <p>Management VLAN</p>
Link Aggregation	<p>IEEE 802.3ad LACP and static trunk</p> <p>Supports 8 groups of 8-port trunk</p>
Spanning Tree Protocol	<p>STP, IEEE 802.1D Spanning Tree Protocol</p> <p>RSTP, IEEE 802.1w Rapid Spanning Tree Protocol</p> <p>MSTP, IEEE 802.1s Multiple Spanning Tree Protocol</p> <p>STP BPDU Guard, BPDU Filtering and BPDU Forwarding</p>
IGMP Snooping	<p>IPv4 IGMP (v2/v3) Snooping</p> <p>IGMP Querier</p> <p>Up to 256 multicast groups</p>
MLD Snooping	<p>IPv6 MLD (v1/v2) snooping, up to 256 multicast groups</p>
Access Control List	<p>IPv4/IPv6 IP-based ACL / MAC-based ACL</p> <p>IPv4/IPv6 IP-based ACE / MAC-based ACE</p>
QoS	<p>8 mapping ID to 8 level priority queues</p> <ul style="list-style-type: none"> - Port Number - 802.1p priority - DSCP / IP Precedence of IPv4 / IPv6 packets <p>Traffic classification based, strict priority and WRR</p> <p>Ingress / Egress Rate Limit per port bandwidth control</p>
Security	<p>IEEE 802.1X port-based authentication</p> <p>Built-in RADIUS client to co-operate with RADIUS server</p> <p>RADIUS / TACACS+ authentication</p> <p>IP-MAC port binding</p> <p>MAC filtering</p> <p>Static MAC address</p> <p>DHCP snooping and DHCP Option82</p> <p>STP BPDU guard, BPDU filtering and BPDU forwarding</p> <p>DoS attack prevention</p> <p>ARP inspection</p> <p>IP source guard</p> <p>Storm control support</p> <ul style="list-style-type: none"> - Broadcast / Unknown-Unicast / Unknown-Multicast
Management Functions	
Basic Management Interfaces	<p>RJ45 Console / Web browser / Telnet / SNMP v1, v2c, v3</p> <p>Firmware upgrade by HTTP / TFTP protocol through Ethernet network</p> <p>Configuration upload / download through HTTP / TFTP</p> <p>Remote / Local Syslog</p> <p>System log</p> <p>LLDP protocol</p> <p>SNTP</p>

	PLANET Smart Discovery Utility
Secure Management Interfaces	HTTPs, SNMP v3
SNMP MIBs	RFC 3635 Ethernet-like MIB RFC 2863 Interface Group MIB RFC 2819 RMON (1, 2, 3, 9) RFC 1493 Bridge MIB
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX / 100BASE-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000BASE-T IEEE 802.3x Flow Control and Back pressure IEEE 802.3ad Port Trunk with LACP IEEE 802.1D Spanning Tree protocol IEEE 802.1w Rapid Spanning Tree protocol IEEE 802.1s Multiple Spanning Tree protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control IEEE 802.1ab LLDP RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2 RFC 3376 IGMP version 3 RFC 2710 MLD version 1 RFC 3810 MLD version 2
Environment	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
Storage	Temperature: -10 ~ 70 degrees C Relative Humidity: 5 ~ 95% (non-condensing)

Product	GS-4210-24P2S
Hardware Specifications	
10/100/1000T Copper Ports	24 x RJ45 auto-MDI/MDI-X ports
PoE Injector Port	24 802.3af / 802.3at PoE Injector Ports
SFP/mini-GBIC Slots	2 100/1000BASE-X SFP interfaces, supporting 100/1000Mbps dual mode
Console	1 x RS-232-to-RJ45 serial port (115200, 8, N, 1)
Reset Button	System factory default
Switch Architecture	Store-and-Forward
Switch Fabric	52Gbps / non-blocking
Switch Throughput@64 bytes	38.6Mpps @64 bytes
MAC Address Table	8K entries
Shared Data Buffer	4.1 megabits
Flow Control	IEEE 802.3x pause frame for full-duplex Back pressure for half-duplex
Jumbo Frame	9216 bytes
Reset Button	> 5 sec: Factory default
LED	<p>System: Power (Green)</p> <p>10/100/1000T RJ45 Interfaces (Port 1 to Port 24): 1000 LNK / ACT (Green), 10/100 LNK/ACT (Orange), PoE (Orange)</p> <p>100/1000Mbps SFP Interfaces (Port 25 to Port 26): 1000 LNK / ACT (Green), 100 LNK/ACT (Orange)</p>
Thermal Fan	2
Power Requirements	100~240V AC, 50/60Hz, 4A (max.)
Power Consumption / Dissipation	Max. 330 watts / 1122 BTU
Dimensions (W x D x H)	445 x 207 x 45 mm (1U height)
Weight	2.8kg
ESD Protection	Yes
Enclosure	Metal
Layer 2 Functions	
PoE Standard	IEEE 802.3af Power over Ethernet / PSE IEEE 802.3at Power over Ethernet Plus / PSE
PoE Power Output	Per Port 52V DC, 300mA. Max. 15.4 watts (IEEE 802.3af) Per Port 52V DC, 600mA. Max. 30 watts (IEEE 802.3at)
PoE Power Budget	300 watts
Number of PDs, 7 watts	24
Number of PDs, 15.4 watts	19
Number of PDs, 30 watts	9
Layer 2 Functions	
Port Mirroring	TX / RX / Both Many-to-1 monitor

<p>VLAN</p>	<p>802.1Q tagged-based VLAN Up to 256 VLAN groups, out of 4094 VLAN IDs 802.1ad Q-in-Q tunneling (VLAN stacking) Voice VLAN Protocol VLAN Private VLAN (Protected port) GVRP Management VLAN</p>
<p>Link Aggregation</p>	<p>IEEE 802.3ad LACP and static trunk Supports 8 groups of 8-port trunk</p>
<p>Spanning Tree Protocol</p>	<p>STP, IEEE 802.1D Spanning Tree Protocol RSTP, IEEE 802.1w Rapid Spanning Tree Protocol MSTP, IEEE 802.1s Multiple Spanning Tree Protocol STP BPDU Guard, BPDU Filtering and BPDU Forwarding</p>
<p>IGMP Snooping</p>	<p>IPv4 IGMP (v2/v3) Snooping IGMP Querier Up to 256 multicast groups</p>
<p>MLD Snooping</p>	<p>IPv6 MLD (v1/v2) snooping, up to 256 multicast groups</p>
<p>Access Control List</p>	<p>IPv4/IPv6 IP-based ACL / MAC-based ACL IPv4/IPv6 IP-based ACE / MAC-based ACE</p>
<p>QoS</p>	<p>8 mapping ID to 8 level priority queues - Port Number - 802.1p priority - DSCP / IP Precedence of IPv4 / IPv6 packets Traffic classification based, strict priority and WRR Ingress / Egress Rate Limit per port bandwidth control</p>
<p>Security</p>	<p>IEEE 802.1X port-based authentication Built-in RADIUS client to co-operate with RADIUS server RADIUS / TACACS+ authentication IP-MAC port binding MAC filtering Static MAC address DHCP snooping and DHCP Option82 STP BPDU guard, BPDU filtering and BPDU forwarding DoS attack prevention ARP inspection IP source guard Storm control support - Broadcast / Unknown-Unicast / Unknown-Multicast</p>
<p>Management Functions</p>	
<p>Basic Management Interfaces</p>	<p>RJ45 Console / Web browser / Telnet / SNMP v1, v2c, v3 Firmware upgrade by HTTP / TFTP protocol through Ethernet network Configuration upload / download through HTTP / TFTP</p>

	<p>Remote / Local Syslog</p> <p>System log</p> <p>LLDP protocol</p> <p>SNTP</p> <p>PLANET Smart Discovery Utility</p>
Secure Management Interfaces	<p>HTTPs, SNMP v3</p>
SNMP MIBs	<p>RFC 3635 Ethernet-like MIB</p> <p>RFC 2863 Interface Group MIB</p> <p>RFC 2819 RMON (1, 2, 3, 9)</p> <p>RFC 1493 Bridge MIB</p>
Standards Conformance	
Regulation Compliance	<p>FCC Part 15 Class A, CE</p>
Standards Compliance	<p>IEEE 802.3 10BASE-T</p> <p>IEEE 802.3u 100BASE-TX / 100BASE-FX</p> <p>IEEE 802.3z Gigabit SX/LX</p> <p>IEEE 802.3ab Gigabit 1000BASE-T</p> <p>IEEE 802.3x Flow Control and Back pressure</p> <p>IEEE 802.3ad Port Trunk with LACP</p> <p>IEEE 802.1D Spanning Tree protocol</p> <p>IEEE 802.1w Rapid Spanning Tree protocol</p> <p>IEEE 802.1s Multiple Spanning Tree protocol</p> <p>IEEE 802.1p Class of Service</p> <p>IEEE 802.1Q VLAN Tagging</p> <p>IEEE 802.1x Port Authentication Network Control</p> <p>IEEE 802.1ab LLDP</p> <p>IEEE 802.3af Power over Ethernet</p> <p>IEEE 802.3at High Power over Ethernet</p> <p>RFC 768 UDP</p> <p>RFC 793 TFTP</p> <p>RFC 791 IP</p> <p>RFC 792 ICMP</p> <p>RFC 2068 HTTP</p> <p>RFC 1112 IGMP version 1</p> <p>RFC 2236 IGMP version 2</p> <p>RFC 3376 IGMP version 3</p> <p>RFC 2710 MLD version 1</p> <p>RFC 3810 MLD version 2</p>
Environment	
Operating	<p>Temperature: 0 ~ 50 degrees C</p> <p>Relative Humidity: 5 ~ 95% (non-condensing)</p>
Storage	<p>Temperature: -10 ~ 70 degrees C</p> <p>Relative Humidity: 5 ~ 95% (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. [Figure 2-1-1](#), [Figure 2-1-2](#) and [Figure 2-1-3](#) show their front panels.

Front Panel

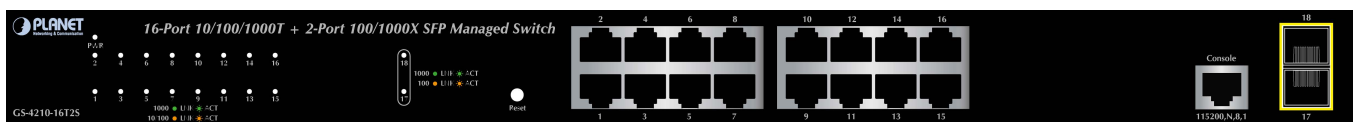


Figure 2-1-1: GS-4210-16T2S Front Panel

Front Panel

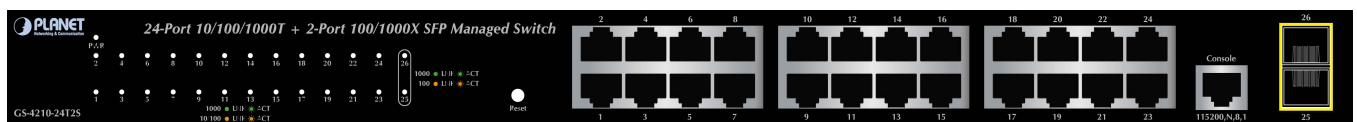


Figure 2-1-2: GS-4210-24T2S Front Panel

Front Panel

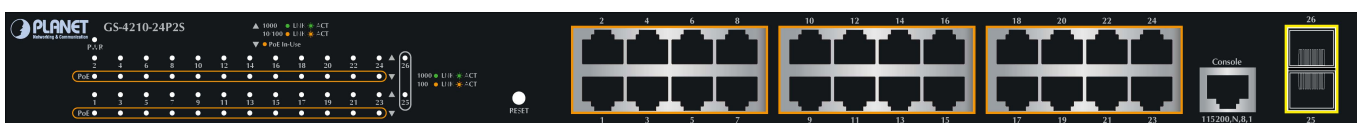


Figure 2-1-3: GS-4210-24P2S Front Panel

■ Gigabit TP Interface

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

802.3af / 802.3at PoE Injector (**GS-4210-24P2S**)

■ 100/1000BASE-X SFP Slots

Each of the SFP (Small Form-factor Pluggable) slot supports dual-speed, 1000BASE-SX / LX or 100BASE-FX

- For 1000BASE-SX/LX SFP transceiver module: From 550 meters (multi-mode fiber) to 10/20/30/40/50/60/70/120 kilometers (Single-mode fiber).
- For 100BASE-FX SFP transceiver module: From 2 kilometers (multi-mode fiber) to 20/40/60 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**

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

Reset Button Pressed and Released	Function
> 5 seconds: 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

2.1.2 LED Indications

The front panel LEDs indicate instant status of port links, data activity, PoE status and system power; helps monitor and troubleshoot when needed. [Figure 2-1-4](#), [Figure 2-1-5](#) and [Figure 2-1-6](#) show their LED indications.

LED Indication

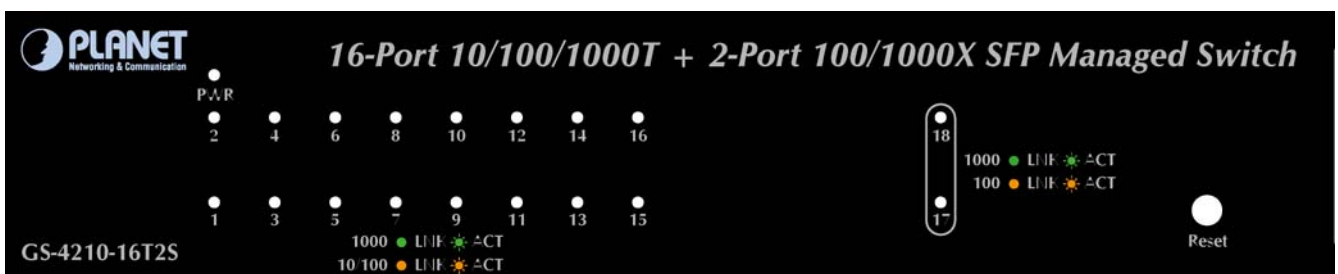


Figure 2-1-4: GS-4210-16T2S LED Panel

■ **System**

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.

■ 10/100/1000BASE-T Interfaces

LED	Color	Function
1000 LNK/ACT	Green	Lights: To indicate the link through that port is successfully established at 1000Mbps. Blinks: To indicate that the switch is actively sending or receiving data over that port.
10/ 100 LNK/ACT	Orange	Lights: To indicate the link through that port is successfully established at 10Mbps or 100Mbps. Blinks: To indicate that the switch is actively sending or receiving data over that port.

■ 100 / 1000BASE-X SFP Interfaces

LED	Color	Function
1000 LNK/ACT	Green	Lights: To indicate the link through that port is successfully established at 1000Mbps. Blinks: To indicate that the switch is actively sending or receiving data over that port.
100 LNK/ACT	Orange	Lights: To indicate the link through that port is successfully established at 100Mbps. Blinks: To indicate that the switch is actively sending or receiving data over that port.

LED Indication

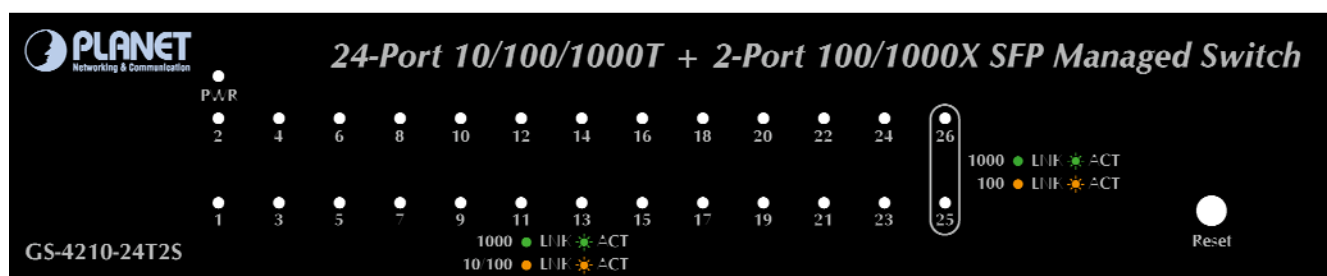


Figure 2-1-5: GS-4210-24T2S LED Panel

■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.

■ 10/100/1000BASE-T Interfaces

LED	Color	Function
1000 LNK/ACT	Green	Lights: To indicate the link through that port is successfully established at 1000Mbps. Blinks: To indicate that the switch is actively sending or receiving data over that port.
10/ 100 LNK/ACT	Orange	Lights: To indicate the link through that port is successfully established at 10Mbps or 100Mbps. Blinks: To indicate that the switch is actively sending or receiving data over that port.

■ 100 / 1000BASE-X SFP Interfaces

LED	Color	Function
1000 LNK/ACT	Green	Lights: To indicate the link through that port is successfully established at 1000Mbps. Blinks: To indicate that the switch is actively sending or receiving data over that port.
100 LNK/ACT	Orange	Lights: To indicate the link through that port is successfully established at 100Mbps. Blinks: To indicate that the switch is actively sending or receiving data over that port.

LED Indication

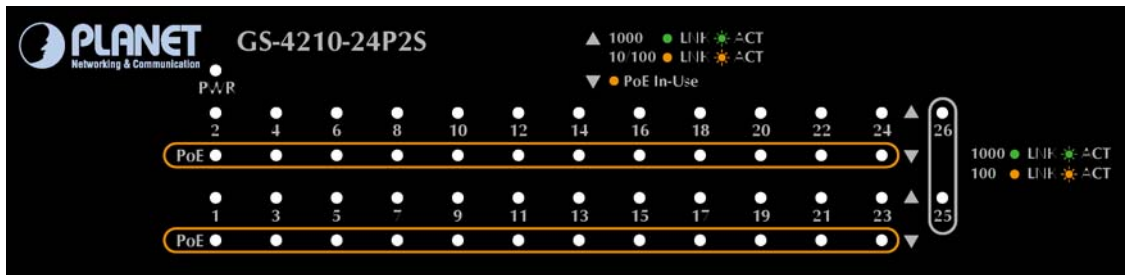


Figure 2-1-6: GS-4210-24P2S LED Panel

■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.

■ 10/100/1000BASE-T Interfaces

LED	Color	Function
1000 LNK/ACT	Green	Lights: To indicate the link through that port is successfully established at 1000Mbps. Blinks: To indicate that the switch is actively sending or receiving data over that port.
10/ 100 LNK/ACT	Orange	Lights: To indicate the link through that port is successfully established at 10Mbps or 100Mbps. Blinks: To indicate that the switch is actively sending or receiving data over that port.
PoE-in-Use	Orange	Lights: To indicate the port is providing 52V DC in-line power. Off: To indicate the connected device is not a PoE Powered Device (PD)

■ 100 / 1000BASE-X SFP Interfaces

LED	Color	Function
1000 LNK/ACT	Green	Lights: To indicate the link through that port is successfully established at 1000Mbps. Blinks: To indicate that the switch is actively sending or receiving data over that port.
100 LNK/ACT	Orange	Lights: To indicate the link through that port is successfully established at 100Mbps. 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 indicates an AC inlet power socket, which accepts input power from 100 to 240V AC, 50-60Hz, 0.8A / 4A. [Figure 2-1-7](#) and [Figure 2-1-8](#) show their rear panels.

Rear Panel



Figure 2-1-7: Rear Panel of GS-4210-16T2S / GS-4210-24T2S

Rear Panel

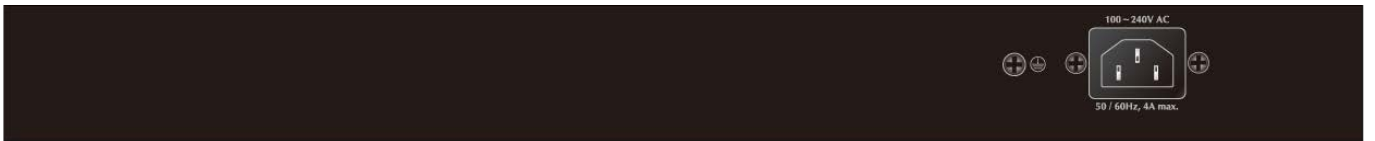


Figure 2-1-8: Rear Panel of GS-4210-24P2S

■ AC Power Receptacle

For compatibility with electrical outlet in most areas of the world, the Managed Switch's power supply automatically adjusts to line power in the range of 100-240V AC and 50/60Hz, 0.8A / 4A.

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

Power Notice: The device is a power-required device, which means it will not work till it is powered. If your networks should be active all the time, please consider using UPS (Uninterrupted Power Supply) for your device. It will prevent you from network data loss or network downtime.

Power Notice: 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 Managed Switch or the power adapter.

2.2 Installing the Switch

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

2.2.1 Desktop Installation

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

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

Step2: Place the Managed Switch on the desktop or the shelf near an AC power source, as shown in Figure 2-1-9.

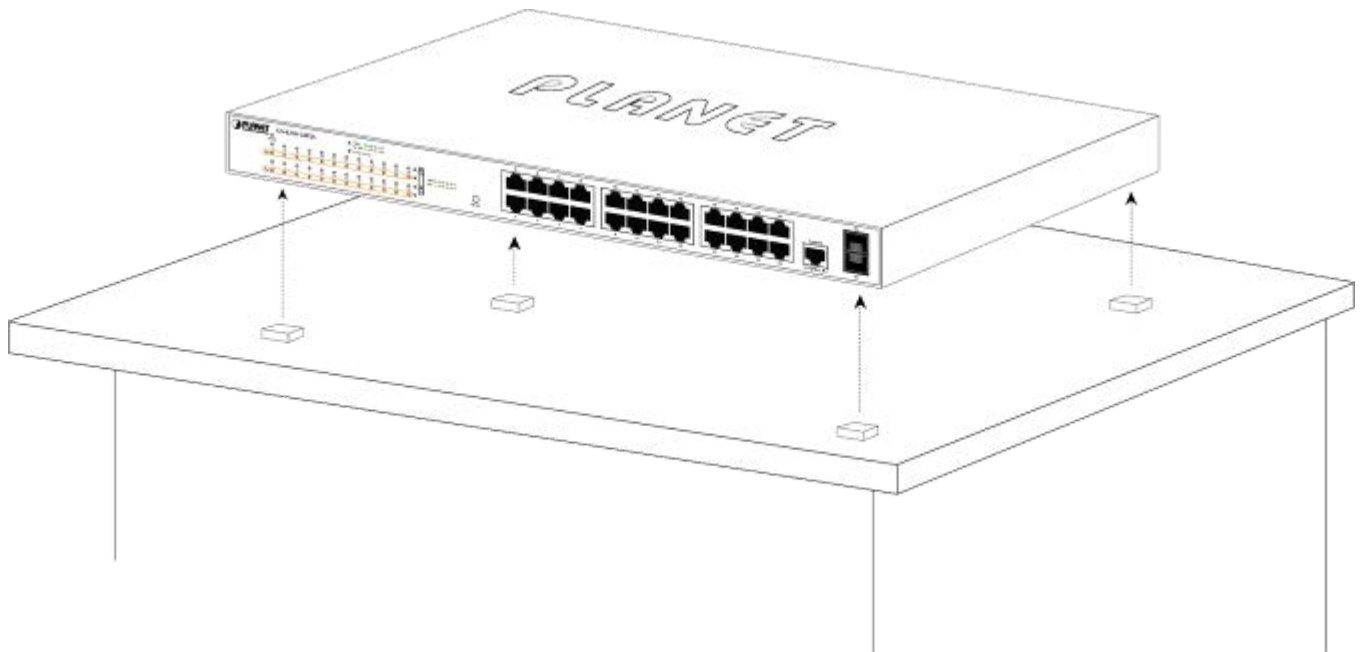


Figure 2-1-9: Place the Managed Switch on the desktop

Step3: 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: Connecting 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 and 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 5 network cabling with RJ45 tips. For more information, please see the Cabling Specification in Appendix A.

Step 5: Supplying power to the Managed Switch.

Connect one end of the power cable to the Managed Switch and the power plug of the power cable to a standard wall outlet. When the Managed Switch receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting

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

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

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

Figure 2-1-10 shows how to attach brackets to one side of the Managed Switch.

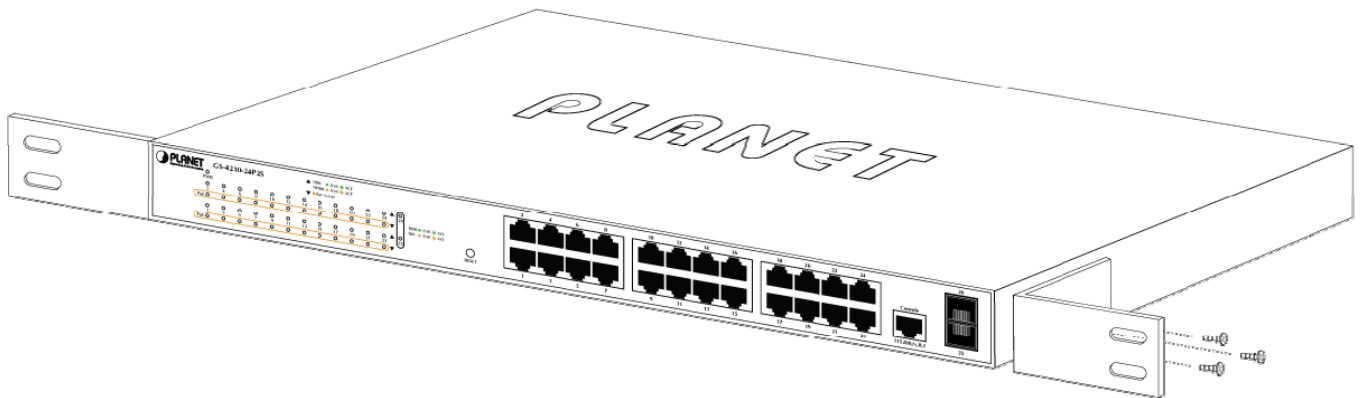


Figure 2-1-10: Attach Brackets to the Managed Switch



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 2-1-11.

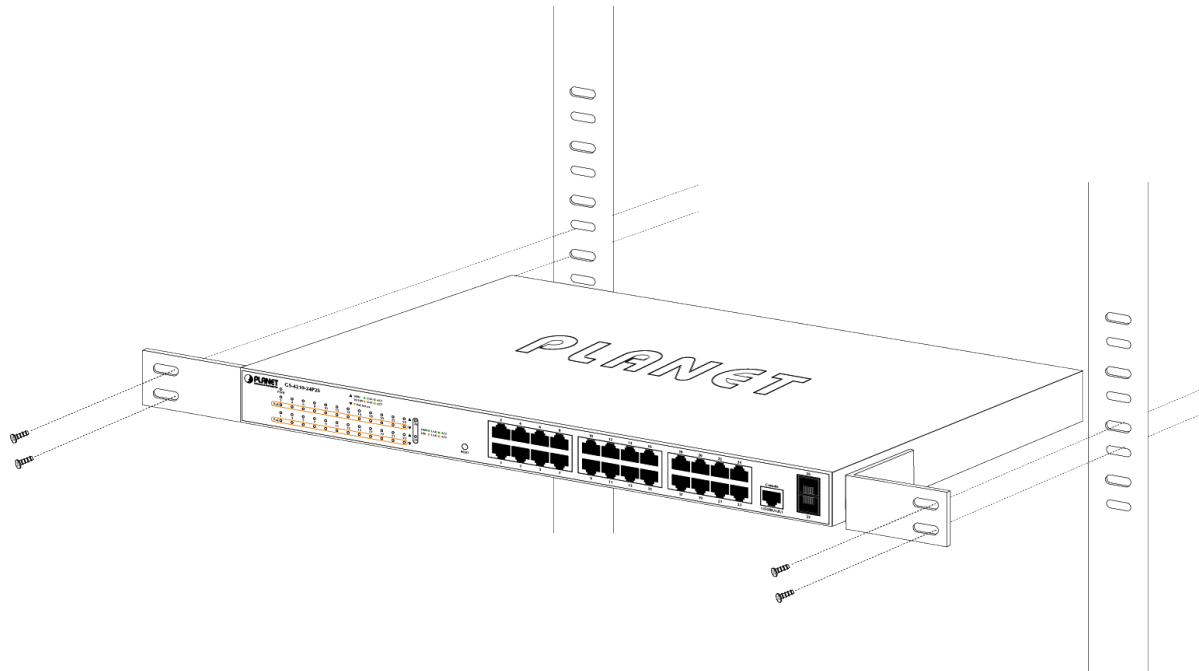


Figure 2-1-11: Mounting Managed Switch in a Rack

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 transceiver

The sections describe how to insert an SFP transceiver into an SFP slot. The SFP transceivers are hot-pluggable and hot-swappable. You can plug in and out the transceiver to/from any SFP port without having to power down the Managed Switch, as the Figure 2-1-12 shows.

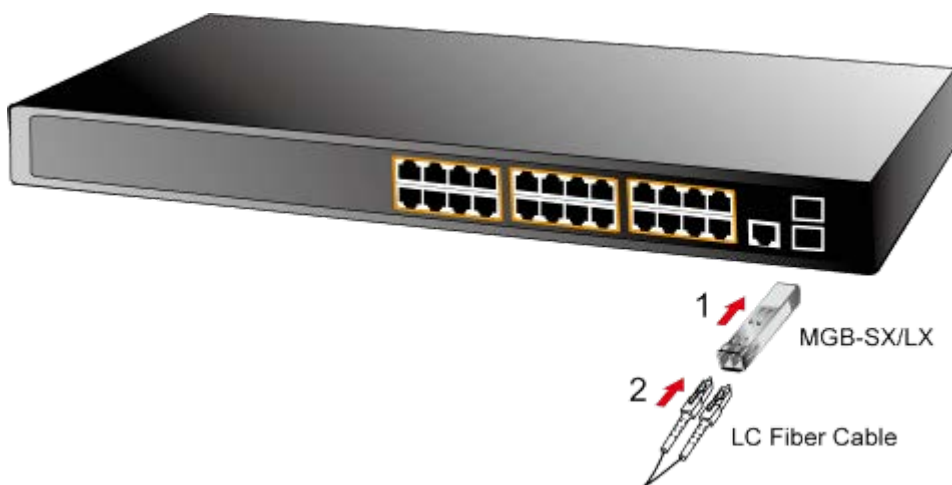


Figure 2-1-12: Plug In the SFP Transceiver

■ Approved PLANET SFP Transceivers

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

Gigabit SFP Transceiver Modules

- **MGB-GT** SFP-Port 1000BASE-T Module
- **MGB-SX** SFP-Port 1000BASE-SX mini-GBIC module
- **MGB-LX** SFP-Port 1000BASE-LX mini-GBIC module -10KM
- **MGB-L30** SFP-Port 1000BASE-LX mini-GBIC module -30KM
- **MGB-L50** SFP-Port 1000BASE-LX mini-GBIC module -50KM
- **MGB-L70** SFP-Port 1000BASE-LX mini-GBIC module -70KM
- **MGB-L120** SFP-Port 1000BASE-LX mini-GBIC module -120KM
- **MGB-LA10** SFP-Port 1000BASE-LX (WDM,TX:1310nm) -10KM
- **MGB-LB10** SFP-Port 1000BASE-LX (WDM,TX:1550nm) -10KM
- **MGB-LA20** SFP-Port 1000BASE-LX (WDM,TX:1310nm) -20KM
- **MGB-LB20** SFP-Port 1000BASE-LX (WDM,TX:1550nm) -20KM
- **MGB-LA40** SFP-Port 1000BASE-LX (WDM,TX:1310nm) -40KM
- **MGB-LB40** SFP-Port 1000BASE-LX (WDM,TX:1550nm) -40KM

Fast Ethernet SFP Transceiver Modules

- **MFB-FX** SFP-Port 100BASE-FX Transceiver -2KM
- **MFB-F20** SFP-Port 100BASE-FX Transceiver -20KM
- **MFB-F40** SFP-Port 100BASE-FX Transceiver -40KM
- **MFB-F60** SFP-Port 100BASE-FX Transceiver -60KM
- **MFB-FA20** SFP-Port 100BASE-BX Transceiver (WDM,TX:1310nm) -20KM
- **MFB-FB20** SFP-Port 100BASE-BX Transceiver (WDM,TX:1550nm) -20KM



Note

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



Note

In the installation steps below, this Manual uses Gigabit SFP transceiver as an example. However, the steps for Fast Ethernet SFP transceiver are similar.

1. Before we connect Managed Switch 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, 1000Bas-LX to 1000BASE-LX.
2. Check whether the fiber-optic cable type matches with the SFP transceiver requirement.
 - To connect to 1000BASE-SX SFP transceiver, please use the multi-mode fiber cable with one side being the male duplex LC connector type.
 - To connect to 1000BASE-LX SFP transceiver, please use the single-mode fiber cable with one side being the male duplex LC connector type.

■ **Connecting the Fiber Cable**

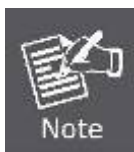
1. Insert the duplex LC connector into the SFP transceiver.
2. Connect the other end of the cable to a device with SFP transceiver installed.
3. Check the LNK/ACT LED of the SFP slot on the front of the Managed Switch. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link fails. To function with some fiber-NICs or Media Converters, user has to set the port Link mode to “**1000 Force**” or “**100 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 2-1-13: How to Pull Out the 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 module slot of the Managed Switch.

3. SWITCH MANAGEMENT

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

This chapter covers the following topics:

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

3.1 Requirements

- **Workstations** running Windows 2000/XP, 2003, Vista/7/8, 2008, MAC OS9 or later, Linux, UNIX or other platforms are compatible with **TCP/IP** protocols.
- **Workstation** is installed with **Ethernet NIC** (Network Interface Card)
- **Serial Port** connect (Terminal)
 - The above PC with COM Port (DB9 / RS-232) or USB-to-RS-232 converter
- Ethernet Port connection
 - Network cables -- Use standard network (UTP) cables with RJ45 connectors.
- The above Workstation is installed with **WEB browser** and **JAVA runtime environment** Plug-in



It is recommended to use Internet Explore 8.0 or above to access Managed Switch.

3.2 Management Access Overview

The Managed Switch gives you the flexibility to access and manage it using any or all of the following methods:

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

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

Method	Advantages	Disadvantages
Console	<ul style="list-style-type: none"> • No IP address or subnet needed • Text-based • Telnet functionality and HyperTerminal built into Windows 2000/XP, 2003, Vista/7/8, 2008 operating systems • Secure 	<ul style="list-style-type: none"> • Must be near the switch or use dial-up connection • Not convenient for remote users • Modem connection may prove to be unreliable or slow
Web Browser	<ul style="list-style-type: none"> • Ideal for configuring the switch remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing 	<ul style="list-style-type: none"> • Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	<ul style="list-style-type: none"> • Communicates with switch functions at the MIB level • Based on open standards 	<ul style="list-style-type: none"> • Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)

Table 3-1: Comparison of Management Methods

3.3 Administration Console

The administration console is an internal, character-oriented, and command line user interface for performing system administration such as displaying statistics or changing option settings. Using this method, you can view the administration console from a terminal, personal computer, Apple Macintosh, or workstation connected to the Managed Switch's console port. There are two ways to use this management method: via direct access or modem port access. The following sections describe these methods. For more information about using the console, refer to **Chapter 5 Command Line Interface Console Management**.

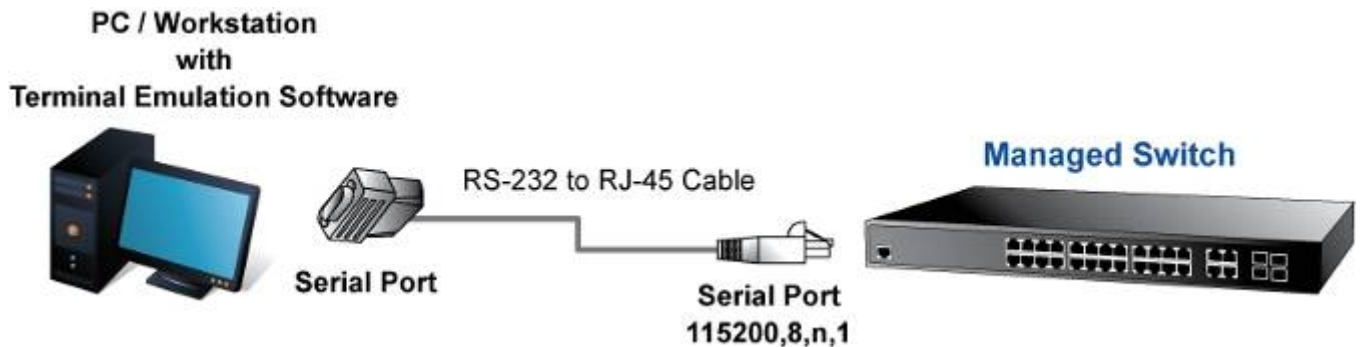


Figure 3-1: Console Management

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 **HyperTerminal**) to the Managed Switch console (serial) port. When using this management method, a **straight RS-232 to RJ45 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

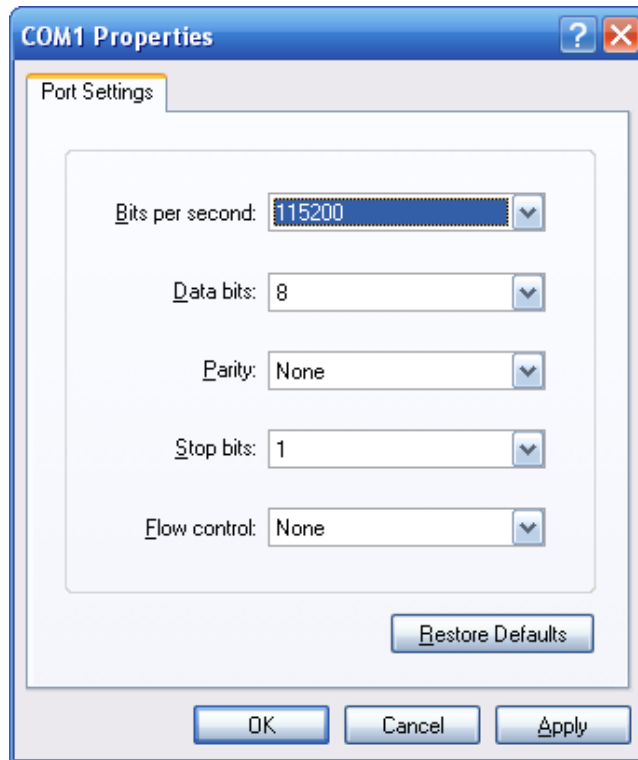


Figure 3-2: Terminal Parameter Settings

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 Managed Switch, you can access the Managed Switch's Web interface applications directly in your Web browser by entering the IP address of the Managed Switch.

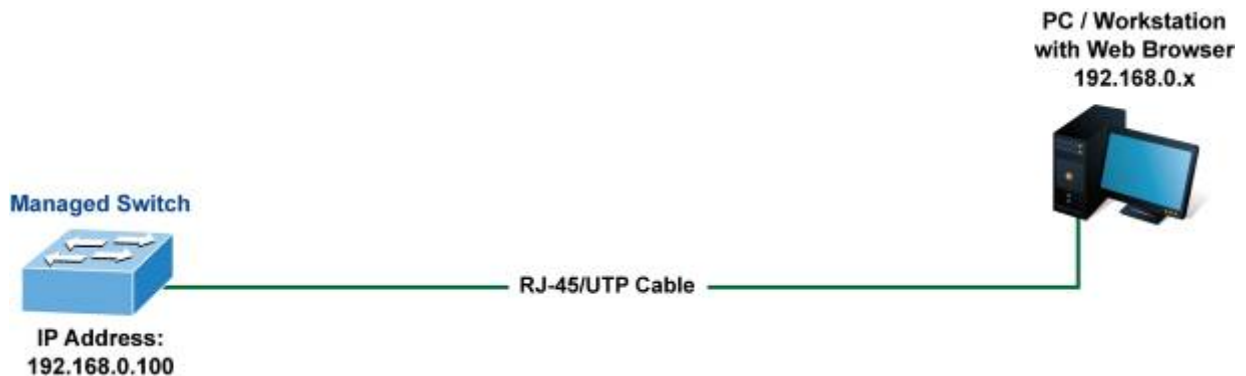


Figure 3-3: Web Management

You can then use your Web browser to list and manage the Managed Switch configuration parameters from one central location, 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 1.5** or later.



The following web screen based on GS-4210-24T2S will be the same as that of GS-4210-16T2S and GS-4210-24P2S.

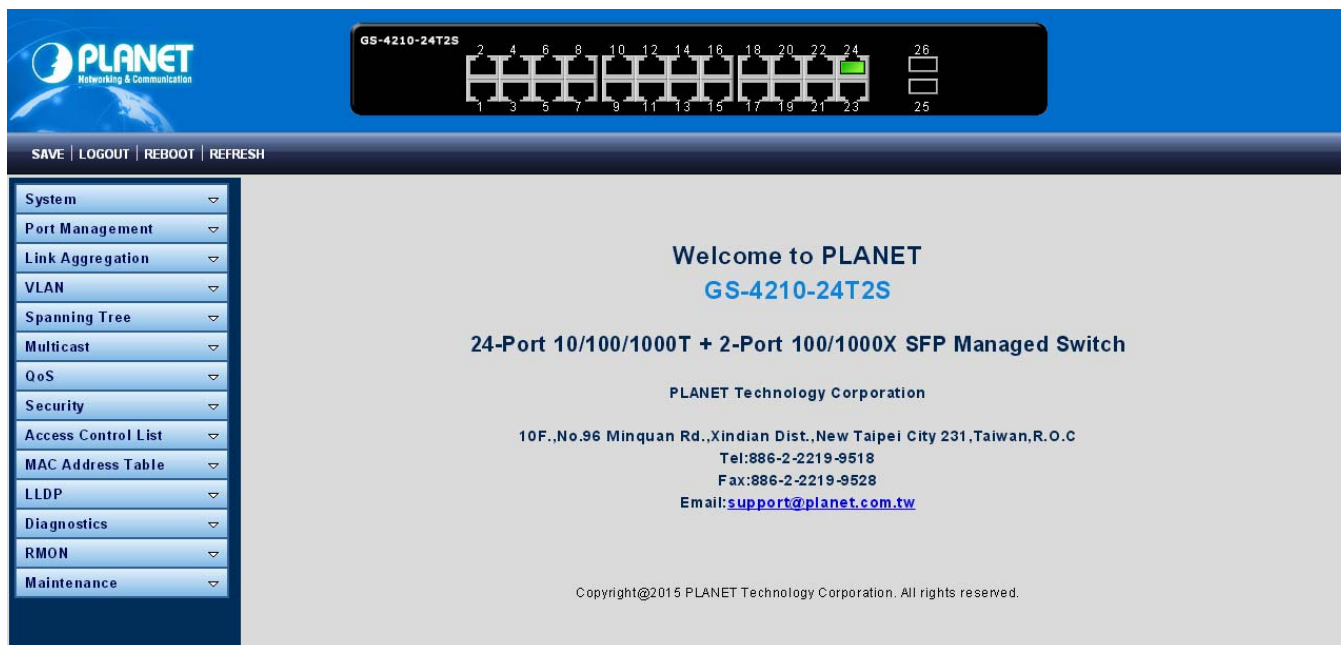


Figure 3-4: Web Main Screen of Managed Switch

3.5 SNMP-based Network Management

You can use an external SNMP-based application to configure and manage the Managed Switch, such as SNMPc 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 gets and sets community strings for the Managed Switch are public.

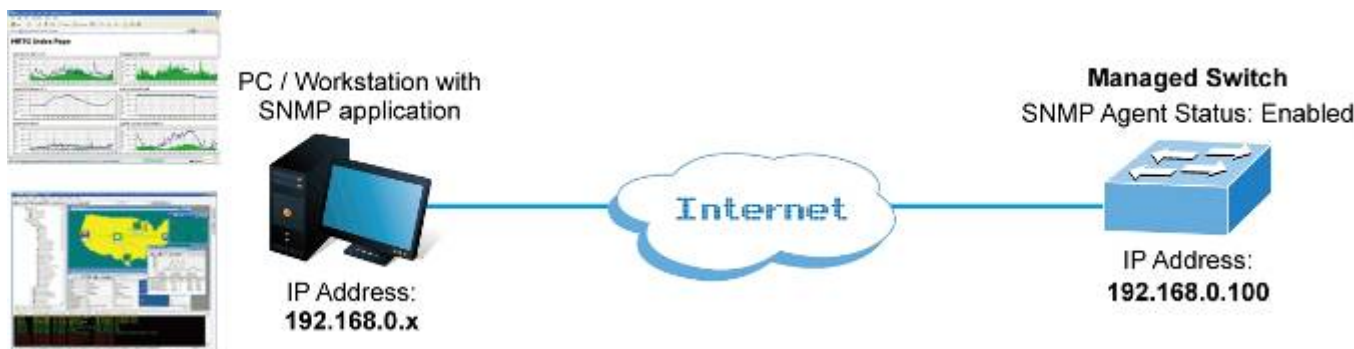


Figure 3-5: SNMP Management

3.6 PLANET Smart Discovery Utility

For easily listing the Managed Switch in your Ethernet environment, the Planet Smart Discovery Utility is an ideal solution. The following installation instructions are to guide you to running the Planet Smart Discovery Utility.

1. Download the PLANET Smart Discovery Utility from PLANET Official Website.
2. Deposit the Planet Smart Discovery Utility in administrator PC.
3. Run this utility as the following screen appears.

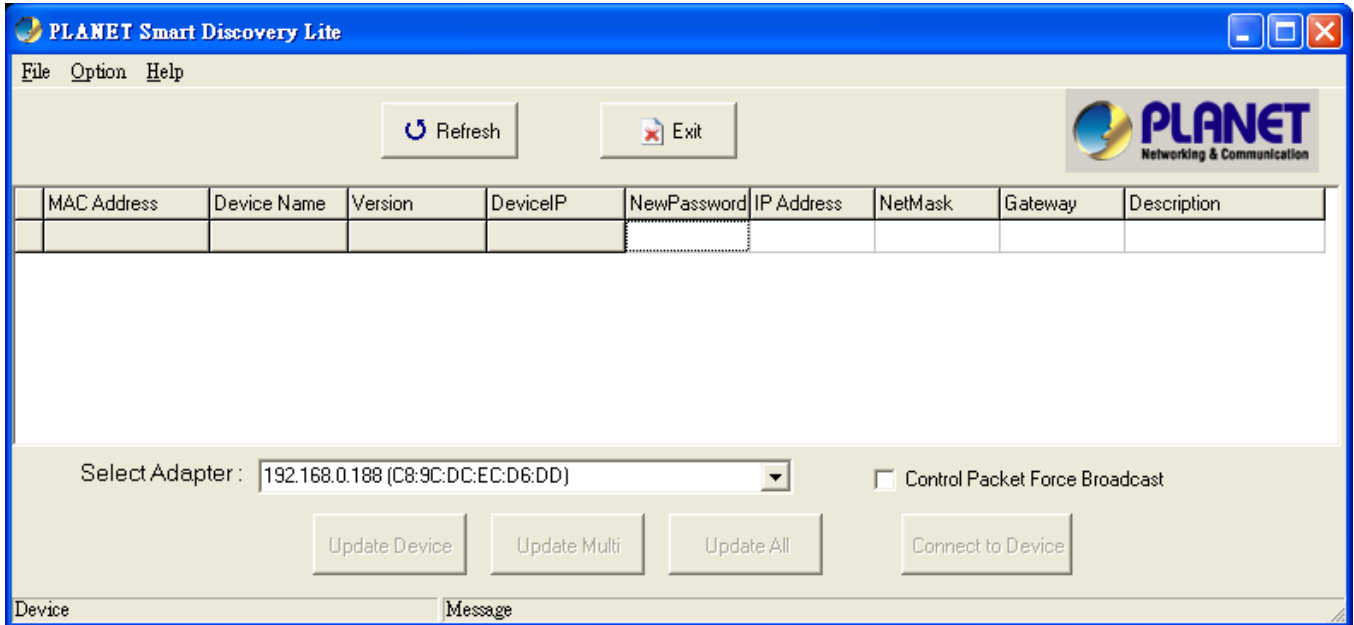


Figure 3-6: Planet Smart Discovery Utility Screen



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

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

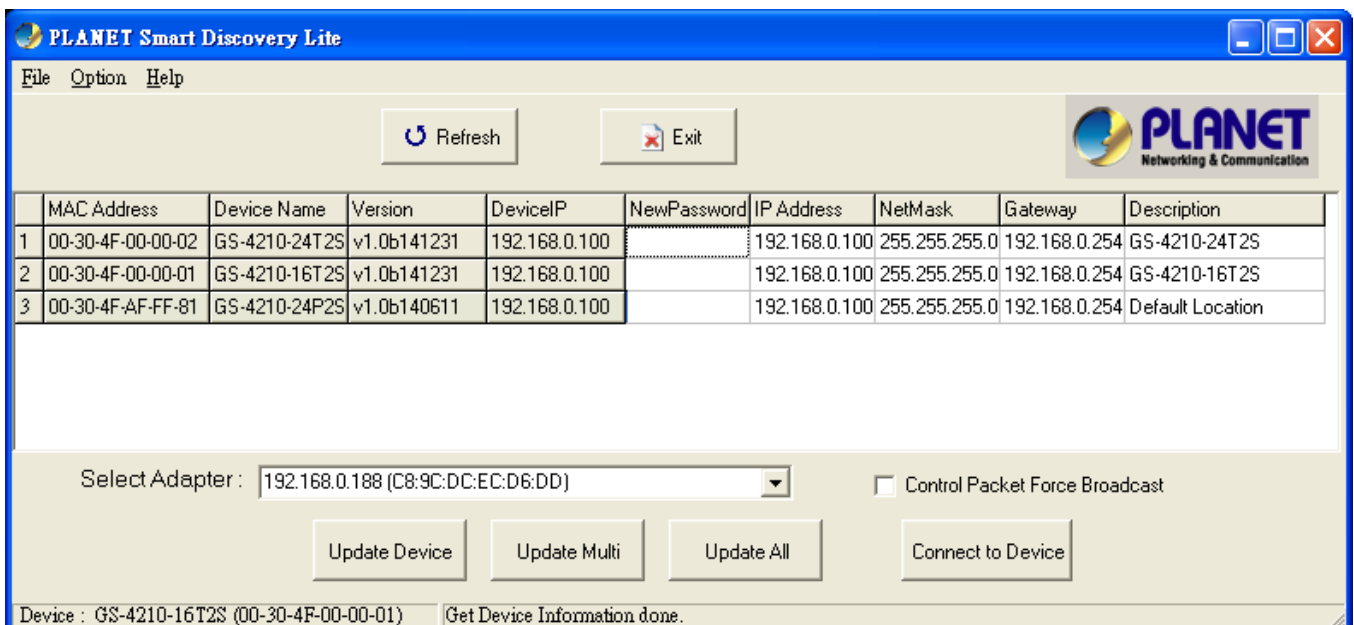


Figure 3-7: Planet Smart Discovery Utility Screen

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 for the devices.
2. After setup is completed, press "**Update Device**", "**Update Multi**" or "**Update All**" button to take effect. The meaning of the 3 buttons above are shown 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 "**Connect to Device**" button and the input username / password in web login screen and the web main screen appears in [Figure 3-4](#).
5. Press "**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.

About Web-based Management

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

The Web-based Management supports Internet Explorer 8.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.



By default, IE8.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

The Managed Switch can be configured through an Ethernet connection, making sure the manager PC must be set on the same IP subnet address as the Managed Switch.

For example, the default IP address of the Managed Switch is **192.168.0.100**, then the manager PC should be set at **192.168.0.x** (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

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

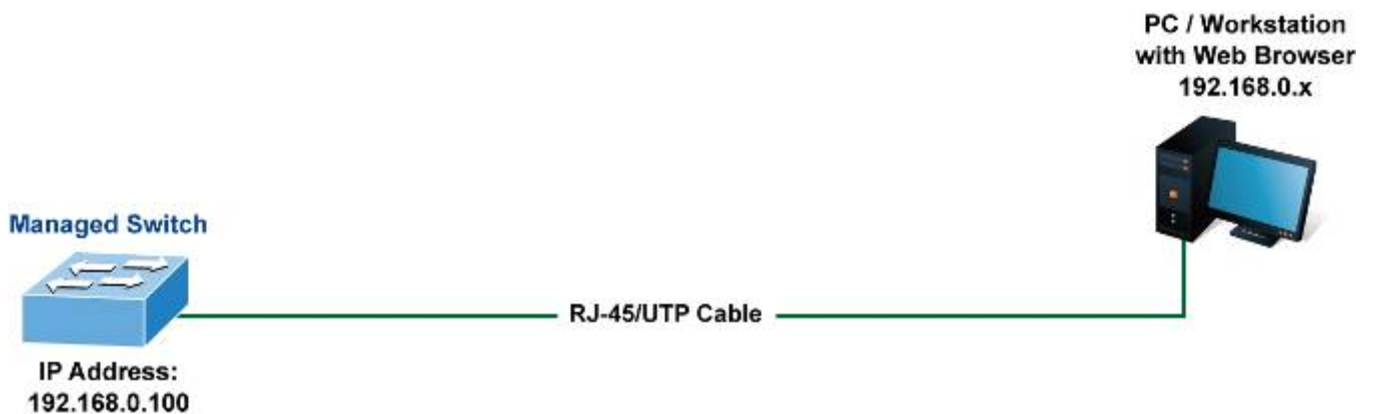


Figure 4-1-1: Web Management

■ Logging on the Managed Switch

1. Use Internet Explorer 8.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP Address as following:

<http://192.168.0.100>

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

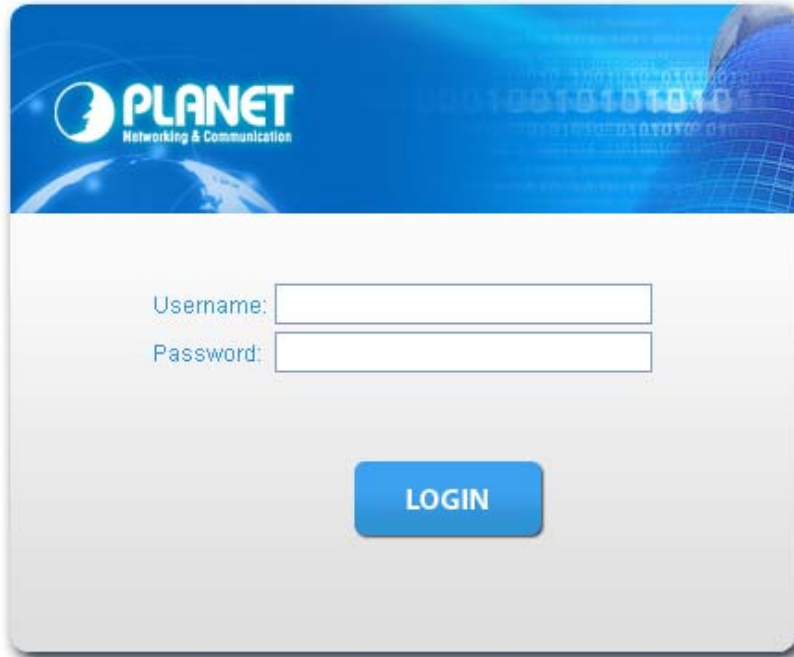


Figure 4-1-2: Login Screen

Default User name: **admin**

Default Password: **admin**



The following web screen based on GS-4210-24T2S will be the same as that of GS-4210-16T2S and GS-4210-24P2S.

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



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

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



- It is recommended to use Internet Explore 8.0 or above to access Managed Switch.
 - The changed IP address takes effect immediately after clicking on the **Apply** button. You need to use the new IP address to access the Web interface.
-



- For security reason, please change and memorize the new password after this first setup.
 - Only accept command in lowercase letter under web interface.
-

4.1 Main Web Page

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

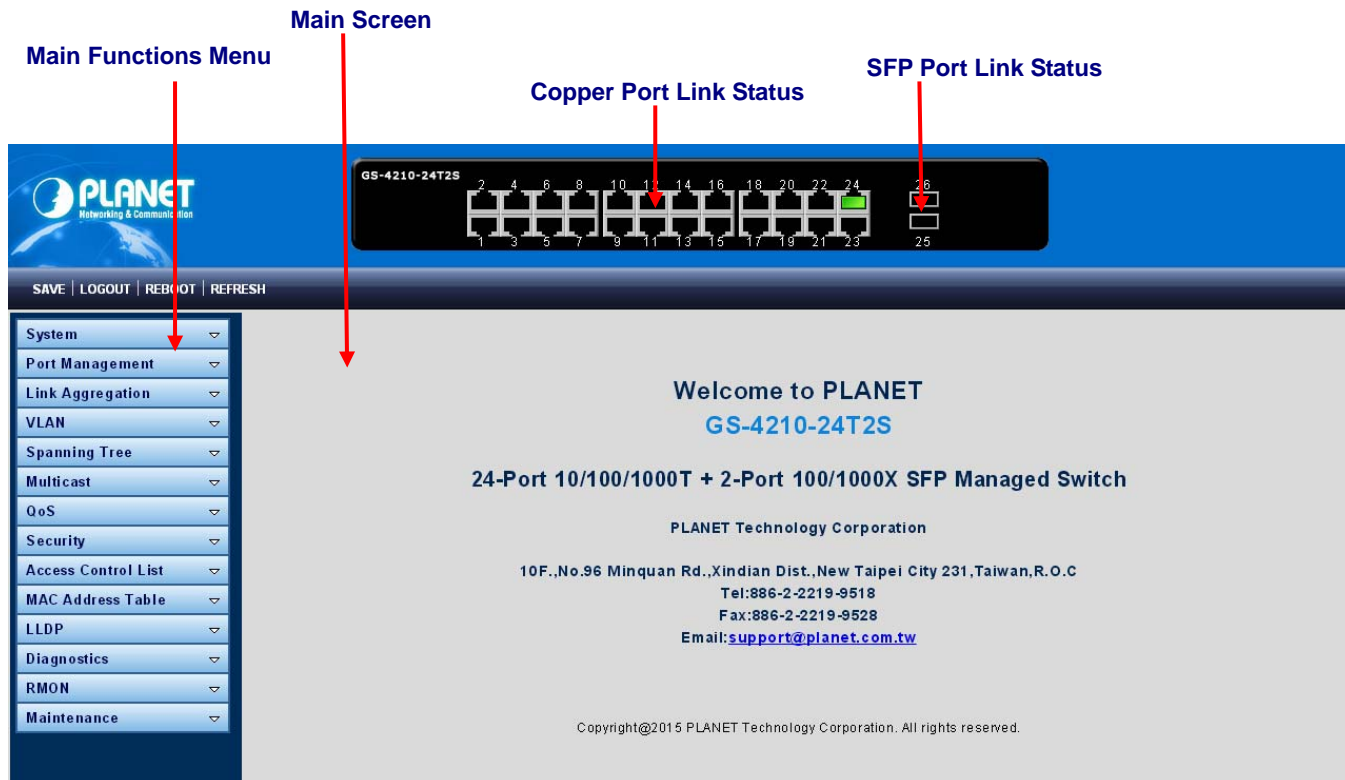


Figure 4-1-4: Web Main Page

Panel Display

The web agent displays an image of the Managed Switch's ports. The Mode can be set to display different information for the ports, including Link up or Link down. Clicking on the image of a port opens the **Port Status** page.

The port states are illustrated as follows:

State	Disabled	Down	Link
RJ45 Ports			
SFP Ports			

Main Menu

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

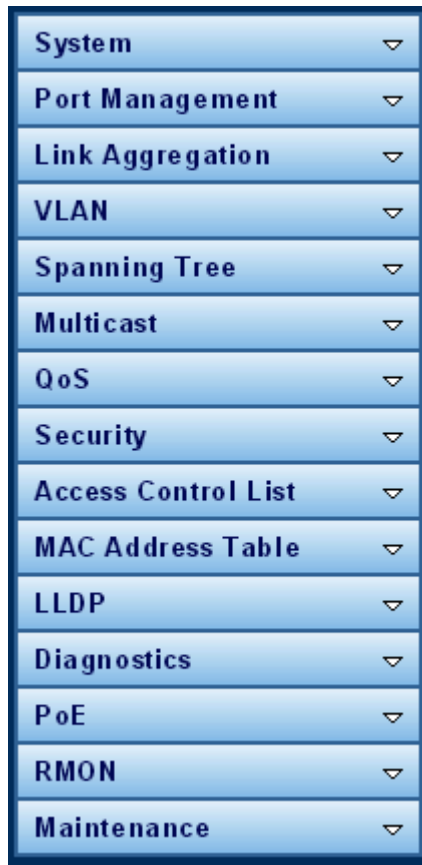


Figure 4-1-5: Managed Switch Main Functions Menu


Buttons

SAVE: Click to save changes or reset to default.

LOGOUT: Click to logout the Managed Switch.

REBOOT: Click to reboot the Managed Switch.

REFRESH: Click to refresh the page.

 The PoE function only available on GS-4210-24P2S, the GS-4210-16T2S / GS-4210-24T2S does not support this function.

4.1.1 Save Button

This save button allows to save the running / startup / backup configuration or reset switch in default parameter. The screen in [Figure 4-1-6](#) appears.

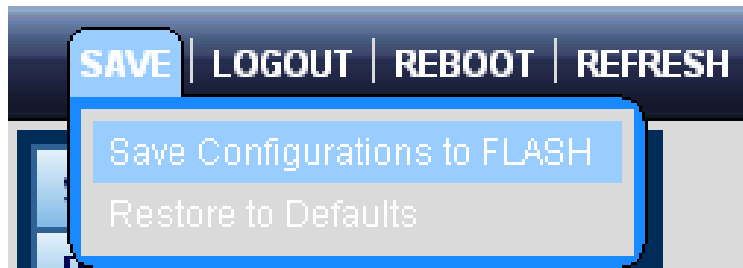


Figure 4-1-6: Save Button Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Save Configuration to FLASH 	Click to save the configuration. For more detailed information, please refer to the chapter 4.1.2.
<ul style="list-style-type: none"> • Restore to Default 	Click to reset switch in default parameter. For more detailed information, please refer to the chapter 4.15.1.

4.1.2 Configuration Manager

The system file folder contains configuration settings. The screen in [Figure 4-1-7](#) appears.

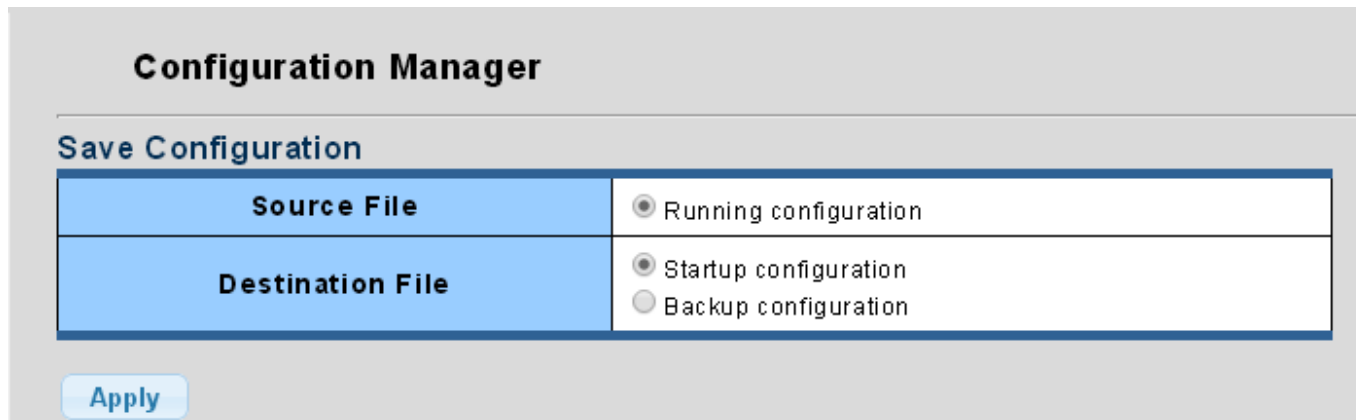



Figure 4-1-7: Save Button Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Running Configuration 	Refers to the running configuration sequence use in the switch. In switch, the running configuration file stores in the RAM. In the current version, the running configuration sequence running-config can be saved from the RAM to FLASH by saving “ Source File = Running Configuration ” to “ Destination File = Startup Configuration ”, so that the running configuration sequence becomes the start

	up configuration file, which is called configuration save. To prevent illicit file upload and easier configuration, switch mandates the name of running configuration file to be running-config.
<ul style="list-style-type: none"> • Startup Configuration 	Refers to the configuration sequence used in switch startup. Startup configuration file stores in nonvolatile storage, corresponding to the so-called configuration save. If the device supports multi-config file, name the configuration file to be .cfg file, the default is startup.cfg. If the device does not support multi-config file, mandates the name of startup configuration file to be startup-config.
<ul style="list-style-type: none"> • Backup Configuration 	The backup configuration is empty in FLASH; please save the backup configuration first by " Maintenance > Backup Manager ".

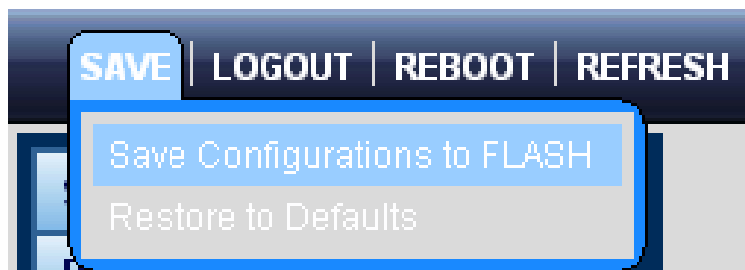
Button

: Click to save configuration.

4.1.2.1 Saving Configuration

In the Managed Switch, the running configuration file stores in the RAM. In the current version, the running configuration sequence of running-config can be saved from the RAM to FLASH by "**Save Configurations to FLASH**" function, so that the running configuration sequence becomes the startup configuration file, which is called configuration save. To save all applied changes and set the current configuration as a startup configuration. The startup-configuration file will be loaded automatically across a system reboot.

1. Click "**SAVE > Save Configurations to FLASH**" to login "**Configuration Manager**" Page.



2. Select "Source File = Running Configuration" and "Destination File = Startup Configuration".

Configuration Manager

Save Configuration

Source File	<input checked="" type="radio"/> Running configuration
Destination File	<input checked="" type="radio"/> Startup configuration <input type="radio"/> Backup configuration

Apply

3. Press the "Apply" button to save running configuration to startup configuration.

4.2 System

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

- **System Information** The switch system information is provided here.
- **IP Configuration** Configure the switch-managed IP information on this page.
- **IPv6 Configuration** Configure the switch-managed IPv6 information on this page.
- **User Configuration** Configure new user name and password on this page.
- **Time Settings** Configure SNTP on this page.
- **Log Management** The switch log information is provided here.
- **SNMP Management** Configure SNMP on this page.

4.2.1 System Information

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

System Information	
Information Name	Information Value
System Name	Edit GS-4210-24T2S
System Description	Edit GS-4210-24T2S
System Contact	Edit Default Contact
MAC Address	00:30:4F:00:00:02
IP Address	10.1.0.213
Subnet Mask	255.255.255.0
Gateway	10.1.0.253
Loader Version	2011.12.41872
Loader Date	Mar 18 2014 - 11:20:25
Firmware Version	v1.0b141231
Firmware Date	Thu Jan 8 19:52:11 CST 2015
System Object ID	1.3.6.1.4.1.10456.1.1543
System Up Time	0 days, 1 hours, 10 mins, 10 secs

Figure 4-2-1: System Information Page Screenshot

The page includes the following fields:

Object	Description
• System Name	Display the current system name.
• System Description	Display the current system description.
• System Contact	Display the current system contact.
• MAC Address	The MAC Address of Managed Switch.
• IP Address	The IP Address of Managed Switch.

• Subnet Mask	The subnet mask of Managed Switch.
• Gateway	The gateway of Managed Switch.
• Loader Version	The loader version of Managed Switch.
• Loader Date	The loader date of Managed Switch.
• Firmware Version	The firmware version of Managed Switch.
• Firmware Date	The firmware date of Managed Switch.
• System Object ID	The system object ID of the Managed Switch.
• System Up Time	The period of time the device has been operational.

Button



: Click to edit parameter.

4.2.2 IP Configuration

The IP Configuration includes the IP Address, Subnet Mask and Gateway. The Configured column is used to view or change the IP configuration. Fill up the IP Address, Subnet Mask and Gateway for the device. The screens in [Figure 4-2-2](#) & [Figure 4-2-3](#) appear.

IP Address

IP Address Setting

Mode	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IP Address	<input type="text" value="192.168.0.100"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.0.254"/>

Figure 4-2-2: IP Address Setting Page Screenshot

The page includes the following fields:

Object	Description
• Mode	<p>Indicates the IP address mode operation. Possible modes are:</p> <p>Static: Enable NTP mode operation.</p> <p>When enable NTP mode operation, the agent forward and to transfer NTP messages between the clients and the server when they are not on the same subnet domain.</p>

	<p>DHCP: Enable DHCP client mode operation.</p> <p>Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.</p>
• IP Address	Provide the IP address of Managed Switch in dotted decimal notation.
• Subnet Mask	Provide the subnet mask of Managed Switch dotted decimal notation.
• Gateway	Provide the IP address of the router in dotted decimal notation.

Button

: Click to apply changes.

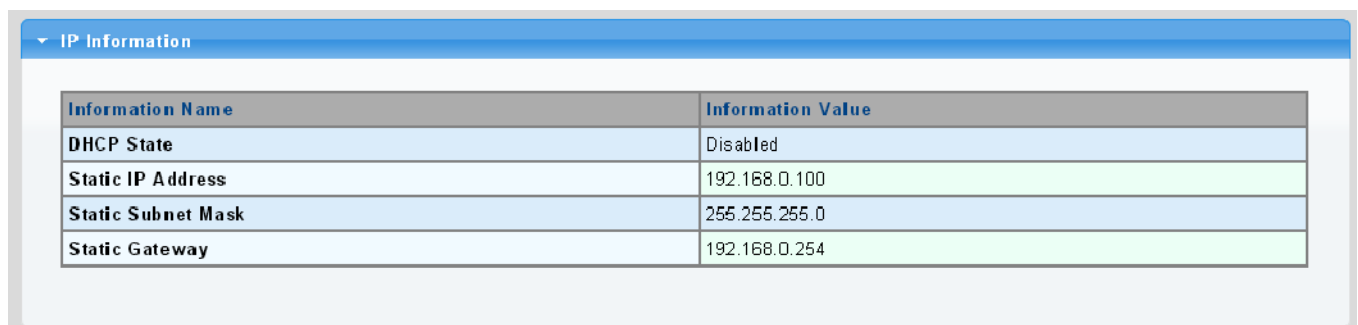


Figure 4-2-3: IP Information Page Screenshot

The page includes the following fields:

Object	Description
• DHCP State	Display the current DHCP state.
• Static IP Address	Display the current IP address.
• Static Subnet Mask	Display the current subnet mask.
• Static Gateway	Display the current gateway.

4.2.3 IPv6 Configuration

The IPv6 Configuration includes Auto Configuration, IPv6 Address and Gateway. The configured column is used to view or change the IPv6 configuration. Fill out the Auto Configuration, IPv6 Address and Gateway for the device. The screens in [Figure 4-2-4](#) and [Figure 4-2-5](#) appear.

Figure 4-2-4: IPv6 Address Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Auto Configuration 	<p>Enable IPv6 auto-configuration by checking this box.</p> <p>If it fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds; the total time needed to complete auto-configuration can be significantly longer.</p>
<ul style="list-style-type: none"> • IPv6 Address 	<p>Provide the IPv6 address of this switch.</p> <p>IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'.</p> <p>The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also uses the following legally IPv4 address. For example, ':192.1.2.34'.</p> <p>Provide the IPv6 Prefix of this switch. The allowed range is 1 through 128.</p>
<ul style="list-style-type: none"> • Gateway 	<p>Provide the IPv6 gateway address of this switch.</p> <p>IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'.</p>
<ul style="list-style-type: none"> • DHCPv6 Client 	<p>To enable this Managed Switch to accept a configuration from a Dynamic Host Configuration Protocol version 6 (DHCPv6) server. By default, the Managed Switch does not perform DHCPv6 client actions. DHCPv6 clients request the delegation of long-lived prefixes that they can push to individual local hosts.</p>

Button

: Click to apply changes.

The screenshot shows a web interface with a blue header bar labeled "IPv6 Information". Below the header is a table with two columns: "Information Name" and "Information Value".

Information Name	Information Value
Auto Configuration	Enabled
IPv6 In Use Address	fe80::2e0:4cff:fe00:0 / 64
IPv6 In Use Router	::
IPv6 Static Address	fe80::2e0:4cff:fe00:0 / 0
IPv6 Static Router	::
DHCPv6 Client	Disabled

Figure 4-2-5: IPv6 Information Page Screenshot

The page includes the following fields:

Object	Description
• Auto Configuration	Display the current auto configuration state.
• IPv6 In Use Address	Display the current IPv6 in-use address.
• IPv6 In Use Router	Display the current in-use gateway.
• IPv6 Static Address	Display the current IPv6 static address.
• IPv6 Static Router	Display the current IPv6 static gateway.
• DHCPv6 Client	Display the current DHCPv6 client status.

4.2.4 User Configuration

This page provides an overview of the current users and privilege type. Currently the only way to login as another user on the web server is to close and reopen the browser. After setup completed, please press “**Apply**” button to take effect. Please login web interface with new user name and password as the screens in [Figure 4-2-6](#) and [Figure 4-2-7](#) appear.

User Name	Password Type	Password	Retype Password
<input type="text"/>	Clear Text ▼	<input type="text"/>	<input type="text"/>

Apply

Figure 4-2-6: Local User Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • User Name 	The name identifying the user. Maximum length: 31 characters; Maximum number of users: 8
<ul style="list-style-type: none"> • Password Type 	The password types for the user. Options: <ul style="list-style-type: none"> • Clear Text • Encrypted • No Password
<ul style="list-style-type: none"> • Password 	Enter the user’s new password here. (Range: 0-30 characters in plain text; case sensitive)
<ul style="list-style-type: none"> • Retype Password 	Please enter the user’s new password here again to confirm.

Button



: Click to apply changes.

User Name	Password Type	Privilege Type	Modify
admin	Encrypted	Admin	Delete

Figure 4-2-7: Local User Page Screenshot

The page includes the following fields:

Object	Description
• User Name	Display the current username.
• Password Type	Display the current password type.
• Privilege Type	Display the current privilege type.
• Modify	Click to modify the local user entry. Delete : Delete the current user

4.2.5 Time Settings

4.2.5.1 System Time

Configure SNTP on this page.

SNTP is an acronym for **Simple Network Time Protocol**, a network protocol for synchronizing the clocks of computer systems. You can specify SNTP Servers and set GMT Time zone. The SNTP Configuration screens in [Figure 4-2-8](#) and [Figure 4-2-9](#) appear.

System Time

System Time Setting

Enable SNTP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Manual Time	Year <input type="text" value="2000"/> Month <input type="text" value="Jan"/> Day <input type="text" value="1"/> Hours <input type="text" value="0"/> Minutes <input type="text" value="0"/> Seconds <input type="text" value="0"/>
Time Zone	<input type="text" value="None"/>
Daylight Saving Time	<input type="text" value="Disable"/>
Daylight Saving Time Offset	<input type="text" value="60"/> (1 - 1440) Minutes
Recurring From	Day <input type="text" value="Sun"/> Week <input type="text" value="1"/> Month <input type="text" value="Jan"/> Hours <input type="text" value="0"/> Minutes <input type="text" value="0"/>
Recurring To	Day <input type="text" value="Sun"/> Week <input type="text" value="1"/> Month <input type="text" value="Jan"/> Hours <input type="text" value="0"/> Minutes <input type="text" value="0"/>
Non-recurring From	Year <input type="text" value="2000"/> Month <input type="text" value="Jan"/> Date <input type="text" value="1"/> Hours <input type="text" value="0"/> Minutes <input type="text" value="0"/>
Non-recurring To	Year <input type="text" value="2000"/> Month <input type="text" value="Jan"/> Date <input type="text" value="1"/> Hours <input type="text" value="0"/> Minutes <input type="text" value="0"/>


Figure 4-2-8: SNTP Setup Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Enable SNTP 	<p>Enabled: Enable SNTP mode operation.</p> <p>When enable SNTP mode operation, the agent forward and to transfer SNTP messages between the clients and the server when they are not on the same subnet domain.</p> <p>Disabled: Disable SNTP mode operation.</p>
<ul style="list-style-type: none"> • Manual Time 	<p>To set time manually.</p> <ul style="list-style-type: none"> • Year - Select the starting Year. • Month - Select the starting month. • Day - Select the starting day. • Hours - Select the starting hour. • Minutes - Select the starting minute. • Seconds - Select the starting seconds.
<ul style="list-style-type: none"> • Time Zone 	<p>Allow select the time zone according to current location of switch.</p>
<ul style="list-style-type: none"> • Daylight Saving Time 	<p>This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default: Disabled).</p>
<ul style="list-style-type: none"> • Daylight Saving Time Offset 	<p>Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440 Minutes)</p>
<ul style="list-style-type: none"> • Recurring From 	<ul style="list-style-type: none"> • Day - Select the starting day. • Week - Select the starting week number. • Month - Select the starting month. • Hours - Select the starting hour. • Minutes - Select the starting minute.
<ul style="list-style-type: none"> • Recurring To 	<ul style="list-style-type: none"> • Day - Select the starting day. • Week - Select the starting week number. • Month - Select the starting month. • Hours - Select the starting hour. • Minutes - Select the starting minute.
<ul style="list-style-type: none"> • Non-recurring From 	<ul style="list-style-type: none"> • Year - Select the starting Year. • Month - Select the starting month. • Date - Select the starting date. • Hours - Select the starting hour. • Minutes - Select the starting minute.

<ul style="list-style-type: none"> • Non-recurring To 	<ul style="list-style-type: none"> • Year - Select the starting Year. • Month - Select the starting month. • Date - Select the starting date. • Hours - Select the starting hour. • Minutes - Select the starting minute.
---	---

Button

: Click to apply changes.

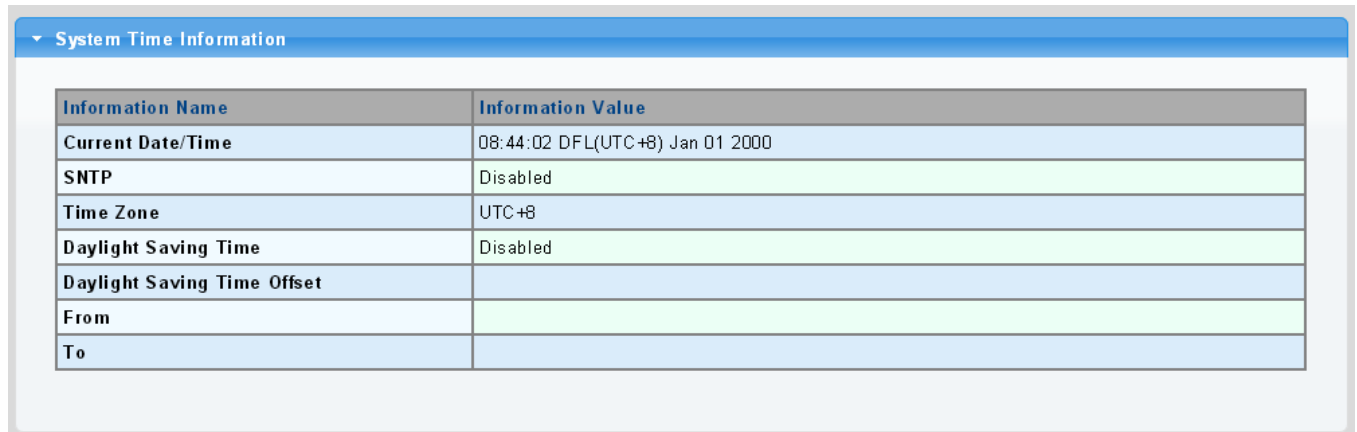


Figure 4-2-9: Time Information Page Screenshot

The page includes the following fields:

Object	Description
• Current Date/Time	Display the current date / time.
• SNTP	Display the current SNTP state.
• Time Zone	Display the current time zone.
• Daylight Saving Time	Display the current daylight saving time state.
• Daylight Saving Time Offset	Display the current daylight saving time offset state.
• From	Display the current daylight saving time from.
• To	Display the current daylight saving time to.

4.2.5.2 SNTP Configuration

The SNTP Server Configuration screens in [Figure 4-2-10](#) & [Figure 4-2-11](#) appear.

Figure 4-2-10: SNTP Setup Page Screenshot

The page includes the following fields:

Object	Description
• SNTP / NTP Server Address	Type the IP address or domain name of the SNTP / NTP server.
• Server Port	Type the port number of the server port. Options: 1-65535 Default: 123

Button

: Click to apply changes.

Figure 4-2-11: SNTP Server Information Page Screenshot

The page includes the following fields:

Object	Description
• SNTP Server Address	Display the current SNTP server address.
• SNTP Server Port	Display the current SNTP server port.

4.2.6 Log Management

The Managed Switch log management is provided here. The local logs allow 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 6 to be logged to RAM. The following table lists the event levels of the Managed Switch:

Level	Severity Name	Description
7	Debug	Debugging messages.
6	Informational	Informational messages only.
5	Notice	Normal but significant condition, such as cold start.
4	Warning	Warning conditions (e.g., return false, unexpected return).
3	Error	Error conditions (e.g., invalid input, default used).
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted).
1	Alert	Immediate action needed.
0	Emergency	System unusable.

4.2.6.1 Logging Service

The Managed Switch system local log information is provided here. The local Log screens in [Figure 4-2-12](#) and [Figure 4-2-13](#) appear.

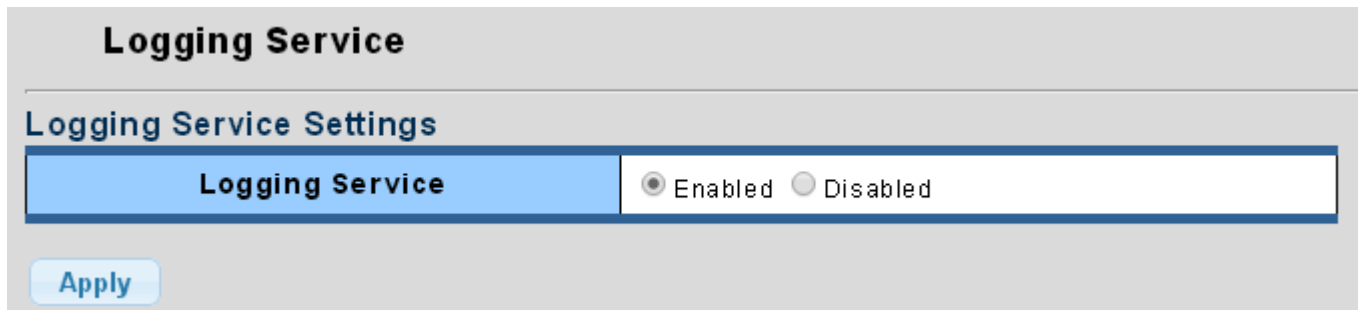


Figure 4-2-12: Logging Settings Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Logging Service 	<p>Enabled: Enable logging service operation.</p> <p>Disabled: Disable logging service operation.</p>

Button

: Click to apply changes.

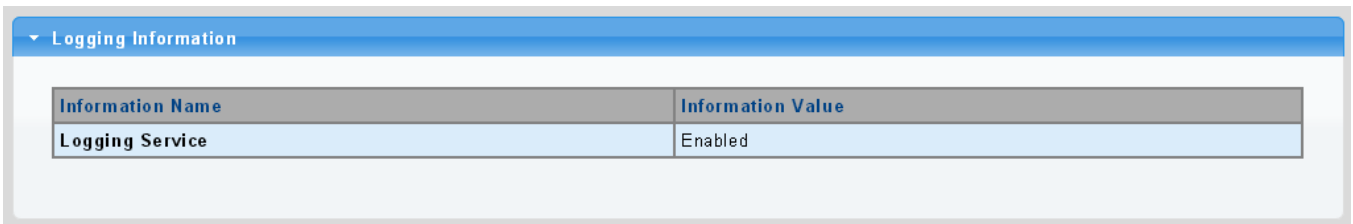


Figure 4-2-13: Logging Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Logging Service 	Display the current logging service status.

4.2.6.2 Local Logging

The Managed Switch system local log information is provided here. The local Log screens in [Figure 4-2-14](#) and [Figure 4-2-15](#) appear.

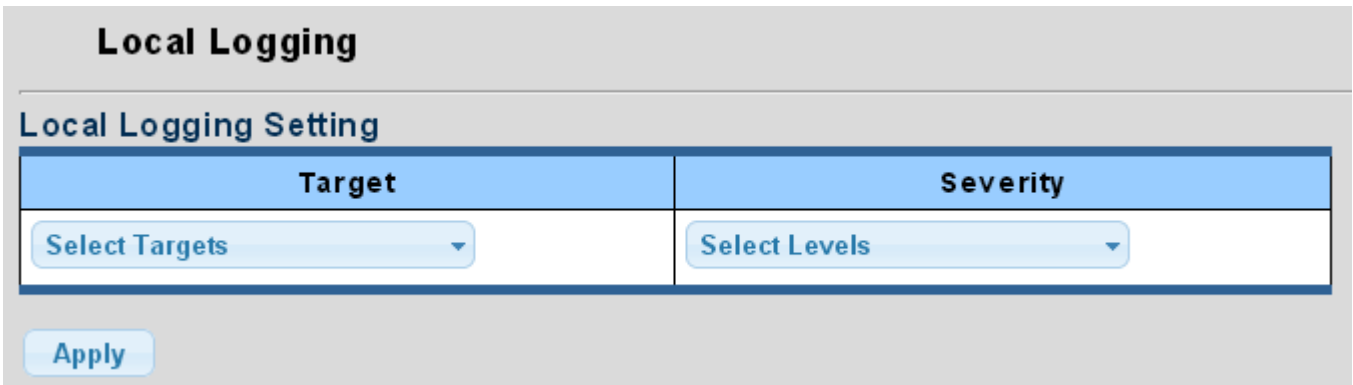


Figure 4-2-14: Local Log Target Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Target 	The target of the local log entry. The following target types are supported: <ul style="list-style-type: none"> Buffered: Target the buffer of the local log. Flash: Target the Flash of the local log.
<ul style="list-style-type: none"> Severity 	The severity of the local log entry. The following severity types are supported: <ul style="list-style-type: none"> Emerg: Emergency level of the system unable for local log. Alert: Alert level of the immediate action needed for local log. Crit: Critical level of the critical conditions for local log. Error: Error level of the error conditions for local log. Warning: Warning level of the warning conditions for local log. Notice: Notice level of the normal but significant conditions for local log. Info: Informational level of the informational messages for local log. Debug: Debug level of the debugging messages for local log.

Button

Apply: Click to apply changes.

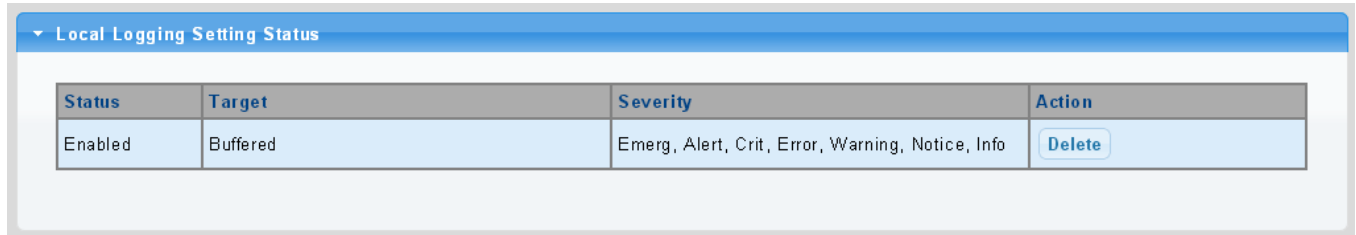


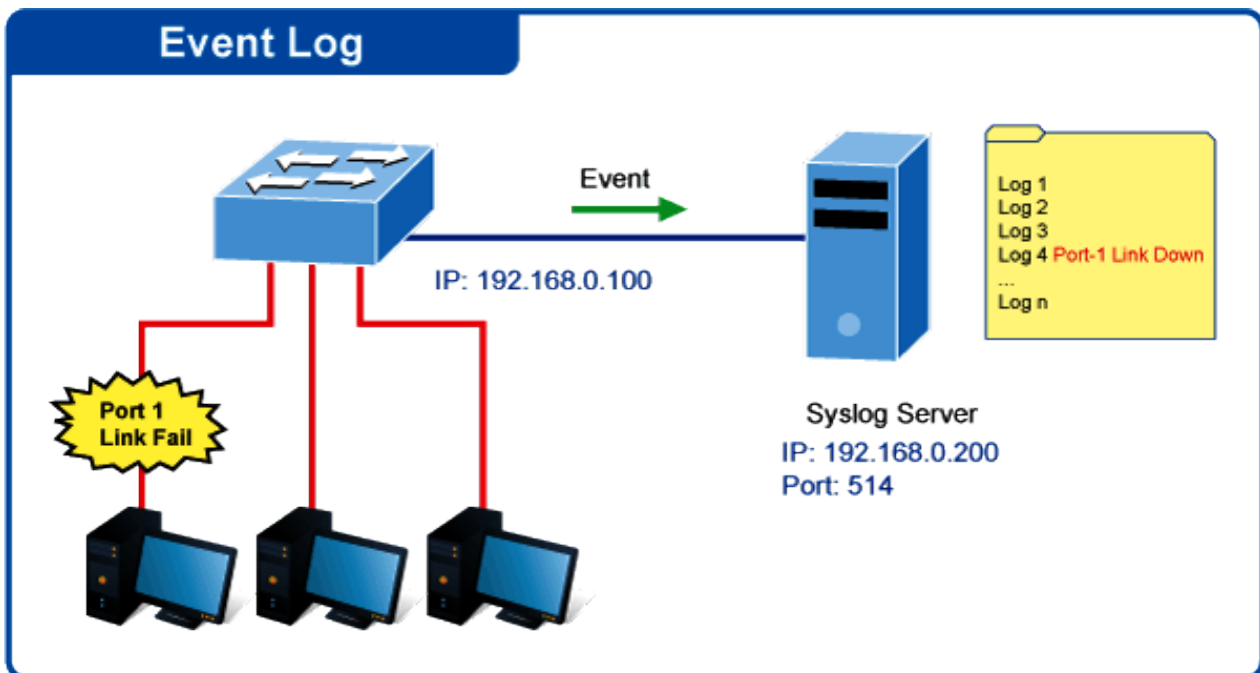
Figure 4-2-15: Local Log Setting Status Page Screenshot

The page includes the following fields:

Object	Description
• Status	Display the current local log state.
• Target	Display the current local log target.
• Severity	Display the current local log severity.
• Action	Delete : Delete the current status.

4.2.6.3 Remote Syslog

Configure remote syslog on this page. The Remote Syslog page allows you to configure the logging of messages that are sent to syslog servers or other management stations. You can also limit the event messages sent to only those messages below a specified level.



The Remote Syslog screens in Figure 4-2-16 and Figure 4-2-17 appear.

Figure 4-2-16: Remote Log Target Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Server Address 	Provide the remote syslog IP address of this Managed Switch.
<ul style="list-style-type: none"> • Server Port 	Provide the port number of remote syslog server. Options: 1-65535 Default Port no: 514
<ul style="list-style-type: none"> • Severity 	The severity of the local log entry. The following severity types are supported: <ul style="list-style-type: none"> ■ Emerg: Emergency level of the system unable for local log. ■ Alert: Alert level of the immediate action needed for local log. ■ Crit: Critical level of the critical conditions for local log. ■ Error: Error level of the error conditions for local log. ■ Warning: Warning level of the warning conditions for local log. ■ Notice: Notice level of the normal but significant conditions for local log. ■ Info: Informational level of the informational messages for local log. ■ Debug: Debug level of the debugging messages for local log.
<ul style="list-style-type: none"> • Facility 	Local0~7 : local user 0~7

Button

: Click to apply changes.

Figure 4-2-17: Remote Log Setting Status Page Screenshot

The page includes the following fields:

Object	Description
• Status	Display the current remote syslog state.
• Server Info	Display the current remote syslog server information.
• Severity	Display the current remote syslog severity.
• Facility	Display the current remote syslog facility.
• Action	Delete : Delete the remote server entry.

4.2.6.4 Logging Message

The switch log view is provided here. The Log View screens in [Figure 4-2-18](#), [Figure 4-2-19](#) and [Figure 4-2-20](#) appear.



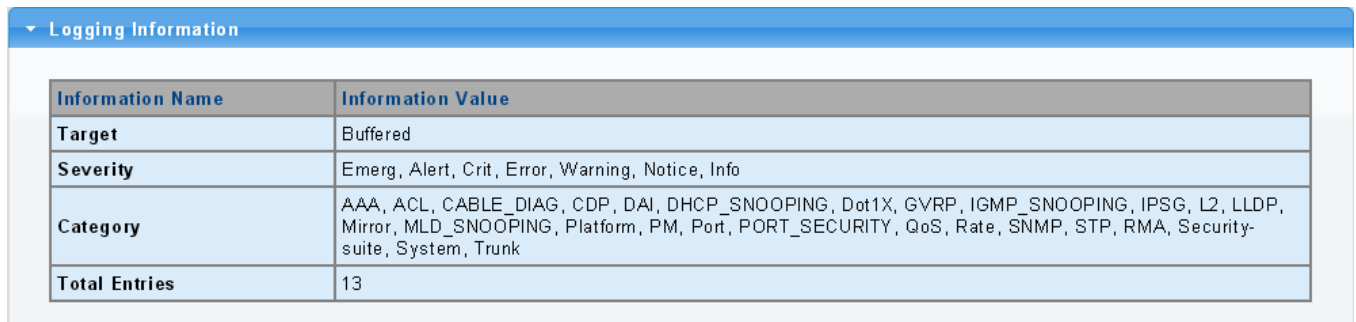
Figure 4-2-18: Log Information Select Page Screenshot

The page includes the following fields:

Object	Description
• Target	The target of the log view entry. The following target types are supported: <ul style="list-style-type: none"> ■ Buffered: Target the buffered of the log view. ■ Flash: Target the Flash of the log view.
• Severity	The severity of the log view entry. The following severity types are supported: <ul style="list-style-type: none"> ■ Emerg: Emergency level of the system unable for log view. ■ Alert: Alert level of the immediate action needed for log view. ■ Crit: Critical level of the critical conditions for log view. ■ Error: Error level of the error conditions for log view. ■ Warning: Warning level of the warning conditions for log view. ■ Notice: Notice level of the normal but significant conditions for log view. ■ Info: Informational level of the informational messages for log view. ■ Debug: Debug level of the debugging messages for log view.
• Category	The category of the log view that includes: AAA, ACL, CABLE_DIAG, CDP, DAI, DHCP_SNOOPING, Dot1X, GVRP, IGMP_SNOOPING, IPSG, L2, LLDP, Mirror, MLD_SNOOPING, Platform, PM, Port, PORT_SECURITY, QoS, Rate, SNMP,STP,RMA, Security-suite,Ststem, Trunk

Button

View: Click to view log.

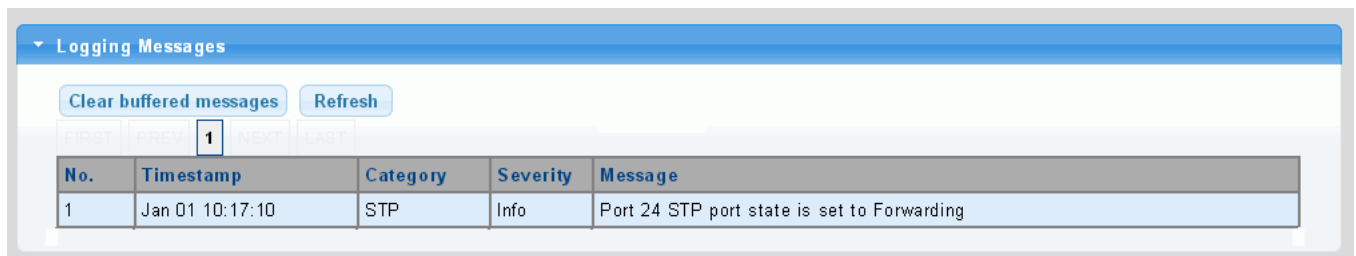


Information Name	Information Value
Target	Buffered
Severity	Emerg, Alert, Crit, Error, Warning, Notice, Info
Category	AAA, ACL, CABLE_DIAG, CDP, DAI, DHCP_SNOOPING, Dot1X, GVRP, IGMP_SNOOPING, IPSPG, L2, LLDP, Mirror, MLD_SNOOPING, Platform, PM, Port, PORT_SECURITY, QoS, Rate, SNMP, STP, RMA, Security-suite, System, Trunk
Total Entries	13

Figure 4-2-19: Logging Information Page Screenshot

The page includes the following fields:

Object	Description
• Target	Display the current log target.
• Severity	Display the current log severity.
• Category	Display the current log category.
• Total Entries	Display the current log entries.



No.	Timestamp	Category	Severity	Message
1	Jan 01 10:17:10	STP	Info	Port 24 STP port state is set to Forwarding

Figure 4-2-20: Logging Messages Page Screenshot

The page includes the following fields:

Object	Description
• No.	This is the number for logs.
• Timestamp	Display the time of log.
• Category	Display the category type.
• Severity	Display the severity type.
• Message	Display the log message.

Buttons

Clear buffered messages: Click to clear the log.

Refresh: Click to refresh the log.

4.2.7 SNMP Management

4.2.7.1 SNMP Overview

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

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

- **Network management stations (NMSs)** : Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **Agents** : Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB)** : A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **network-management protocol** : A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

SNMP Operations

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

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

SNMP community

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

- **Write** = private
- **Read** = public

4.2.7.2 SNMP Setting

Configure SNMP setting on this page. The SNMP System global setting screens in [Figure 4-2-21](#) and [Figure 4-2-22](#) appear.

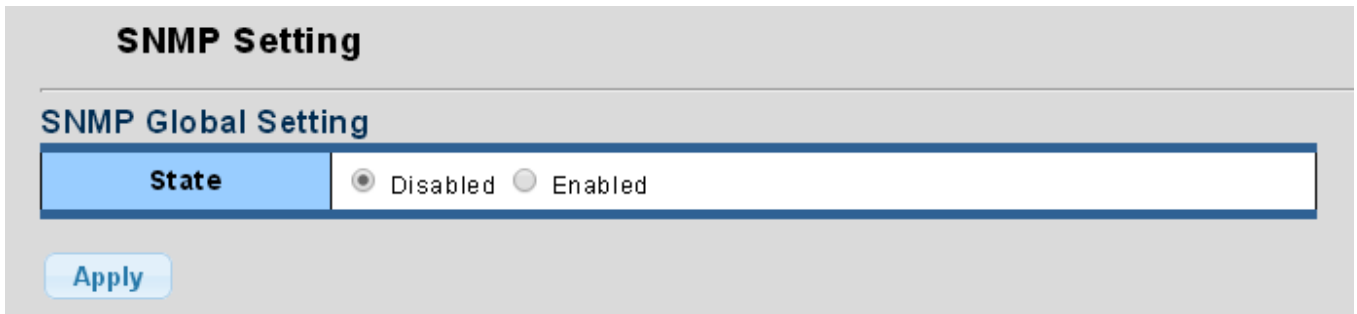


Figure 4-2-21: SNMP Global Setting Page Screenshot

The page includes the following fields:

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

Button

Apply: Click to apply changes.

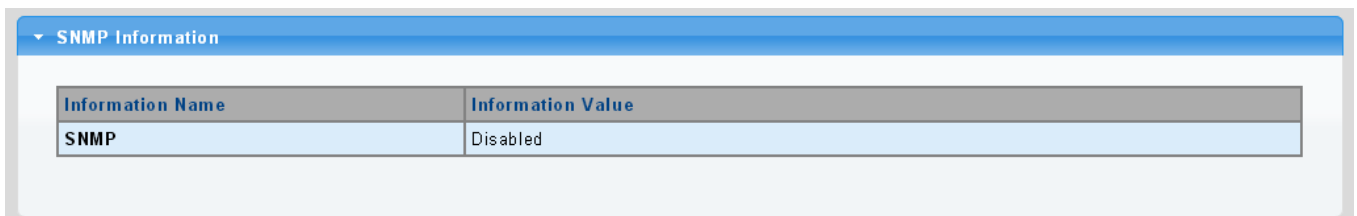


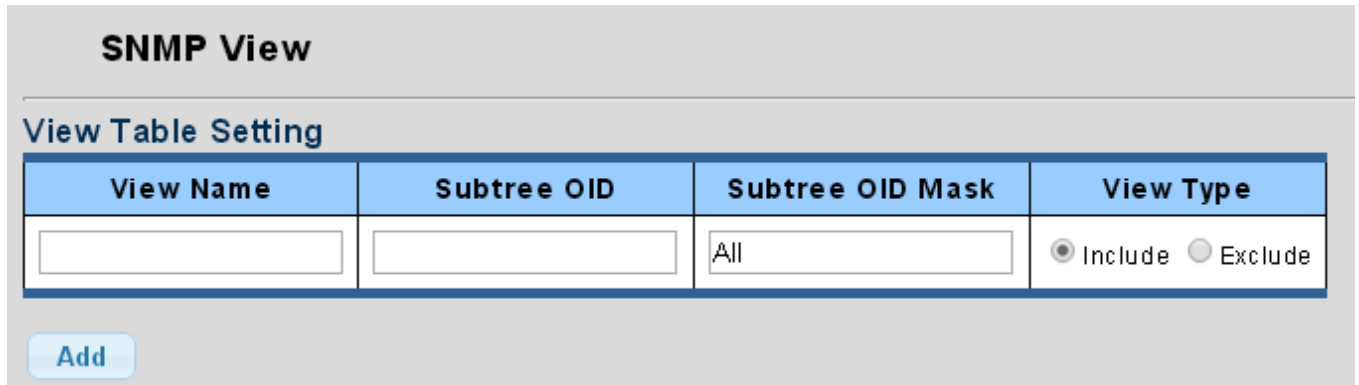
Figure 4-2-22: SNMP Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • SNMP 	Display the current SNMP status

4.2.7.3 SNMP View

Configure SNMPv3 view table on this page. The entry index keys are **View Name** and **OID Subtree**. The SNMPv3 View Table Setting screens in [Figure 4-2-23](#) and [Figure 4-2-24](#) appear.



The screenshot shows the 'SNMP View' configuration page. It features a 'View Table Setting' section with a table for adding new entries. The table has four columns: 'View Name', 'Subtree OID', 'Subtree OID Mask', and 'View Type'. The 'Subtree OID Mask' column contains the text 'All'. The 'View Type' column has two radio buttons: 'Include' (which is selected) and 'Exclude'. Below the table is an 'Add' button.

View Name	Subtree OID	Subtree OID Mask	View Type
<input type="text"/>	<input type="text"/>	All	<input checked="" type="radio"/> Include <input type="radio"/> Exclude

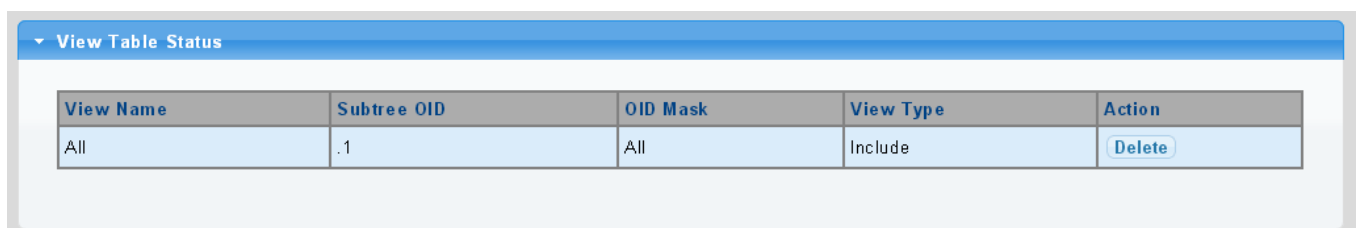
Figure 4-2-23: SNMPv3 View Table Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> View Name 	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 16.
<ul style="list-style-type: none"> Subtree OID 	The OID defining the root of the subtree to add to the named view. The allowed string content is digital number or asterisk(*).
<ul style="list-style-type: none"> Subtree OID Mask 	The bitmask identifies which positions in the specified object identifier are to be regarded as "wildcards" for the purpose of pattern-matching.
<ul style="list-style-type: none"> View Type 	Indicates the view type that this entry should belong to. Possible view type are: Included: An optional flag to indicate that this view subtree should be included. Excluded: An optional flag to indicate that this view subtree should be excluded. General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.

Button

: Click to add a new view entry.



The screenshot shows the 'View Table Status' page. It displays a table with the following data:

View Name	Subtree OID	OID Mask	View Type	Action
All	.1	All	Include	<input type="button" value="Delete"/>

Figure 4-2-24: SNMP View Table Status Page Screenshot

The page includes the following fields:

Object	Description
• View Name	Display the current SNMP view name.
• Subtree OID	Display the current SNMP subtree OID.
• OID Mask	Display the current SNMP OID mask.
• View Type	Display the current SNMP view type.
• Action	Delete : Delete the view table entry.

4.2.7.4 SNMP Access Group

Configure SNMPv3 access group on this page. The entry index keys are **Group Name**, **Security Model** and **Security Level**. The SNMPv3 Access Group Setting screens in [Figure 4-2-25](#) and [Figure 4-2-26](#) appear.

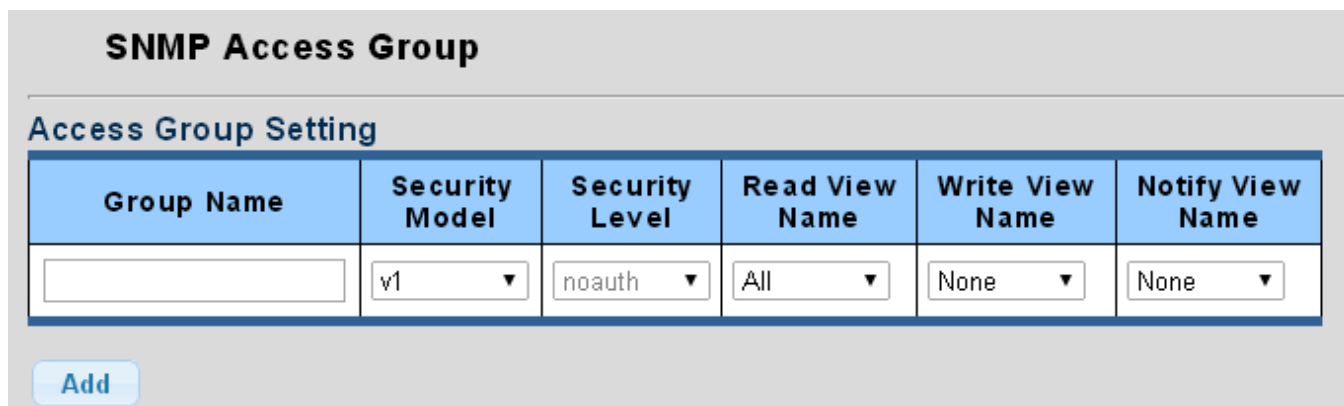



Figure 4-2-25: SNMPv3 Access Group Setting Page Screenshot

The page includes the following fields:

Object	Description
• Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 16.
• Security Model	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none"> ■ v1: Reserved for SNMPv1. ■ v2c: Reserved for SNMPv2c. ■ V3: Reserved for SNMPv3 or User-based Security Model (USM)
• Security Level	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none"> ■ Noauth: None authentication and none privacy security levels are assigned to the group. ■ auth: Authentication and none privacy.

	<ul style="list-style-type: none"> ■ priv: Authentication and privacy. <p>Note: The Security Level applies to SNMPv3 only.</p>
<ul style="list-style-type: none"> • Read View Name 	<p>Read view name is the name of the view in which you can only view the contents of the agent.</p> <p>The allowed string length is 1 to 16.</p>
<ul style="list-style-type: none"> • Write View Name 	<p>Write view name is the name of the view in which you enter data and configure the contents of the agent.</p> <p>The allowed string length is 1 to 16.</p>
<ul style="list-style-type: none"> • Notify View Name 	<p>Notify view name is the name of the view in which you specify a notification, inform, or trap.</p>

Button

 : Click to add a new access entry.

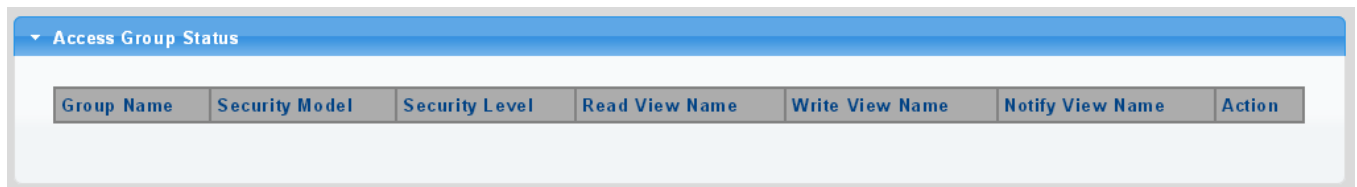



Figure 4-2-26: SNMP view Table Status Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Group Name 	Display the current SNMP access group name.
<ul style="list-style-type: none"> • Security Model 	Display the current security model.
<ul style="list-style-type: none"> • Security Level 	Display the current security level.
<ul style="list-style-type: none"> • Read View Name 	Display the current read view name.
<ul style="list-style-type: none"> • Write View Name 	Display the current write view name.
<ul style="list-style-type: none"> • Notify View Name 	Display the current notify view name.
<ul style="list-style-type: none"> • Action 	 : Delete the access group entry.

4.2.7.5 SNMP Community

Configure SNMP Community on this page. The SNMP Community screens in [Figure 4-2-27](#) and [Figure 4-2-28](#) appear.

The screenshot shows the 'SNMP Community' configuration page. Under the 'Community Setting' section, there is a table with five columns: 'Community Name', 'Community Mode', 'Group Name', 'View Name', and 'Access Right'. Each column contains a text input field or a dropdown menu. The 'Community Mode' dropdown is set to 'Basic', 'View Name' is set to 'All', and 'Access Right' is set to 'ro'. Below the table is a blue 'Add' button.

Figure 4-2-27: Community Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Community Name 	Indicates the community read/write access string to permit access to SNMP agent. The allowed string length is 0 to 16.
<ul style="list-style-type: none"> Community Mode 	Indicates the SNMP community supported mode. Possible versions are: <ul style="list-style-type: none"> ■ Basic: Set SNMP community mode supported version 1 and 2c. ■ Advanced: Set SNMP community mode supported version 3.
<ul style="list-style-type: none"> Group Name 	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 16.
<ul style="list-style-type: none"> View Name 	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 16.
<ul style="list-style-type: none"> Access Right 	Indicates the SNMP community type operation. Possible types are: <ul style="list-style-type: none"> RO=Read-Only: Set access string type in read-only mode. RW=Read-Write: Set access string type in read-write mode.

Button

Add: Click to add a new community name.

The screenshot shows the 'Community Status' page. It features a table with the following columns: 'Community Name', 'Group Name', 'View Name', 'Access Right', and 'Action'. One row is visible with 'public' in the 'Community Name' column, an empty 'Group Name' column, 'All' in the 'View Name' column, 'rw' in the 'Access Right' column, and a 'Delete' button in the 'Action' column.

Figure 4-2-28: Community Status Page Screenshot

The page includes the following fields:

Object	Description
• Community Name	Display the current community type.
• Group Name	Display the current SNMP access group's name.
• View Name	Display the current view name.
• Access Right	Display the current access type.
• Action	Delete : Delete the community entry.

4.2.7.6 SNMP User

Configure SNMPv3 users table on this page. 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. The entry index key is **User Name**. The SNMPv3 User Setting screens in [Figure 4-2-29](#) and [Figure 4-2-30](#) appear.

SNMP User Table

User Setting

User Name	Group	Privilege Mode	Authentication Protocol	Authentication Password	Encryption Protocol	Encryption Key
<input type="text"/>	<input type="text" value=""/>	<input type="text" value="noauth"/>	<input type="text" value="None"/>	<input type="text" value=""/> <small>(8 ~ 16 chars)</small>	<input type="text" value="None"/>	<input type="text" value=""/> <small>(8 ~ 16 chars)</small>


Figure 4-2-29: SNMPv3 Users Configuration Page Screenshot

The page includes the following fields:

Object	Description
• User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 16.
• Group	The SNMP Access Group. A string identifying the group name that this entry should belong to.
• Privilege Mode	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none"> ■ NoAuth: None authentication and none privacy. ■ Auth: Authentication and none privacy. ■ Priv: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means you must first ensure that the value is set correctly.
• Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: <ul style="list-style-type: none"> ■ None: None authentication protocol.

	<ul style="list-style-type: none"> ■ MD5: An optional flag to indicate that this user using MD5 authentication protocol. ■ SHA: An optional flag to indicate that this user using SHA authentication protocol. <p>The value of security level cannot be modified if entry already exists. That means you must first ensure that the value is set correctly.</p>
• Authentication Password	A string identifying the authentication pass phrase. For both MD5 and SHA authentication protocol, the allowed string length is 8 to 16.
• Encryption Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocol are: <ul style="list-style-type: none"> ■ None: None privacy protocol. ■ DES: An optional flag to indicate that this user using DES authentication protocol.
• Encryption Key	A string identifying the privacy pass phrase. The allowed string length is 8 to 16.

Button

 : Click to add a new user entry.

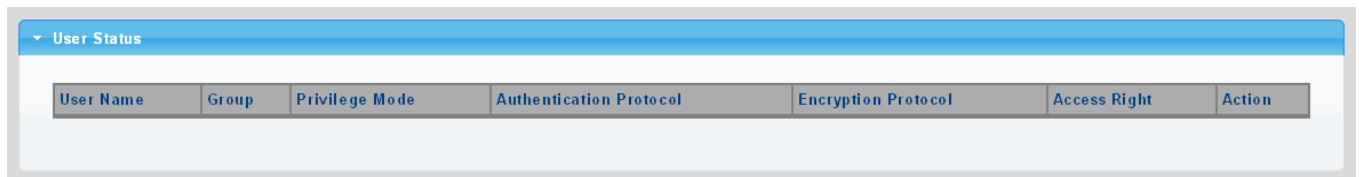



Figure 4-2-30: SNMPv3 Users Status Page Screenshot

The page includes the following fields:

Object	Description
• User Name	Display the current user name.
• Group	Display the current group.
• Privilege Mode	Display the current privilege mode.
• Authentication Protocol	Display the current authentication protocol.
• Encryption Protocol	Display the current encryption protocol.
• Access Right	Display the current access right.
• Action	 : Delete the user entry.

4.2.7.7 SNMPv1, 2 Notification Recipients

Configure SNMPv1 and 2 notification recipients on this page. The SNMPv1, 2 Notification Recipients screens in [Figure 4-2-31](#) and [Figure 4-2-32](#) appear.

Server Address	SNMP Version	Notify Type	Community Name	UDP Port	Time Out	Retries
<input type="text"/>	v1	Traps	public	162 (1-65535)	15 (1-300)	3 (1-255)

[Add](#)

Figure 4-2-31: SNMPv1, 2 Notification Recipients Page Screenshot

The page includes the following fields:

Object	Description
• Server Address	Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
• SNMP Version	Indicates the SNMP trap supported version. Possible versions are: <ul style="list-style-type: none"> ■ SNMP v1: Set SNMP trap supported version 1. ■ SNMP v2c: Set SNMP trap supported version 2c.
• Notify Type	Set the notify type in traps or informs.
• Community Name	Indicates the community access string when send SNMP trap packet.
• UDP Port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535 .
• Time Out	Indicates the SNMP trap inform timeout. The allowed range is 1 to 300 .
• Retries	Indicates the SNMP trap inform retry times. The allowed range is 1 to 255 .

Button

[Add](#): Click to add a new SNMPv1, 2 host entry.

Server Address	SNMP Version	Notify Type	Community Name	UDP Port	Time Out	Retry	Action
----------------	--------------	-------------	----------------	----------	----------	-------	--------

Figure 4-2-32: SNMPv1, 2 Host Status Page Screenshot

The page includes the following fields:

Object	Description
• Server Address	Display the current server address.
• SNMP Version	Display the current SNMP version.
• Notify Type	Display the current notify type.
• Community Name	Display the current community name.
• UDP Port	Display the current UDP port.
• Time Out	Display the current time out.
• Retry	Displays the current retry times.
• Action	Delete : Delete the SNMPv1, 2 host entry.

4.2.7.8 SNMPv3 Notification Recipients

Configure SNMPv3 notification recipients on this page. The SNMPv1, 2 Notification Recipients screens in [Figure 4-2-33](#) and [Figure 4-2-34](#) appear.

Notification Recipients SNMPv3

SNMPv3 Host Setting

Server Address	Notify Type	User Name	UDP Port	TimeOut	Retries
<input style="width: 90%;" type="text"/>	Traps ▼	<input style="width: 90%;" type="text"/>	162 <small>(1-65535)</small>	15 <small>(1-300)</small>	3 <small>(1-255)</small>

Figure 4-2-33: SNMPv3 Notification Recipients Page Screenshot

The page includes the following fields:

Object	Description
• Server Address	Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It can also represent a legally valid IPv4 address. For example, ':::192.1.2.34'.
• Notify Type	Set the notify type in traps or informs.
• User Name	Indicates the user string when send SNMP trap packet.
• UDP Port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message

	via this port, the port range is 1~65535 .
• Time Out	Indicates the SNMP trap inform timeout. The allowed range is 1 to 300 .
• Retries	Indicates the SNMP trap inform retry times. The allowed range is 1 to 255 .

Button

Add : Click to add a new SNMPv3 host entry.

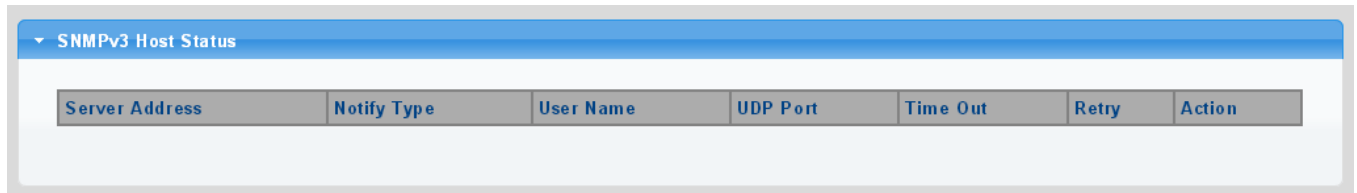


Figure 4-2-34: SNMPv3 Host Status Page Screenshot

The page includes the following fields:

Object	Description
• Server Address	Display the current server address.
• Notify Type	Displays the current notify type.
• User Name	Display the current user name.
• UDP Port	Display the current UDP port.
• Time Out	Display the current time out.
• Retry	Displays the current retry times.
• Action	Delete : Delete the SNMPv3 host entry.

4.2.7.9 SNMP Engine ID

Configure SNMPv3 Engine ID on this page. The entry index key is Engine ID. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. The SNMPv3 Engine ID Setting screens in [Figure 4-2-35](#) and [Figure 4-2-36](#) appear.

Figure 4-2-35: SNMPv3 Engine ID Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Engine ID 	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.

Button

: Click to apply changes.

Figure 4-2-36: SNMPv3 Engine ID Status Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • User Default 	Display the current status.
<ul style="list-style-type: none"> • Engine ID 	Display the current engine ID.

4.2.7.10 SNMP Remote Engine ID

Configure SNMPv3 remote Engine ID on this page. The SNMPv3 Remote Engine ID Setting screens in [Figure 4-2-37](#) and [Figure 4-2-38](#) appear.

Figure 4-2-37: SNMPv3 Remote Engine ID Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Remote IP Address 	Indicates the SNMP remote engine ID address. It allows a valid IP address in dotted decimal notation ('x.y.z.w').
<ul style="list-style-type: none"> • Engine ID 	An octet string identifying the engine ID that this entry should belong to.

Buttons

Add: Click to add a new Engine ID entry.

Figure 4-2-38: SNMPv3 Remote Engine ID Status Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Remote IP Address 	Display the current remote IP address.
<ul style="list-style-type: none"> • Remote Engine ID 	Display the current engine ID.
<ul style="list-style-type: none"> • Action 	<div style="border: 1px solid black; padding: 2px; display: inline-block;">Delete</div> : Delete the remote IP address entry.

4.3 Port Management

Use the Port Menu to display or configure the Managed Switch's ports. This section has the following items:

- **Port Configuration** Configures port configuration settings
- **Port Counters** Lists Ethernet and RMON port statistics
- **Bandwidth Utilization** Display current bandwidth utilization
- **Port Mirroring** Sets the source and target ports for mirroring
- **Jumbo Frame** Set the jumbo frame on the switch
- **Port Error Disabled Configuration** Configures port error disable settings
- **Port Error Disabled Status** Disable port error status
- **Protected Ports** Configures protected ports settings
- **EEE** Configures EEE settings

4.3.1 Port Configuration

This page displays current port configurations and status. Ports can also be configured here. The table has one row for each port on the selected switch in a number of columns, which are:

The Port Configuration screens in [Figure 4-3-1](#) and [Figure 4-3-2](#) appear.

The screenshot shows a web interface titled "Port Setting". Below the title is a section "Port Settings" containing a table with five columns: "Port Select", "Enabled", "Speed", "Duplex", and "Flow Control".

Port Select	Enabled	Speed	Duplex	Flow Control
Select Ports	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Auto	Auto	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Fiber Ports	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Auto-1000M	Full	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Below the table is an "Apply" button.

Figure 4-3-1: Port Settings Page Screenshot

The page includes the following fields:

Object	Description
• Port Select	Select port number for this drop down list.
• Enabled	Indicates the port state operation. Possible state are: Enabled - Start up the port manually. Disabled – Shut down the port manually.
• Speed	Select any available link speed for the given switch port. Draw the menu bar to select the mode.

	<ul style="list-style-type: none"> ■ Auto - Setup Auto negotiation. ■ Auto-10M - Setup 10M Auto negotiation. ■ Auto-100M - Setup 100M Auto negotiation. ■ Auto-1000M - Setup 1000M Auto negotiation. ■ Auto-10/100M - Setup 10/100M Auto negotiation. ■ 10M - Setup 10M Force mode. ■ 100M - Setup 100M Force mode. ■ 1000M - Setup 1000M Force mode.
<ul style="list-style-type: none"> • Duplex 	<p>Select any available link duplex for the given switch port. Draw the menu bar to select the mode.</p> <ul style="list-style-type: none"> ■ Auto - Setup Auto negotiation. ■ Full - Force sets Full-Duplex mode. ■ Half - Force sets Half-Duplex mode.
<ul style="list-style-type: none"> • Flow Control 	<p>When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner.</p> <p>When a fixed-speed setting is selected, that is what is used.</p> <p>Current Rx column indicates whether pause frames on the port are obeyed.</p> <p>Current Tx column indicates whether pause frames on the port are transmitted.</p> <p>The Rx and Tx settings are determined by the result of the last Auto-Negotiation.</p> <p>Check the configured column to use flow control.</p> <p>This setting is related to the setting for Configured Link Speed.</p> <p>Possible state are:</p> <p>Enabled – Enable the flow control function.</p> <p>Disabled – Disable the flow control function.</p>

Button



: Click to apply changes.

Port Status							
Port	Description	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
GE1	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE2	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE3	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE4	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE5	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE6	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE7	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE8	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE9	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE10	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE11	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE12	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE13	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE14	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE15	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE16	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE17	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE18	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE19	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE20	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE21	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE22	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE23	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE24	Edit	Enabled	UP	A-1000M	A-Full	Disabled	Disabled
GE25	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE26	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled

Figure 4-3-2: Port Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	This is the logical port number for this row.
• Description	Click Edit to indicate the port name.
• Enable State	Display the current port state.
• Link Status	Display the current link status.
• Speed	Display the current speed status of the port.
• Duplex	Display the current duplex status of the port.
• Flow Control Configuration	Display the current flow control configuration of the port.
• Flow Control Status	Display the current flow control status of the port.

4.3.2 Port Counters

This page provides an overview of traffic and trunk statistics for all switch ports. The Port Statistics screens in [Figure 4-3-3](#), [Figure 4-3-4](#), [Figure 4-3-5](#) & [Figure 4-3-6](#) appear.

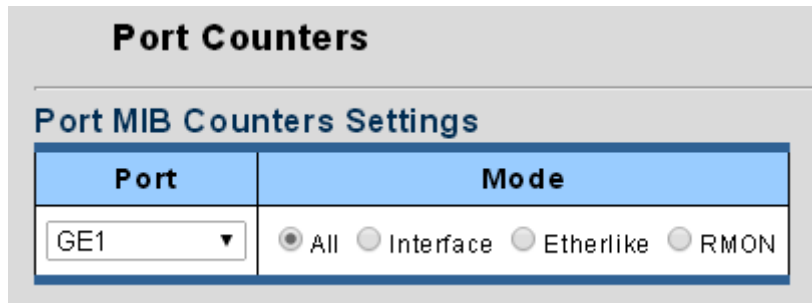


Figure 4-3-3: Port MIB Counters Settings Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	Select port number for this drop down list.
<ul style="list-style-type: none"> • Mode 	Select port counters mode. Options: <ul style="list-style-type: none"> • All • Interface • Etherlike • RMON

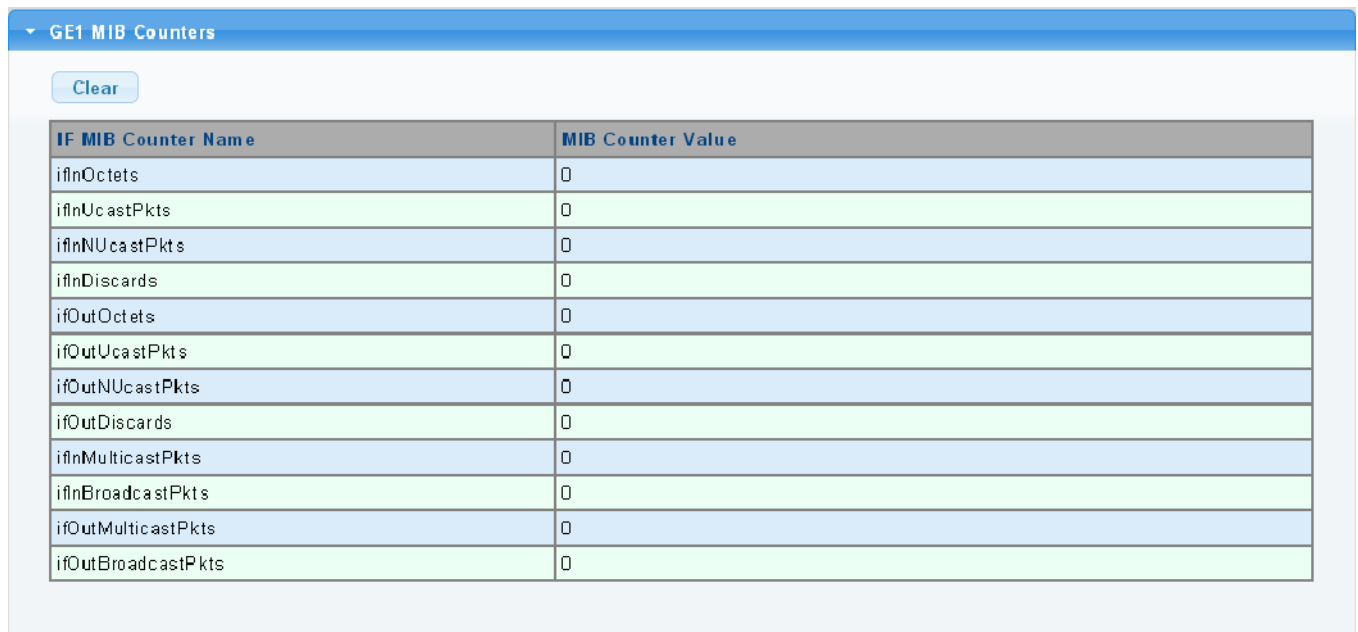


Figure 4-3-4: Interface Counters Page Screenshot

Object	Description
<ul style="list-style-type: none"> • ifInOctets (Received Octets) 	The total number of octets received on the interface, including framing characters.
<ul style="list-style-type: none"> • ifInUcastPkts (Received Unicast Packets) 	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
<ul style="list-style-type: none"> • ifInNUcastPkts (Received Nuknown Unicast Packets) 	The number of packets received via the interfaces which were discarded because of an unknown or unsupported protocol.
<ul style="list-style-type: none"> • ifInDiscards (Received Discards Packets) 	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
<ul style="list-style-type: none"> • ifOutOctets (Transmit Octets) 	The total number of octets transmitted out of the interface, including framing characters.
<ul style="list-style-type: none"> • ifOutUcastPkts (Transmit Unicast Packets) 	The total number of packets that higher-level protocols requested is transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
<ul style="list-style-type: none"> • ifOutNUcastPkts (Transmit Nuknown Unicast Packets) 	The total number of packets that higher-level protocols requested betransmitted to a subnetwork-unicast address, including those that were discarded or not sent.
<ul style="list-style-type: none"> • ifOutDiscards (Transmit Discards Packets) 	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to ahigher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
<ul style="list-style-type: none"> • ifInMulticastPkts (Received Multicast Packets) 	The number of packets, delivered by this sub-layer to a higher (sub-) layer, which were addressed to a multicast address at this sub-layer.
<ul style="list-style-type: none"> • ifInBroadcastPkts (Received Broadcast Packets) 	The number of packets, delivered by this sub-layer to a higher (sub-) layer, which were addressed to a broadcast address at this sub-layer.
<ul style="list-style-type: none"> • ifOutMulticastPkts (Transmit Multicast Packets) 	The total number of packets that higher-level protocols requested betransmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
<ul style="list-style-type: none"> • ifOutBroadcastPkts (Transmit Broadcast Packets) 	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

GE1 MIB Counters	
Clear	
IF MIB Counter Name	MIB Counter Value
dot3StatsAlignmentErrors	0
dot3StatsFCSErrors	0
dot3StatsSingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0
dot3StatsFrameTooLongs	0
dot3StatsSymbolErrors	0
dot3ControlInUnknownOpcodes	0
dot3InPauseFrames	0
dot3OutPauseFrames	0

Figure 4-3-5: Ethernet link Counters Page Screenshot

Object	Description
• dot3StatsAlignmentErrors	The number of alignment errors (missynchronized data packets).
• dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
• dot3StatsSingleCollisionFrames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
• dot3StatsMultipleCollisionFrames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
• dot3StatsDeferredTransmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
• dot3StatsLateCollisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
• dot3StatsExcessiveCollisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
• dot3StatsFrameTooLongs	A count of frames received on particular interfaces that exceed the maximum permitted frame size.
• dot3StatsSymbolErrors	The number of received and transmitted symbol errors.
• dot3ControlInUnknownOpcodes	The number of received control unknown opcodes
• dot3InPauseFrames	The number of received pause frames
• dot3OutPauseFrames	The number of transmitted pause frames

GE1 MIB Counters	
IF MIB Counter Name	MIB Counter Value
etherStatsDropEvents	0
etherStatsOctets	0
etherStatsPkts	0
etherStatsBroadcastPkts	0
etherStatsMulticastPkts	0
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	0
etherStatsPkts65to127Octets	0
etherStatsPkts128to255Octets	0
etherStatsPkts256to511Octets	0
etherStatsPkts512to1023Octets	0
etherStatsPkts1024to1518Octets	0

Figure 4-3-6: RMON Counters Page Screenshot

Object	Description
• etherStatsDropEvents	The total number of events in which packets were dropped due to lack of resources.
• etherStatsOctets	The total number of octets received and transmitted on the interface, including framing characters.
• etherStatsPkts	The total number of packets received and transmitted on the interface.
• etherStatsBroadcastPkts	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
• etherStatsMulticastPkts	The total number of good frames received that were directed to this multicast address.
• etherStatsCRCAlignErrors	The number of CRC/alignment errors (FCS or alignment errors).
• etherStatsUnderSizePkts	The total number of frames received that were less than 64 octets long(excluding framing bits, but including FCS octets) and were otherwise well formed.
• etherStatsOverSizePkts	The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets) and were otherwise well formed.
• etherStatsFragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
• etherStatsJabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS

	or alignment error.
<ul style="list-style-type: none"> • etherStatsCollisions 	The best estimate of the total number of collisions on this Ethernet segment.
<ul style="list-style-type: none"> • etherStatsPkts64Octets 	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
<ul style="list-style-type: none"> • etherStatsPkts65to127Octets • etherStatsPkts128to255Octets • etherStatsPkts256to511Octets • etherStatsPkts512to1023Octets • etherStatsPkts1024to1518Octets 	The total number of frames (including bad packets) received and transmitted where the numbers of octets fall within the specified range (excluding framing bits but including FCS octets).

4.3.3 Bandwidth Utilization

The **Bandwidth Utilization** page displays the percentage of the total available bandwidth being used on the ports. Bandwidth utilization statistics can be viewed using a line graph. The Bandwidth Utilization screen in [Figure 4-3-7](#) appears.

To view the port utilization, click on the **Port Management** folder and then the **Bandwidth Utilization** link:



Figure 4-3-7: Port Bandwidth Utilization Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Refresh Period 	This shows the period interval between last and next refresh. Options: <ul style="list-style-type: none"> ■ 2 sec ■ 5 sec ■ 10 sec
<ul style="list-style-type: none"> IFG 	Allow user to enable or disable this function

4.3.4 Port Mirroring

Configure port Mirroring on this page. This function provide to monitoring network traffic that forwards a copy of each incoming or outgoing packet from one port of a network Switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.

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

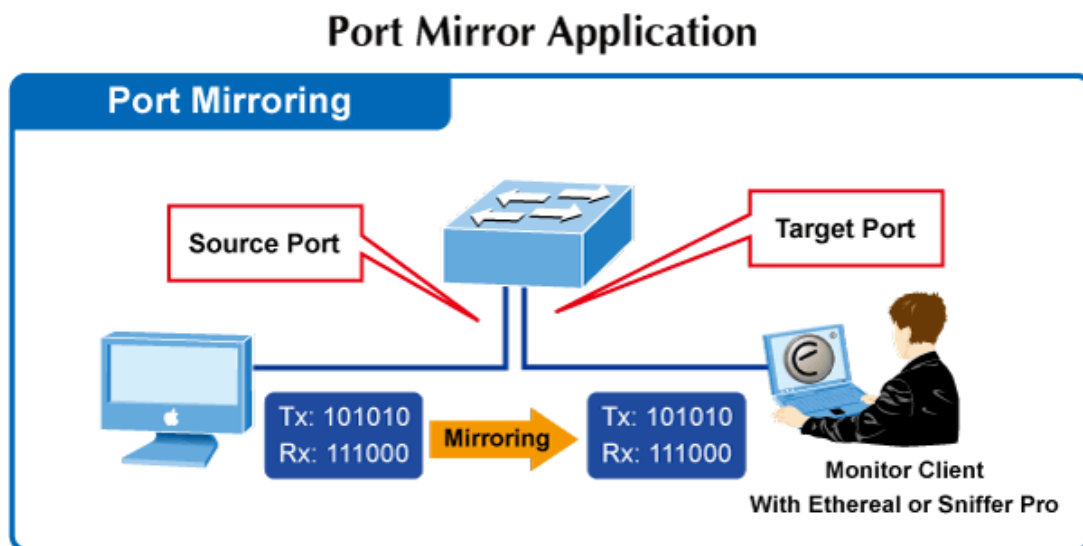


Figure 4-3-8: Port Mirror Application

The traffic to be copied to the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

Mirror Port Configuration

The Port Mirror Configuration screens in [Figure 4-3-9](#) and [Figure 4-3-10](#) appear.

Mirror Setting	
Session ID	Select Session ▼
Monitor Session State	Disabled ▼
Destination Port	GE1 ▼
Allow-Ingress	Disable ▼
Sniffer RX Ports	Select RX Ports ▼
Sniffer TX Ports	Select TX Ports ▼

Apply

Figure 4-3-9: Port Mirroring Settings Page Screenshot

The page includes the following fields:

Object	Description
• Session ID	Set the port mirror session ID. Possible ID are: 1 to 4.
• Monitor Session State	Enable or disable the port mirroring function.
• Destination Port	Select the port to mirror destination port.
• Allow-Ingress	Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port.
• Sniffer RX Ports	Frames received at these ports are mirrored to the mirroring port. Frames transmitted are not mirrored.
• Sniffer TX Ports	Frames transmitted from these ports are mirrored to the mirroring port. Frames received are not mirrored.

Button

: Click to apply changes.

Session ID	Destination Port	Ingress State	Source TX Port	Source RX Port
1	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A

Figure 4-3-10: Mirroring Status Page Screenshot

The page includes the following fields:

Object	Description
• Session ID	Display the session ID.
• Destination Port	This is the mirroring port entry.
• Ingress State	Display the ingress state.
• Source TX Port	Display the current TX ports.
• Source RX Port	Display the current RX ports.

4.3.5 Jumbo Frame

This page provides to select the maximum frame size allowed for the switch port. The Jumbo Frame screens in [Figure 4-3-11](#) and [Figure 4-3-12](#) appear.

Figure 4-3-11: Jumbo Frame Setting Page Screenshot

The page includes the following fields:

Object	Description
• Jumbo Frame (Bytes)	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 64 bytes to 9216 bytes.

Button



: Click to apply changes.

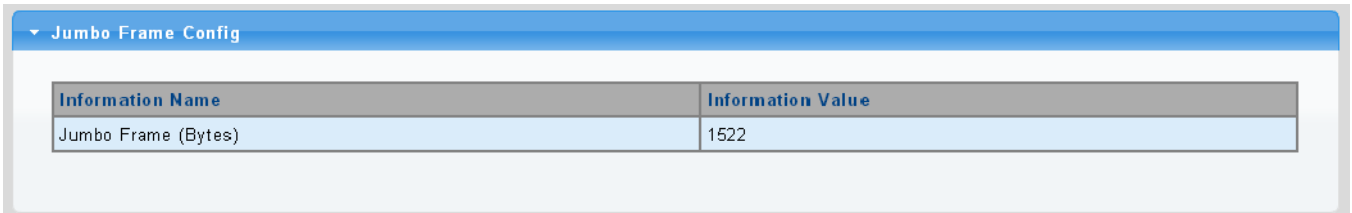


Figure 4-3-12: Jumbo Frame Information Page Screenshot

The page includes the following fields:

Object	Description
• Jumbo	Display the current maximum frame size.

4.3.6 Port Error Disabled Configuration

This page provides to set port error disable function. The Port Error Disable Configuration screens in [Figure 4-3-13](#) and [Figure 4-3-14](#) appear.

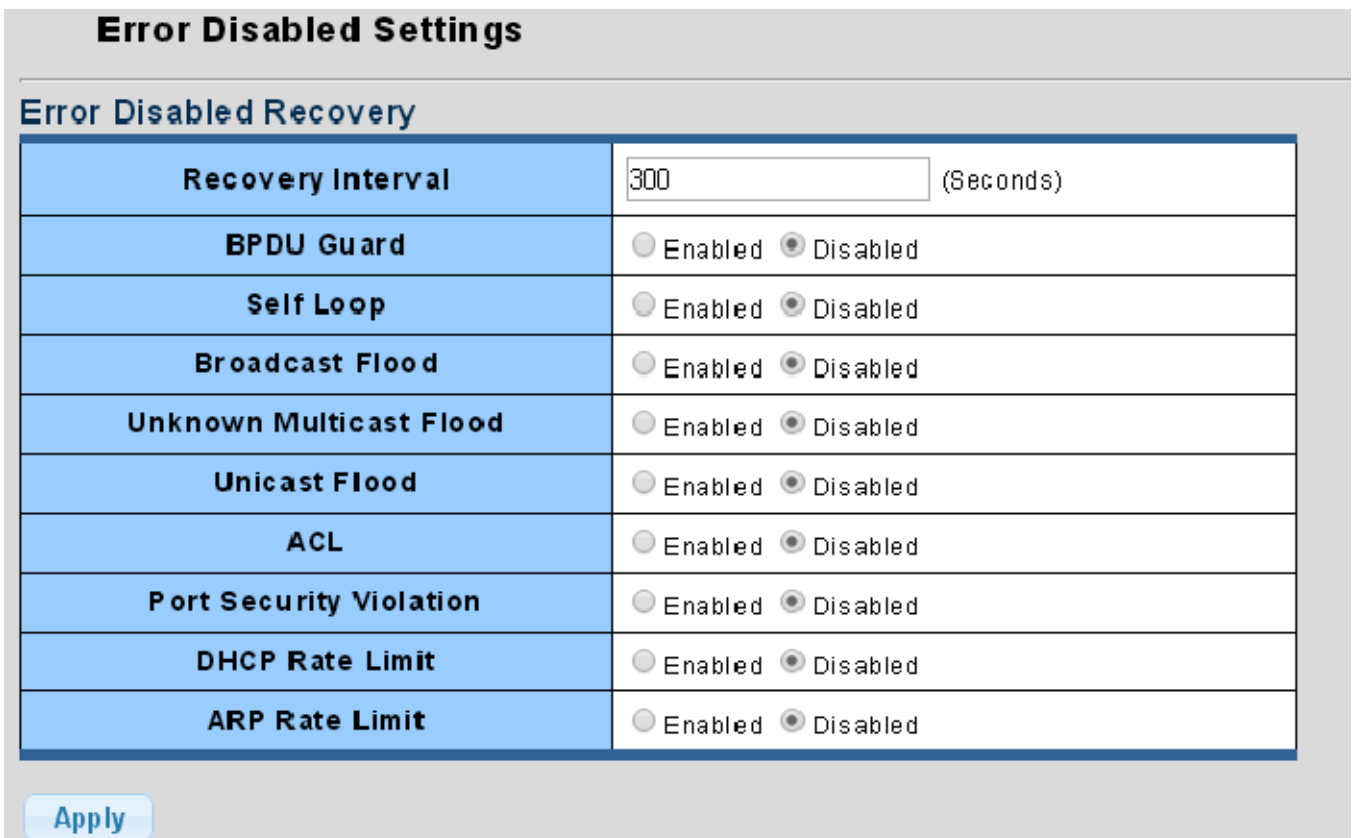



Figure 4-3-13: Error Disabled Recovery Page Screenshot

The page includes the following fields:

Object	Description
• Recovery Interval	The period (in seconds) for which a port will be kept disabled in the event of a port error is detected (and the port action shuts down the port). Default is 300 seconds.
• BPDU Guard	Enable or disable the port error disabled function to check status by BPDU guard.
• Self Loop	Enable or disable the port error disabled function to check status by self loop.
• Broadcast Flood	Enable or disable the port error disabled function to check status by broadcast flood.
• Unknown Multicast Flood	Enable or disable the port error disabled function to check status by unknown multicast flood.
• Unicast Flood	Enable or disable the port error disabled function to check status by unicast flood.
• ACL	Enable or disable the port error disabled function to check status by ACL.
• Port Security Violation	Enable or disable the port error disabled function to check status by port security violation.
• DHCP Rate Limit	Enable or disable the port error disabled function to check status by DHCP rate limit
• ARP Rate Limit	Enable or disable the port error disabled function to check status by ARP rate limit

Button

 : Click to apply changes.

Error Disable Information	
Information Name	Information Value
Recovery Interval	300
BPDU Guard	Disabled
Self Loop	Disabled
Broadcast Flood	Disabled
Unknown Multicast Flood	Disabled
Unicast Flood	Disabled
ACL	Disabled
Port Security Violation	Disabled
DHCP Rate Limit	Disabled
ARP Rate Limit	Disabled

Figure 4-3-14: Error Disabled Information Page Screenshot

The page includes the following fields:

Object	Description
• Recovery Interval	Display the current recovery interval time.
• BPDU Guard	Display the current BPDU guard status.
• Self Loop	Display the current self loop status.
• Broadcast Flood	Display the current broadcast flood status.
• Unknown Multicast Flood	Display the current unknown multicast flood status.
• Unicast Flood	Display the current unicast flood status.
• ACL	Display the current ACL status.
• Port Security Violation	Display the current port security violation status.
• DHCP Rate Limit	Display the current DHCP rate limit status.
• ARP Rate Limit	Display the current ARP rate limit status.

4.3.7 Port Error Disabled Status

This page provides details that transition a port into error disabled and the recovery options. The ports were disabled by some protocols such as BPDU Guard, Loopback and UDLD. The Port Error Disable screen in [Figure 4-3-15](#) appears.

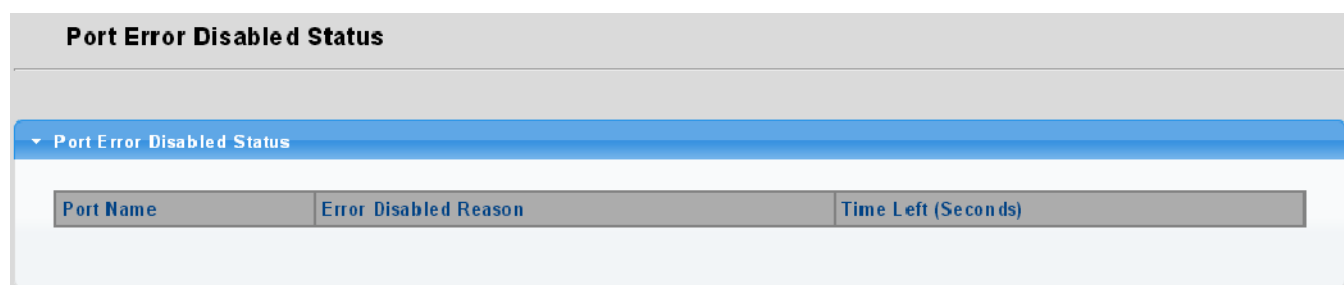


Figure 4-3-15: Port Error Disable Status Page Screenshot

The displayed counters are:

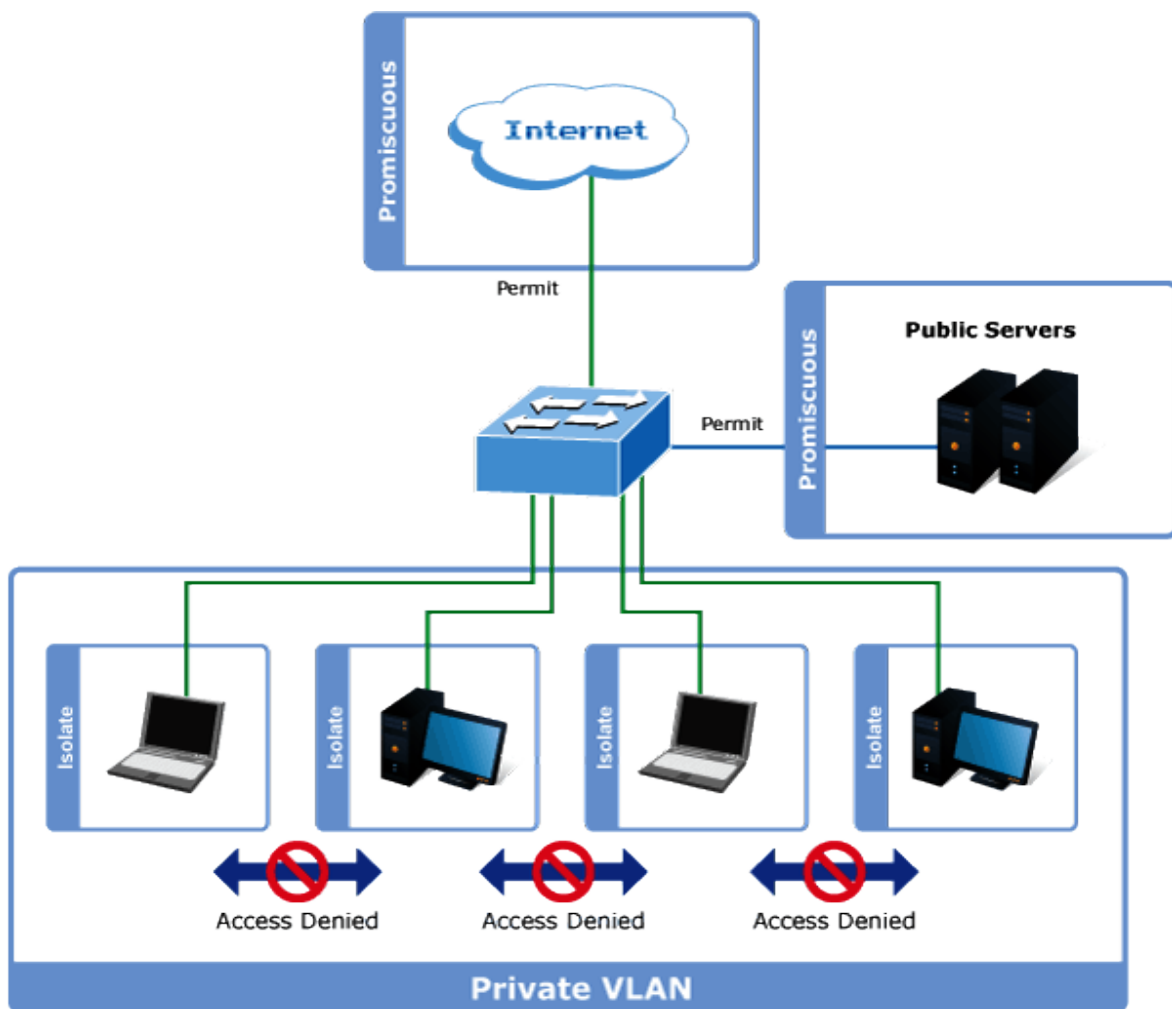
Object	Description
• Port Name	Displays the port for error disabled status.
• Error Disabled Reason	Display the error disabled reason of the port.
• Time Left (Seconds)	Display the time left in seconds.

4.3.8 Protected Ports

Overview

When a switch port is configured to be a member of **protected group** (also called **Private VLAN**), communication between protected ports within that group can be prevented. Two application examples are provided in this section:

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



For protected port group to be applied, the Managed switch must first be configured for standard VLAN operation. Ports in a protected port group fall into one of these two groups:

- **Promiscuous (Unprotected) ports**
 - Ports from which traffic can be forwarded to all ports in the private VLAN
 - Ports which can receive traffic from all ports in the private VLAN
- **Isolated (Protected) ports**
 - Ports from which traffic can only be forwarded to promiscuous ports in the private VLAN

— Ports which can receive traffic from only promiscuous ports in the private VLAN

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

The port settings relate to the currently unit, as reflected by the page header. The Port Isolation Configuration screens in [Figure 4-3-16](#) and [Figure 4-3-17](#) appear.

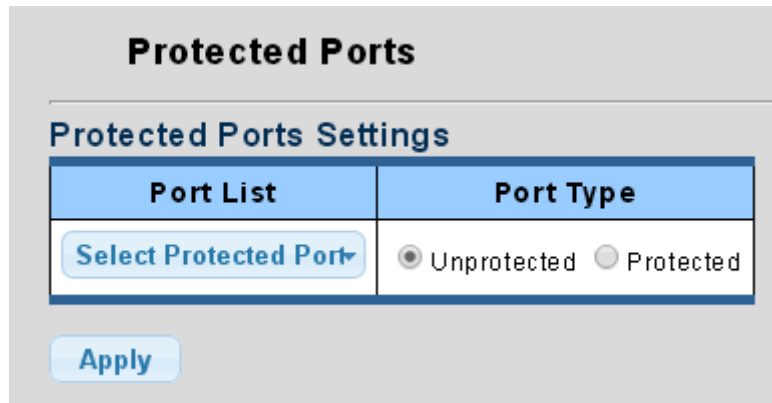



Figure 4-3-16: Protected Ports Settings Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port List 	Select port number for this drop down list.
<ul style="list-style-type: none"> • Port Type 	Displays protected port types. <ul style="list-style-type: none"> - Protected: A single stand-alone VLAN that contains one promiscuous port and one or more isolated (or host) ports. This VLAN conveys traffic between the isolated ports and a lone promiscuous port. - Unprotected: A promiscuous port can communicate with all the interfaces within a private VLAN. This is the default setting.

Button

: Click to apply changes.

Protected Ports Status	
Protected Type	Port List
Protected Ports	
Unprotected Ports	All

Figure 4-3-17: Protect Ports Status Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Protected Ports 	Display the current protected ports.
<ul style="list-style-type: none"> Unprotected Ports 	Display the current unprotected ports.

4.3.9 EEE

What is EEE

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol. EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode. For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for. The EEE port settings relate to the currently unit, as reflected by the page header.

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

The EEE Port Settings screens in [Figure 4-3-18](#) and [Figure 4-3-19](#) appear.

EEE Setup

EEE Port Settings


Port	Enable
<input type="text" value="Select Ports"/>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

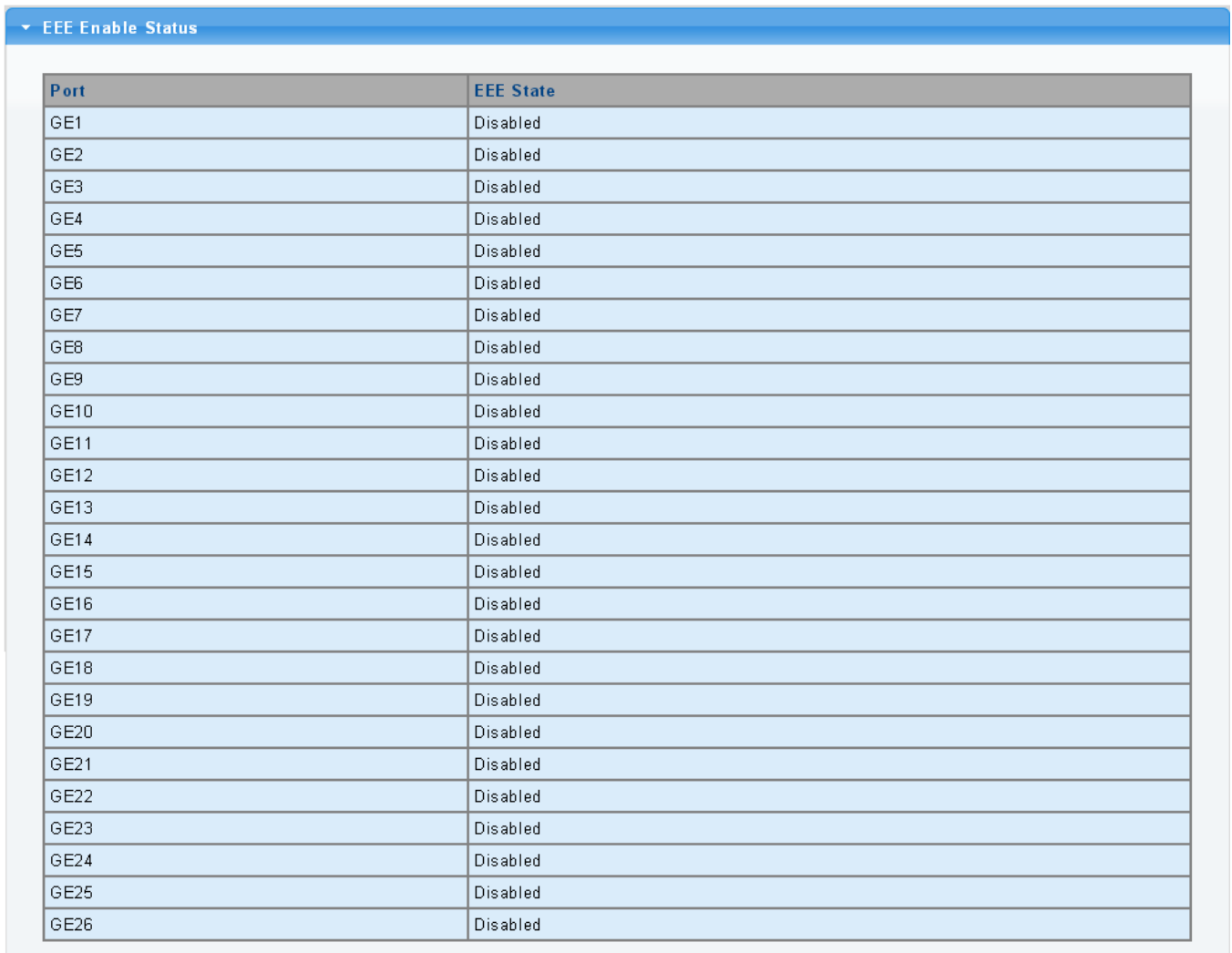
Figure 4-3-18: EEE Port Settings Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	Select port number for this drop down list.
<ul style="list-style-type: none"> • Enable 	Enable or disable the EEE function.

Button

: Click to apply changes.



The screenshot shows a page titled "EEE Enable Status" with a table listing 26 ports (GE1 to GE26) and their corresponding EEE State, which is "Disabled" for all.

Port	EEE State
GE1	Disabled
GE2	Disabled
GE3	Disabled
GE4	Disabled
GE5	Disabled
GE6	Disabled
GE7	Disabled
GE8	Disabled
GE9	Disabled
GE10	Disabled
GE11	Disabled
GE12	Disabled
GE13	Disabled
GE14	Disabled
GE15	Disabled
GE16	Disabled
GE17	Disabled
GE18	Disabled
GE19	Disabled
GE20	Disabled
GE21	Disabled
GE22	Disabled
GE23	Disabled
GE24	Disabled
GE25	Disabled
GE26	Disabled

Figure 4-3-19: EEE Enable Status Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	The switch port number of the logical port.
<ul style="list-style-type: none"> • EEE State 	Display the current EEE state.

4.4 Link Aggregation

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

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

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

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

The device supports the following Aggregation links :

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

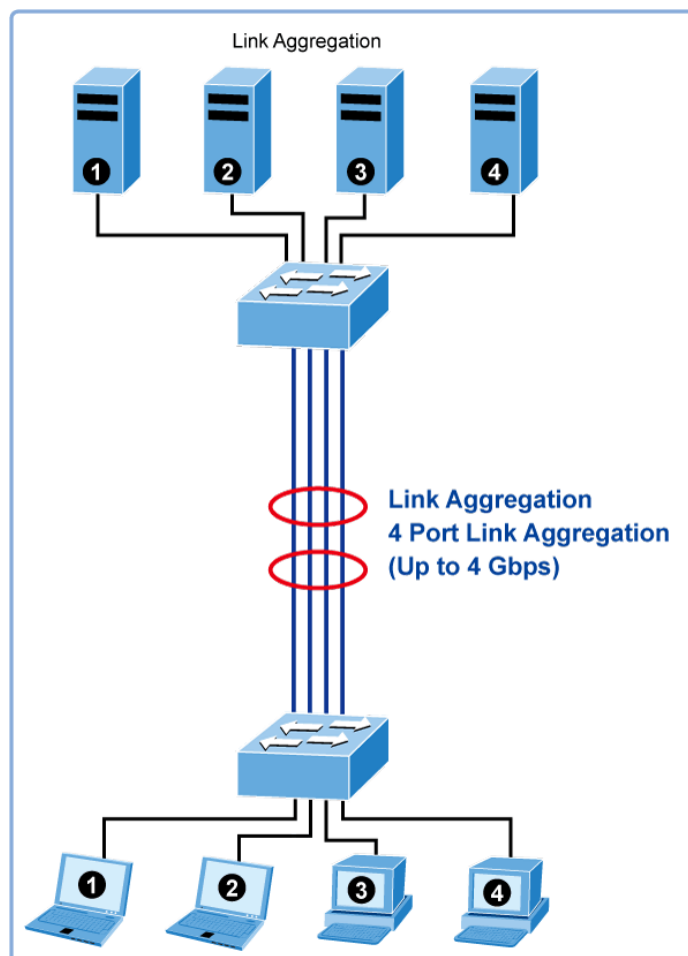


Figure 4-4-1: Link Aggregation

The **Link Aggregation Control Protocol (LACP)** provides a standardized means for exchanging information between Partner Systems that require high speed redundant links. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode, more detail information refer to the IEEE 802.3ad standard.

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation lets you group up to 8 consecutive ports into a single dedicated connection between any two the Switch or other Layer 2 switches. However, before making any physical connections between devices, use the Link aggregation Configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

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

It allows a maximum of 8 ports to be aggregated at the same time. The Managed Switch support Gigabit Ethernet ports (up to 8 groups). If the group is defined as a LACP static link aggregating group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregating group, then the number of ports must be the same as the group member ports.

Use the Link Aggregation Menu to display or configure the Trunk function. This section has the following items:

- | | |
|----------------------------|---|
| ■ LAG Setting | Configures load balance algorithm configuration settings. |
| ■ LAG Management | Configures LAG configuration settings. |
| ■ LAG Port Setting | Configures LAG port settings. |
| ■ LACP Setting | Configures LACP priority settings. |
| ■ LACP Port Setting | Configure LACP configuration settings. |
| ■ LAG Status | Display LAG status / LACP information. |

4.4.1 LAG Setting

This page allows configuring load balance algorithm configuration settings. The LAG Setting screens in [Figure 4-4-2](#) and [Figure 4-4-3](#) appear.

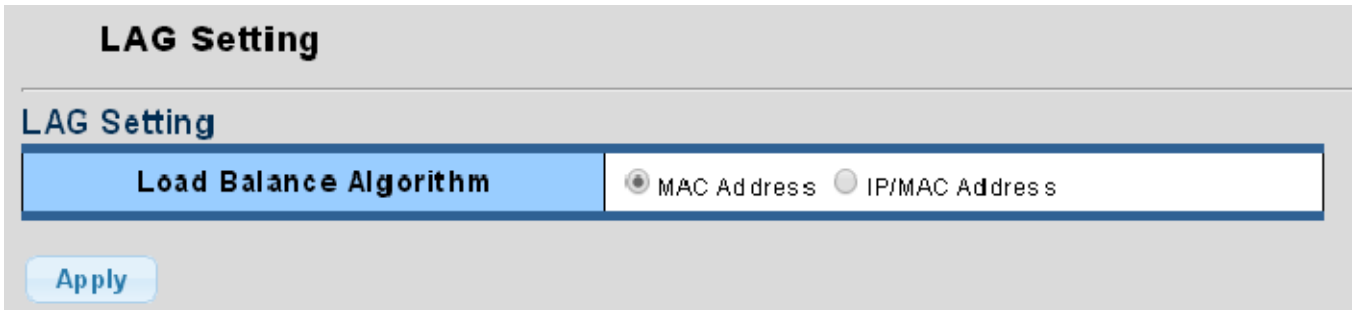



Figure 4-4-2: LAG Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Load Balance Algorithm 	Select load balance algorithm mode: <ul style="list-style-type: none"> ■ MAC Address: The MAC address can be used to calculate the port for the frame. ■ IP/MAC Address: The IP and MAC address can be used to calculate the port for the frame.

Button

: Click to apply changes.

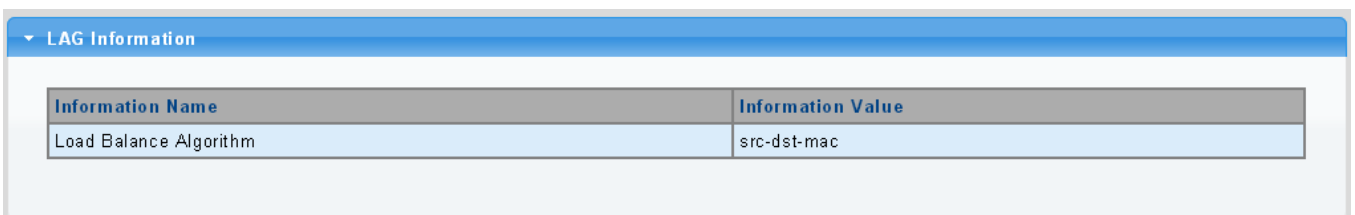


Figure 4-4-3: LAG Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Load Balance Algorithm 	Display the current load balance algorithm.

4.4.2 LAG Management

This page is used to configure the LAG management. The LAG Management screens in Figure 4-4-4 and Figure 4-4-5 appear.

Figure 4-4-4: LAG Management Page Screenshot


The page includes the following fields:

Object	Description
• LAG	Select LAG number for this drop down list, the available range is 1 to 8.
• Name	Indicates per LAG name and the available range are 32 characters.
• Type	Indicates the trunk type. Static : Force aggregated selected ports to be a trunk group. LACP : LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.
• Ports	Select port number for this drop down list to establish Link Aggregation. The available range is 8 ports.

LAG	Name	Type	Link State	Active Member	Standby Member	Modify
LAG1		---	Not Present	-	-	Edit
LAG2		---	Not Present	-	-	Edit
LAG3		---	Not Present	-	-	Edit
LAG4		---	Not Present	-	-	Edit
LAG5		---	Not Present	-	-	Edit
LAG6		---	Not Present	-	-	Edit
LAG7		---	Not Present	-	-	Edit
LAG8		---	Not Present	-	-	Edit

Figure 4-4-5: LAG Management Information Page Screenshot

The page includes the following fields:

Object	Description
• LAG	The LAG for the settings contained in the same row.
• Name	Display the current name.
• Type	Display the current type.
• Link State	Display the link state.
• Active Member	Display the active member.
• Standby Member	Display the standby member.
• Modify	Click  to modify LAG configuraiton.

4.4.3 LAG Port Setting

This page allows setting configuration for per LAG. The LAG Port setting screens in [Figure 4-4-6](#) and [Figure 4-4-7](#) appear.

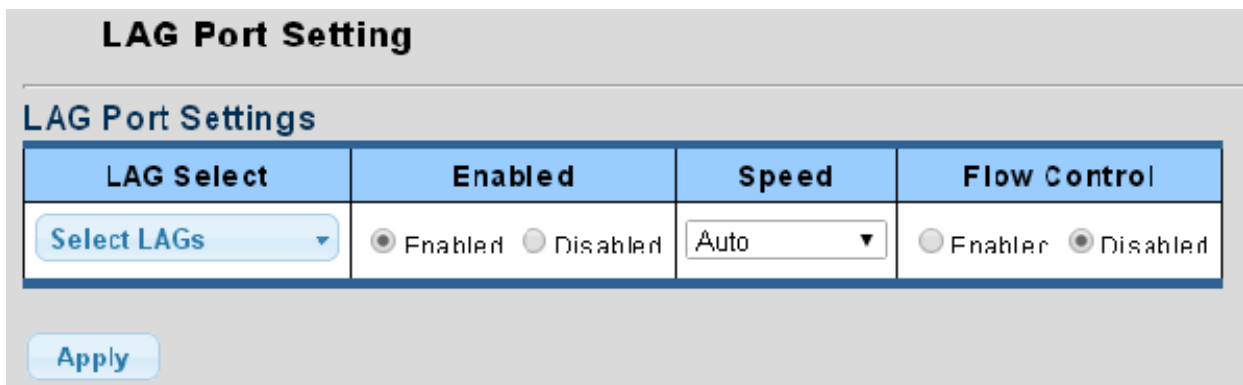


Figure 4-4-6: LAG Port Setting Information Page Screenshot

The page includes the following fields:

Object	Description
• LAG Select	Select LAG number for this drop down list.
• Enabled	Indicates the LAG Port Setting operation. Possible state are: Enabled - Start up the LAG manually. Disabled - Shutdown the LAG manually.
• Speed	Select any available link speed for the given switch port. Draw the menu bar to select the mode. <ul style="list-style-type: none"> ■ Auto - Setup Auto negotiation. ■ Auto-10M - Setup 10M Auto negotiation. ■ Auto-100M - Setup 100M Auto negotiation. ■ Auto-1000M - Setup 1000M Auto negotiation.

	<ul style="list-style-type: none"> ■ Auto-10/100M - Setup 10/100M Auto negotiation. ■ 10M - Setup 10M Force mode. ■ 100M - Setup 100M Force mode. ■ 1000M - Setup 1000M Force mode.
<ul style="list-style-type: none"> • Flow Control 	<p>When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner.</p> <p>When a fixed-speed setting is selected, that is what is used.</p> <p>Current Rx column indicates whether pause frames on the port are obeyed.</p> <p>Current Tx column indicates whether pause frames on the port are transmitted.</p> <p>The Rx and Tx settings are determined by the result of the last Auto-Negotiation.</p> <p>Check the configured column to use flow control.</p> <p>This setting is related to the setting for Configured Link Speed.</p> <p>Possible state are:</p> <p>Enabled - Start up the Flow Control manually.</p> <p>Disabled - Shutdown the Flow Control manually.</p>

Button



: Click to apply changes.

LAG Port Status

LAG	Description	Port Type	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
LAG1			Enabled		Auto	Auto	Disabled	Disabled
LAG2			Enabled		Auto	Auto	Disabled	Disabled
LAG3			Enabled		Auto	Auto	Disabled	Disabled
LAG4			Enabled		Auto	Auto	Disabled	Disabled
LAG5			Enabled		Auto	Auto	Disabled	Disabled
LAG6			Enabled		Auto	Auto	Disabled	Disabled
LAG7			Enabled		Auto	Auto	Disabled	Disabled
LAG8			Enabled		Auto	Auto	Disabled	Disabled

Figure 4-4-7: LAG Port Status Page Screenshot

The page includes the following fields:

Object	Description
• LAG	The LAG for the settings contained in the same row.
• Description	Display the current description.
• Port Type	Display the current port type.
• Enable State	Display the current enable state.
• Link Status	Display the link status of per LAG group.

• Speed	Display the current speed.
• Duplex	Display the current duplex mode.
• Flow Control Config	Display the current flow control configuration.
• Flow Control Status	Display the current flow control status.

4.4.4 LACP Setting

This page is used to configure the LACP system priority setting. The LACP Setting screens in [Figure 4-4-8](#) and [Figure 4-4-9](#) appear.

Figure 4-4-8: LACP Setting Page Screenshot

The page includes the following fields:

Object	Description
• LACP Enable	Disable or enable LACP function.
• System Priority	A value which is used to identify the active LACP. The Managed Switch with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group. The available options are 1 to 65535.

Button

Apply: Click to apply changes.

Information Name	Information Value
State	Disabled
System Priority	1

Figure 4-4-9: LACP Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • State 	Display the current LACP disable / enable status.
<ul style="list-style-type: none"> • System Priority 	Display the current system priority.

4.4.5 LACP Port Setting

This page is used to configure the LACP port setting. The LACP Port Setting screens in [Figure 4-4-10](#) and [Figure 4-4-11](#) appear.

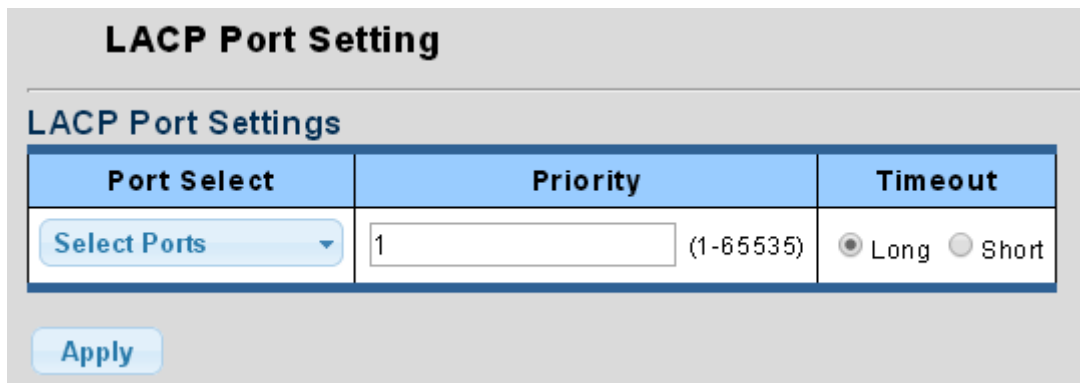


Figure 4-4-10: LACP Port Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port Select 	Select port number for this drop down list to set LACP port setting.
<ul style="list-style-type: none"> • Priority 	<p>The Prio controls the priority of the port.</p> <p>If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role.</p> <p>Lower number means greater priority.</p>
<ul style="list-style-type: none"> • Timeout 	<p>The Timeout controls the period between BPDU transmissions.</p> <p>Short will transmit LACP packets each second, while Long will wait for 30 seconds before sending a LACP packet.</p>

Button

: Click to apply changes.

LACP Port Information		
Port Name	Priority	Timeout
GE1	1	Long
GE2	1	Long
GE3	1	Long
GE4	1	Long
GE5	1	Long
GE6	1	Long
GE7	1	Long
GE8	1	Long
GE9	1	Long
GE10	1	Long
GE11	1	Long
GE12	1	Long
GE13	1	Long
GE14	1	Long
GE15	1	Long
GE16	1	Long
GE17	1	Long
GE18	1	Long
GE19	1	Long
GE20	1	Long
GE21	1	Long
GE22	1	Long
GE23	1	Long
GE24	1	Long
GE25	1	Long
GE26	1	Long

Figure 4-4-11: LACP Port Information Page Screenshot

The page includes the following fields:

Object	Description
• Port Name	The switch port number of the logical port.
• Priority	Display the current LACP priority parameter.
• Timeout	Display the current timeout parameter.

4.4.6 LAG Status

This page displays LAG status. The LAG Status screens in [Figure 4-4-12](#) and [Figure 4-4-13](#) appear.

LAG Status					
LAG Status					
LAG	Name	Type	Link State	Active Member	Standby Member
LAG1		---	Not Present	-	-
LAG2		---	Not Present	-	-
LAG3		---	Not Present	-	-
LAG4		---	Not Present	-	-
LAG5		---	Not Present	-	-
LAG6		---	Not Present	-	-
LAG7		---	Not Present	-	-
LAG8		---	Not Present	-	-

Figure 4-4-12: LAG Status Page Screenshot

The page includes the following fields:

Object	Description
• LAG	Display the current trunk entry.
• Name	Display the current LAG name.
• Type	Display the current trunk type.
• Link State	Display the current link state.
• Active Member	Display the current active member.
• Standby Member	Display the current standby member.

LAG	Port	PartnerSysId	PnKey	AtKey	Sel	Mux	Receiv	PrdTx	AtState	PnState
LAG1	GE1	000000000000	03e8	03e8	U	DETACH	DFLT	FstPRD	A_G__F_	_TG_C_F_
LAG1	GE2	000000000000	03e8	03e8	U	DETACH	DFLT	FstPRD	A_G__F_	_TG_C_F_

Figure 4-4-13: LACP Information Page Screenshot

The page includes the following fields:

Object	Description
• LAG	Display the current LAG ID.
• Port	Display the current port number.
• PartnerSysId	The system ID of link partner. This field would be updated when the port receives LACP PDU from link partner.
• PnKey	Port key of partner. This field would be updated when the port receives LACP PDU from link partner.
• AtKey	Port key of actor. The key is designed to be the same as trunk ID.
• Sel	LACP selection logic status of the port. <ul style="list-style-type: none"> ■ “S” means selected ■ “U” means unselected ■ “D” means standby
• Mux	LACP mux state machine status of the port. <ul style="list-style-type: none"> ■ “DETACH” means the port is in detached state ■ “WAIT” means waiting state ■ “ATTACH” means attach state ■ “CLLCT” means collecting state ■ “DSTRBT” means distributing state
• Receiv	LACP receive state machine status of the port. <ul style="list-style-type: none"> ■ “INIT” means the port is in initialize state ■ “PORTds” means port disabled state ■ “EXPR” means expired state ■ “LACPs” means LACP disabled state

	<ul style="list-style-type: none"> ■ "DFLT" means defaulted state ■ "CRRNT" means current state.
<ul style="list-style-type: none"> • PrdTx 	<p>LACP periodic transmission state machine status of the port.</p> <ul style="list-style-type: none"> ■ "no PRD" means the port is in no periodic state ■ "FstPRD" means fast periodic state ■ "SlwPRD" means slow periodic state ■ "PrdTX" means periodic TX state
<ul style="list-style-type: none"> • AtState 	<p>The actor state field of LACP PDU description.</p> <p>The field from left to right describes: "LACP_Activity", "LACP_Timeout", "Aggregation", "Synchronization", "Collecting", "Distributing", "Defaulted", and "Expired".</p> <p>The contents could be true or false. If the contents are false, the web shows "_"; if the contents are true, the web shows "A", "T", "G", "S", "C", "D", "F" and "E" for each content respectively.</p>
<ul style="list-style-type: none"> • PnState 	<p>The partner state field of LACP PDU description.</p> <p>The field from left to right describes: "LACP_Activity", "LACP_Timeout", "Aggregation", "Synchronization", "Collecting", "Distributing", "Defaulted", and "Expired".</p> <p>The contents could be true or false. If the contents are false, the web shows "_"; if the contents are true, the web shows "A", "T", "G", "S", "C", "D", "F" and "E" for each content respectively.</p>

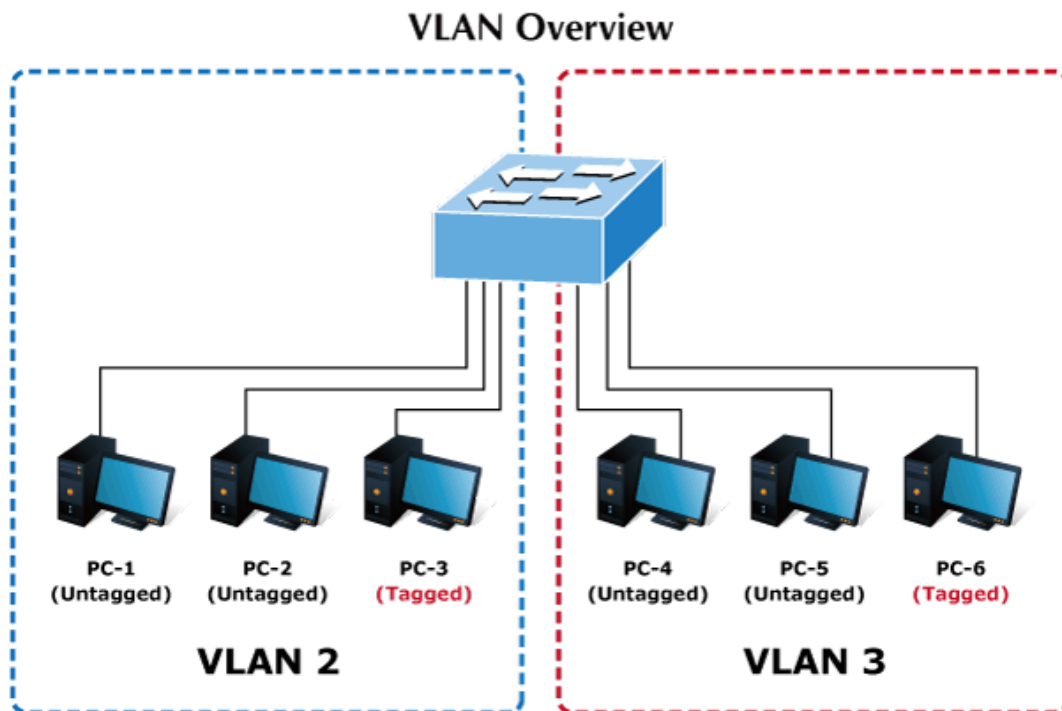
4.5 VLAN

4.5.1 VLAN Overview

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

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

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



1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
2. The Managed Switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.
3. The Managed Switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLAN is created, the member ports assigned to the new VLAN will be removed from the DEFAULT_VLAN port member list. The DEFAULT_VLAN has a VID = 1.



This section has the following items:

- | | |
|--------------------------------------|--|
| ■ Management VLAN | Configures the management VLAN. |
| ■ Create VLAN | Creates the VLAN group. |
| ■ Interface Settings | Configures mode and PVID on the VLAN port. |
| ■ Port to VLAN | Configures the VLAN membership. |
| ■ Port VLAN Membership | Display the VLAN membership. |
| ■ Protocol VLAN Group Setting | Configures the protocol VLAN group. |
| ■ Protocol VLAN Port Setting | Configures the protocol VLAN port setting. |
| ■ GVRP Setting | Configures GVRP global setting. |
| ■ GVRP Port Setting | Configures GVRP port setting. |
| ■ GVRP VLAN | Display the GVRP VLAN database. |
| ■ GVRP Statistics | Display the GVRP port statistics. |

4.5.2 IEEE 802.1Q VLAN

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

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

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

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

This Managed Switch supports the following VLAN features:

- Up to 256 VLANs based on the IEEE 802.1Q standard
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices

■ 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:

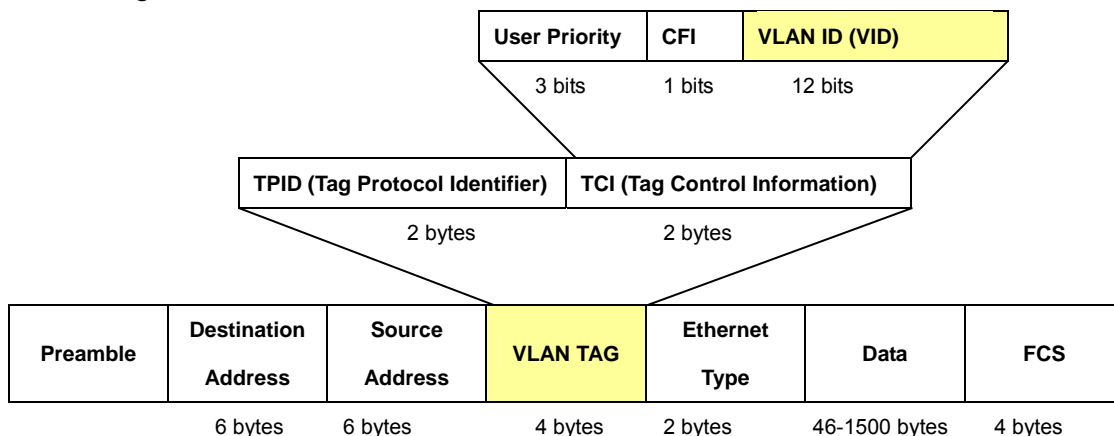
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

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

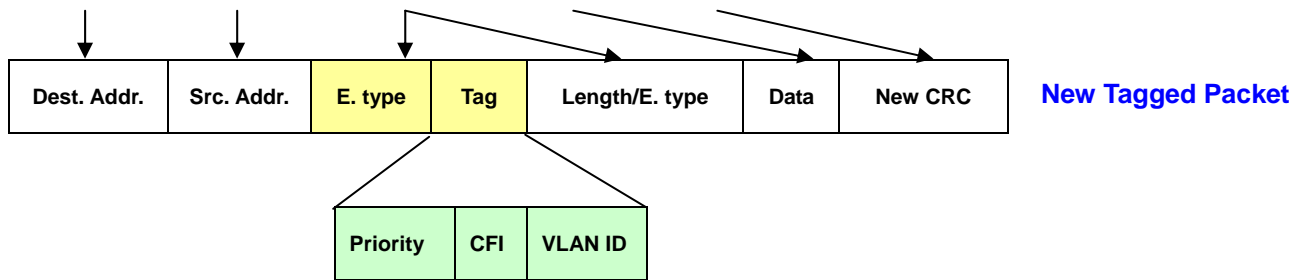


The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q Tag

Dest. Addr.	Src. Addr.	Length/E. type	Data	Old CRC
-------------	------------	----------------	------	---------

Original Ethernet



■ Port VLAN ID

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

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

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

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

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

■ Default VLANs

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

■ Assigning Ports to VLANs

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



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

■ VLAN Classification

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

■ Port Overlapping

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

■ Untagged VLANs

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

4.5.3 Management VLAN

Configure Management VLAN on this page. The screens in [Figure 4-5-1](#) and [Figure 4-5-2](#) appear.

Figure 4-5-1: Management VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
• Management VLAN	Provide the managed VLAN ID.

Button

: Click to apply changes.

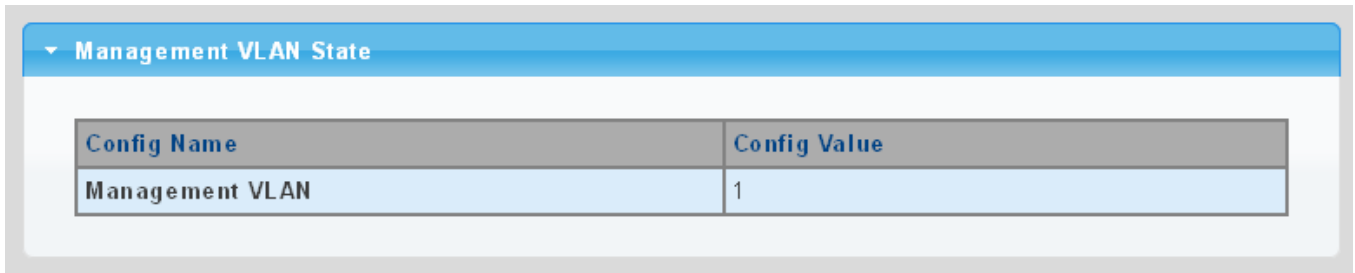


Figure 4-5-2: Management VLAN State Page Screenshot

The page includes the following fields:

Object	Description
• Management VLAN	Display the current management VLAN.

4.5.4 Create VLAN

Create/delete VLAN on this page. The screens in Figure 4-5-3 and Figure 4-5-4 appear.

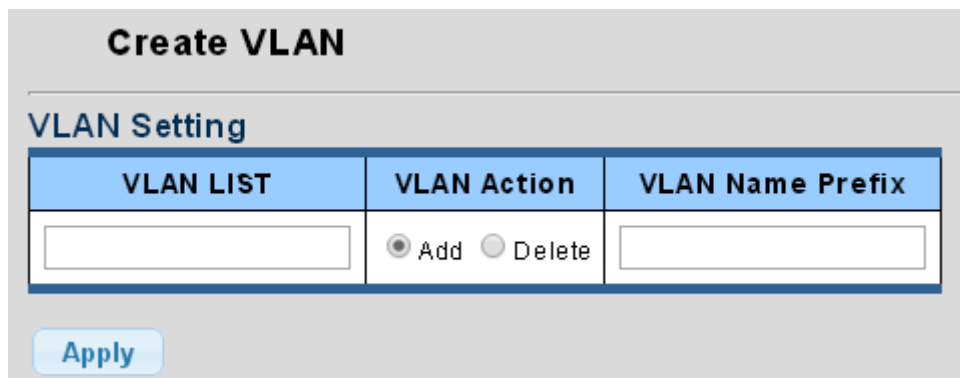


Figure 4-5-3: VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
• VLAN List	Indicates the ID of this particular VLAN.
• VLAN Action	This column allowed users to add or delete VLAN s.
• VLAN Name Prefix	Indicates the name of this particular VLAN, the options are 28 characters.

Button



: Click to apply changes.

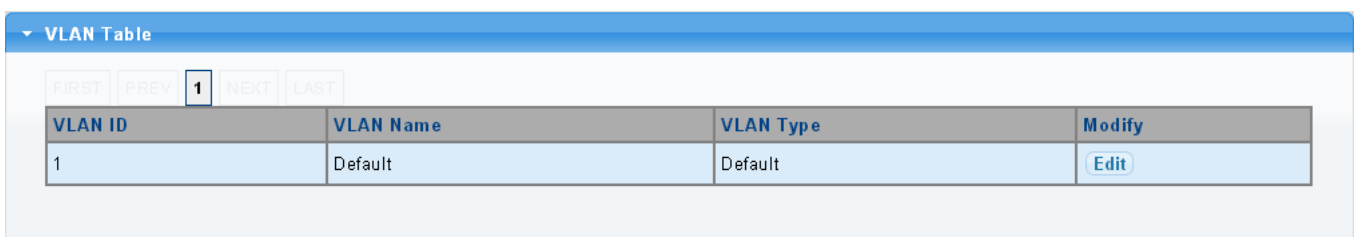



Figure 4-5-4: VLAN Table Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VLAN ID entry.
• VLAN Name	Display the current VLAN ID name.
• VLAN Type	Display the current VLAN ID type.
• Modify	Click  to modify VLAN configuraiton.

4.5.5 Interface Settings

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

Understand nomenclature of the Switch

■ IEEE 802.1Q Tagged and Untagged

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

- **Tagged:** Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.
- **Untagged:** Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

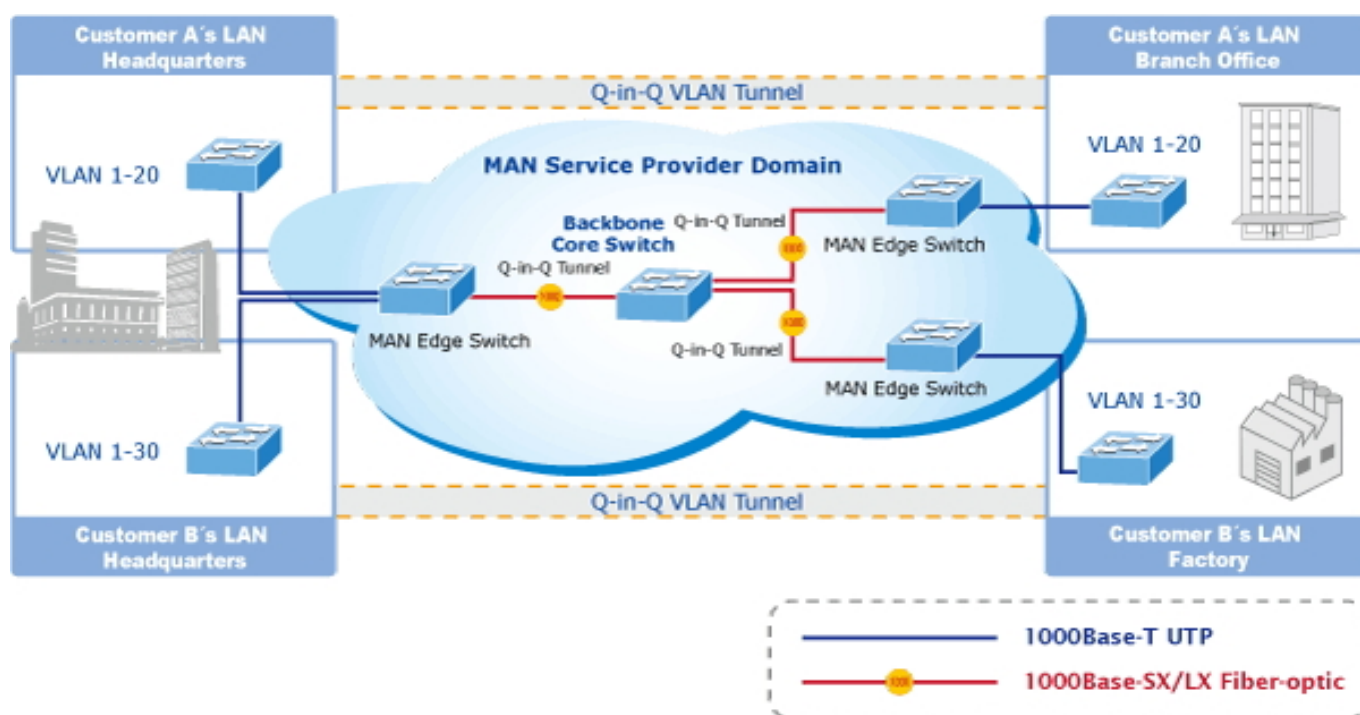
Frame Income / Frame Leave	Income Frame is tagged	Income Frame is untagged
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remain untagged

Table 4-5-1: Ingress / Egress Port with VLAN VID Tag / Untag Table

■ IEEE 802.1Q Tunneling (Q-in-Q)

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

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



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

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

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

Edit Interface Setting

The Edit Interface Setting/Status screens in [Figure 4-5-5](#) & [Figure 4-5-6](#) appear.

Figure 4-5-5: Edit Interface Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port Select 	Select port number for this drop down list to set VLAN port setting.
<ul style="list-style-type: none"> • Interface VLAN Mode 	<p>Set the port in hybrid, access, trunk, tunnel mode.</p> <ul style="list-style-type: none"> ■ Hybrid means the port allows the traffic of multi-VLANs to pass with tag or untag mode. ■ Access indicates the port belongs to one VLAN only. ■ Trunk means the port allows traffic of multiple VLAN. ■ Tunnel configures IEEE 802.1Q tunneling for a downlink port to another device within the customer network.
<ul style="list-style-type: none"> • PVID 	<p>Allow assign PVID for selected port.</p> <p>The PVID will be inserted into all untagged frames entering the ingress port. The PVID must as same as the VLAN ID that the port belong to VLAN group, or the untagged traffic will be dropped.</p> <p>The range for the PVID is 1-4094.</p>
<ul style="list-style-type: none"> • Accepted Type 	<p>Determines whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded.</p> <p>Options:</p> <ul style="list-style-type: none"> ■ All ■ Tag Only ■ Untag Only <p>By default, the field is set to All.</p>
<ul style="list-style-type: none"> • Ingress Filtering 	<ul style="list-style-type: none"> • If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. • If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. <p>However, the port will never transmit frames classified to VLANs that it is not a member of.</p>

• Uplink	Enable/disable uplink function in trunk port.
• TPID	Configure the type (TPID) of the protocol of switch trunk port.

Button


: Click to apply changes.

Port VLAN Status						
Port	Interface VLAN Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
GE1	Trunk	1	ALL	Enabled	Disabled	0x8100
GE2	Trunk	1	ALL	Enabled	Disabled	0x8100
GE3	Trunk	1	ALL	Enabled	Disabled	0x8100
GE4	Trunk	1	ALL	Enabled	Disabled	0x8100
GE5	Trunk	1	ALL	Enabled	Disabled	0x8100
GE6	Trunk	1	ALL	Enabled	Disabled	0x8100
GE7	Trunk	1	ALL	Enabled	Disabled	0x8100
GE8	Trunk	1	ALL	Enabled	Disabled	0x8100
GE9	Trunk	1	ALL	Enabled	Disabled	0x8100
GE10	Trunk	1	ALL	Enabled	Disabled	0x8100
GE11	Trunk	1	ALL	Enabled	Disabled	0x8100
GE12	Trunk	1	ALL	Enabled	Disabled	0x8100
GE13	Trunk	1	ALL	Enabled	Disabled	0x8100
GE14	Trunk	1	ALL	Enabled	Disabled	0x8100
GE15	Trunk	1	ALL	Enabled	Disabled	0x8100
GE16	Trunk	1	ALL	Enabled	Disabled	0x8100
GE17	Trunk	1	ALL	Enabled	Disabled	0x8100
GE18	Trunk	1	ALL	Enabled	Disabled	0x8100
GE19	Trunk	1	ALL	Enabled	Disabled	0x8100
GE20	Trunk	1	ALL	Enabled	Disabled	0x8100
GE21	Trunk	1	ALL	Enabled	Disabled	0x8100
GE22	Trunk	1	ALL	Enabled	Disabled	0x8100
GE23	Trunk	1	ALL	Enabled	Disabled	0x8100
GE24	Trunk	1	ALL	Enabled	Disabled	0x8100
GE25	Trunk	1	ALL	Enabled	Disabled	0x8100
GE26	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG1	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG2	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG3	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG4	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG5	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG6	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG7	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG8	Trunk	1	ALL	Enabled	Disabled	0x8100

Figure 4-5-6: Edit Interface Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Interface VLAN Mode	Display the current interface VLAN mode.
• PVID	Display the current PVID.
• Accepted Frame Type	Display the current access frame type.
• Ingress Filtering	Display the current ingress filtering.
• Uplink	Display the current uplink mode.
• TPID	Display the current TPID.

4.5.6 Port to VLAN

Use the VLAN Static Table to configure port members for the selected VLAN index. This Page allows for adding and deleting port members of each VLAN. The screen in [Figure 4-5-7](#) appears.

Port to VLAN

Port to VLAN Settings

VLAN ID:

Port	Interface VLAN Mode	Membership	PVID
GE1	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE2	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE3	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE4	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE5	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE6	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE7	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE8	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE9	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE10	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE11	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE12	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE13	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE14	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE15	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE16	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE17	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE18	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE19	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE20	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE21	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE22	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE23	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE24	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE25	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE26	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
LAG1	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
LAG2	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
LAG3	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
LAG4	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
LAG5	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
LAG6	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
LAG7	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
LAG8	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>

Figure 4-5-7: Port to VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Select VLAN ID for this drop down list to assign VLAN membership.
• Port	The switch port number of the logical port.
• Interface VLAN Mode	Display the current interface VLAN mode.
• Membership	Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
	Forbidden: Interface is forbidden from automatically joining the VLAN via GVRP.
	Excluded: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
	Tagged: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
	Untagged: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
• PVID	Display the current PVID

Button



: Click to apply changes.

4.5.7 Port VLAN Membership

This Page provides an overview of membership status for VLAN users. The VLAN Membership Status screen in [Figure 4-5-8](#) appears.

Port VLAN Membership				
- Port VLAN Membership Table				
Port	Mode	Administrative VLANs	Operational VLANs	Modify
GE1	Trunk	1UP	1UP	Edit
GE2	Trunk	1UP	1UP	Edit
GE3	Trunk	1UP	1UP	Edit
GE4	Trunk	1UP	1UP	Edit
GE5	Trunk	1UP	1UP	Edit
GE6	Trunk	1UP	1UP	Edit
GE7	Trunk	1UP	1UP	Edit
GE8	Trunk	1UP	1UP	Edit
GE9	Trunk	1UP	1UP	Edit
GE10	Trunk	1UP	1UP	Edit
GE11	Trunk	1UP	1UP	Edit
GE12	Trunk	1UP	1UP	Edit
GE13	Trunk	1UP	1UP	Edit
GE14	Trunk	1UP	1UP	Edit
GE15	Trunk	1UP	1UP	Edit
GE16	Trunk	1UP	1UP	Edit
GE17	Trunk	1UP	1UP	Edit
GE18	Trunk	1UP	1UP	Edit
GE19	Trunk	1UP	1UP	Edit
GE20	Trunk	1UP	1UP	Edit
GE21	Trunk	1UP	1UP	Edit
GE22	Trunk	1UP	1UP	Edit
GE23	Trunk	1UP	1UP	Edit
GE24	Trunk	1UP	1UP	Edit
GE25	Trunk	1UP	1UP	Edit
GE26	Trunk	1UP	1UP	Edit
LAG1	Trunk	1UP	1UP	Edit
LAG2	Trunk	1UP	1UP	Edit
LAG3	Trunk	1UP	1UP	Edit
LAG4	Trunk	1UP	1UP	Edit
LAG5	Trunk	1UP	1UP	Edit
LAG6	Trunk	1UP	1UP	Edit
LAG7	Trunk	1UP	1UP	Edit
LAG8	Trunk	1UP	1UP	Edit

Figure 4-5-8: Port VLAN Membership Table Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Mode	Display the current VLAN mode.
• Administrative VLANs	Display the current administrative VLANs.
• Operational VLANs	Display the current operational VLANs.
• Modify	Click Edit to modify VLAN membership.

4.5.8 Protocol VLAN Group Setting

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this Managed Switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

Command Usage

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 Protocol VLAN Configuration page.
3. Then map the protocol for each interface to the appropriate VLAN using the Protocol VLAN Port Configuration page.

This Page allows for configures protocol-based VLAN Group Setting. The portocol-based VLAN screens in [Figure 4-5-9](#) & [Figure 4-5-10](#) appear.

Figure 4-5-9: Add Protocol VLAN Group Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Group ID 	Protocol Group ID assigned to the Special Protocol VLAN Group.
<ul style="list-style-type: none"> • Frame Type 	Frame Type can have one of the following values: <ul style="list-style-type: none"> ■ Ethernet II ■ IEEE802.3_LL_C_Other ■ RFC_1042 <p>Note: On changing the Frame type field, valid value of the following text field will</p>

	vary depending on the new frame type you selected.
<ul style="list-style-type: none"> • Protocol Value (0x0600-0xFFFE) 	Valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu. Valid values for frame type ranges from 0x0600-0xfffe

Button

: Click to apply changes.

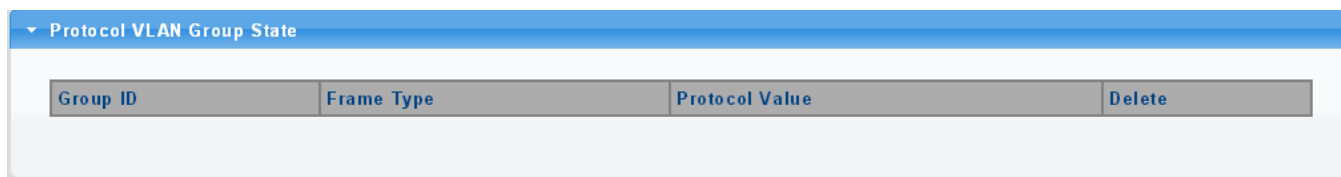



Figure 4-5-10: Protocol VLAN Group State Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Group ID 	Display the current group ID.
<ul style="list-style-type: none"> • Frame Type 	Display the current frame type.
<ul style="list-style-type: none"> • Protocol Value 	Display the current protocol value.
<ul style="list-style-type: none"> • Delete 	Click  to delete the group ID entry.

4.5.9 Protocol VLAN Port Setting

This Page allows you to map a already configured Group Name to a VLAN/port for the switch. The Protocol VLAN Port Setting/State screens in [Figure 4-5-11](#) and [Figure 4-5-12](#) appear.

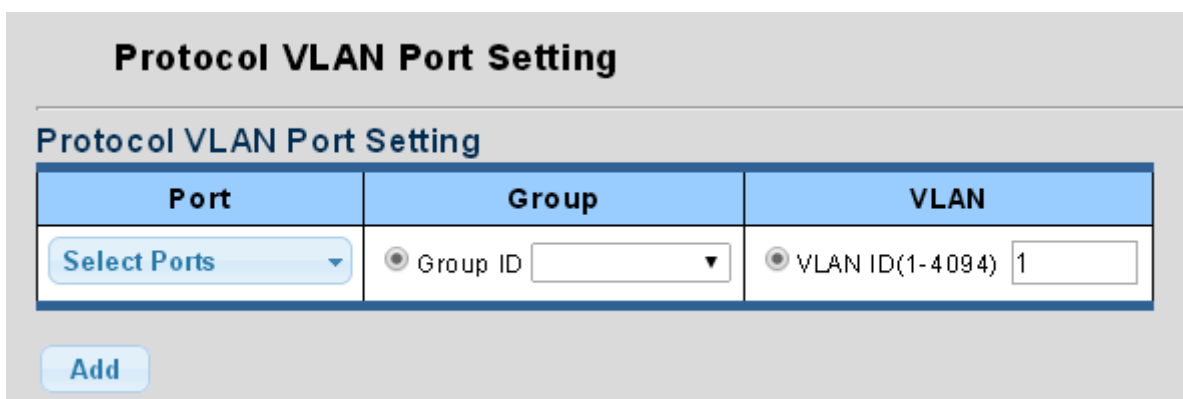



Figure 4-5-11: Protocol VLAN Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port for this drop down list to assign protocol VLAN port.
• Group	Select group ID for this drop down list to protocol VLAN group.
• VLAN	VLAN ID assigned to the Special Protocol VLAN Group.

Button

 : Click to add protocol VLAN port entry.

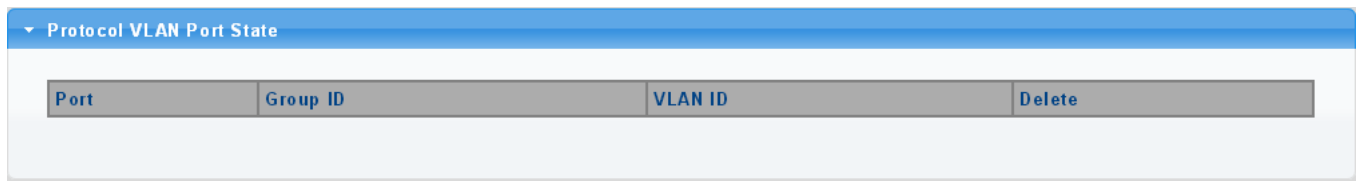


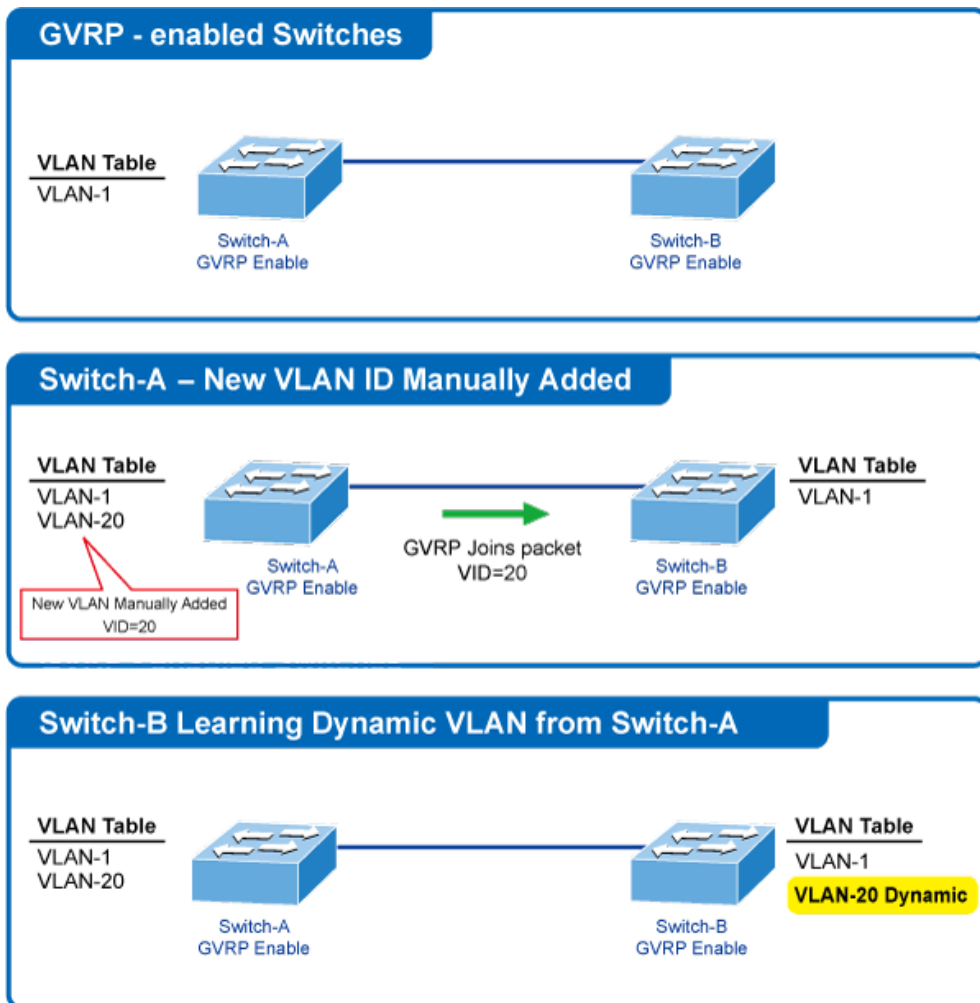
Figure 4-5-12: Protocol VLAN Port State Page Screenshot

The page includes the following fields:

Object	Description
• Port	Display the current port.
• Group ID	Display the current group ID.
• VLAN ID	Display the current VLAN ID.

4.5.10 GVRP Setting

GARP VLAN Registration Protocol (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.

The GVRP Global Setting/Information screens in [Figure 4-5-13](#) and [Figure 4-5-14](#) appear.

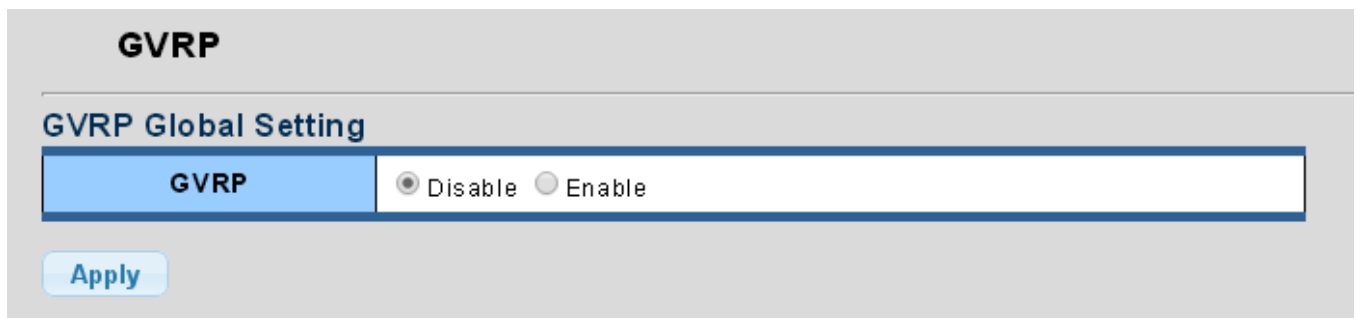


Figure 4-5-13: GVRP Global Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • GVRP 	Controls whether GVRP is enabled or disabled on this Managed Switch.

Button

: Click to apply changes.

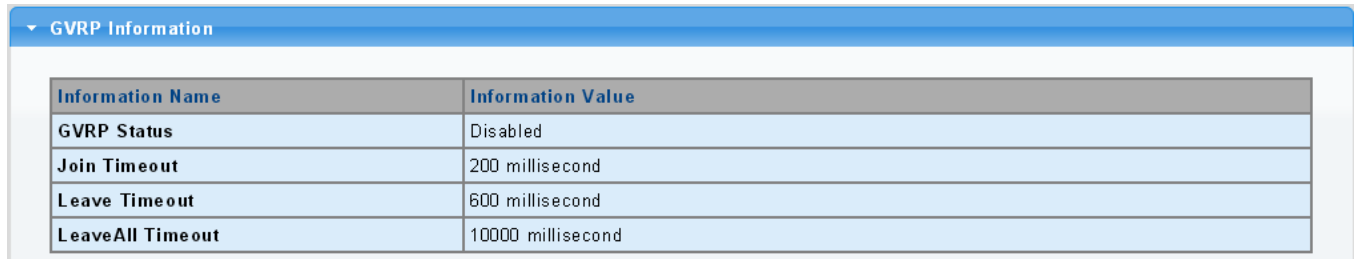


Figure 4-5-14: GVRP Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • GVRP Status 	Display the current GVRP status.
<ul style="list-style-type: none"> • Join Timeout 	Display the current join timeout parameter.
<ul style="list-style-type: none"> • Leave Timeout 	Display the current leave timeout parameter.
<ul style="list-style-type: none"> • LeaveAll Timeout 	Display the current leaveall timeout parameter.

4.5.11 GVRP Port Setting

The GVRP Port Setting/Status screens in [Figure 4-5-15](#) and [Figure 4-5-16](#) appear.

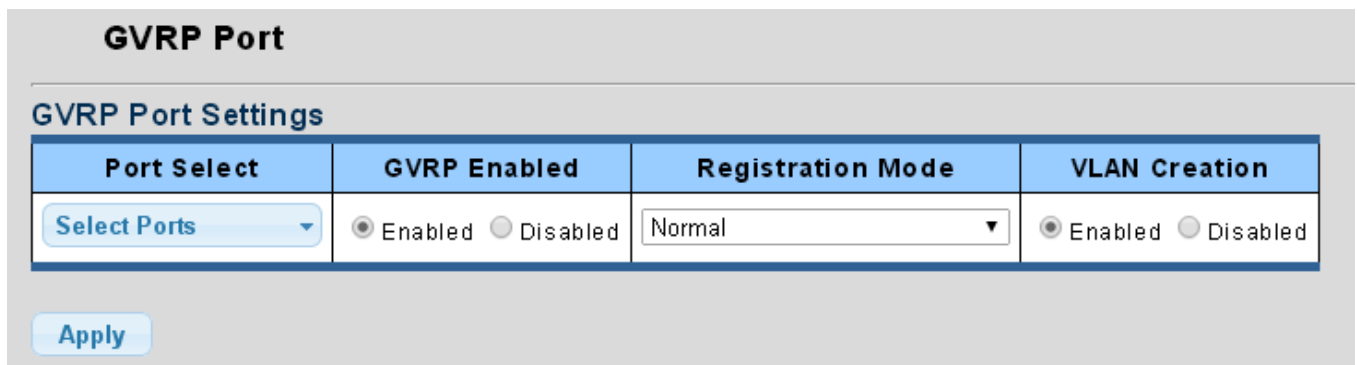


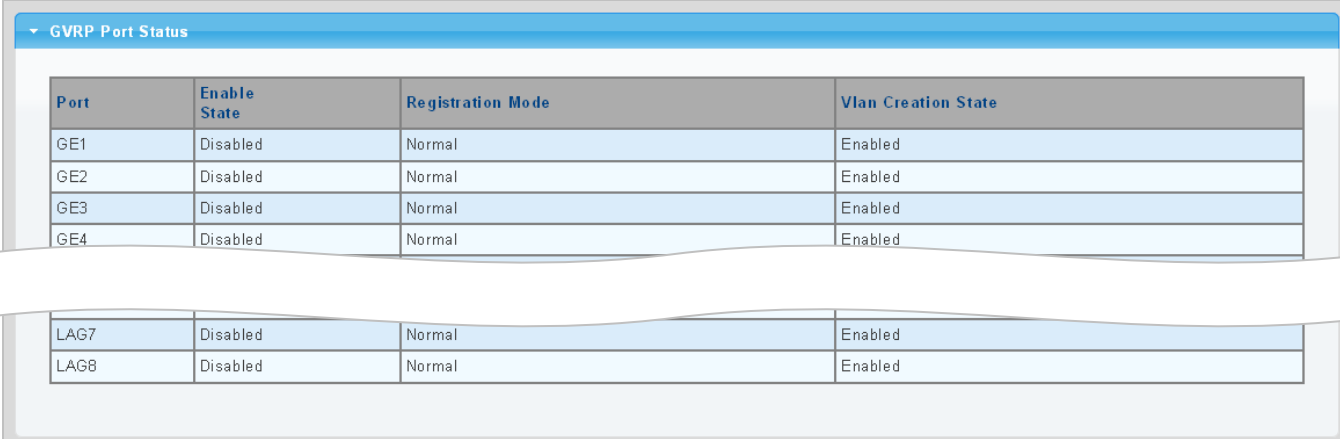
Figure 4-5-15: GVRP Global Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port Select 	Select port for this drop down list to assign protocol VLAN port
<ul style="list-style-type: none"> • GVRP Enabled 	Controls whether GVRP is enabled or disabled on port
<ul style="list-style-type: none"> • Registration Mode 	By default GVRP ports are in Normal registration mode. These ports use GVRP join messages from neighboring switches to prune the VLANs running across the 802.1Q trunk link. If the device on the other side is not capable of sending GVRP messages, or if you do not want to allow the switch to prune any of the VLANs, use the Fixed mode. Fixed mode ports will forward for all VLANs that exist in the switch database. Ports in Forbidden mode forward only for VLAN 1.
<ul style="list-style-type: none"> • VLAN Creation 	GVRP can dynamically create VLANs on switches for trunking purposes. By enabling GVRP dynamic VLAN creation, a switch will add VLANs to its database when it receives GVRP join messages about VLANs it does not have.

Buttons

: Click to apply changes.



Port	Enable State	Registration Mode	Vlan Creation State
GE1	Disabled	Normal	Enabled
GE2	Disabled	Normal	Enabled
GE3	Disabled	Normal	Enabled
GE4	Disabled	Normal	Enabled
LAG7	Disabled	Normal	Enabled
LAG8	Disabled	Normal	Enabled

Figure 4-5-16: GVRP Port Status Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	The switch port number of the logical port.
<ul style="list-style-type: none"> • Enable State 	Display the current GVRP port state.
<ul style="list-style-type: none"> • Registration Mode 	Display the current registration mode.
<ul style="list-style-type: none"> • VLAN Creation State 	Display the current VLAN creation state.

4.5.12 GVRP VLAN

The GVRP VLAN Database screen in [Figure 4-5-17](#) appears.

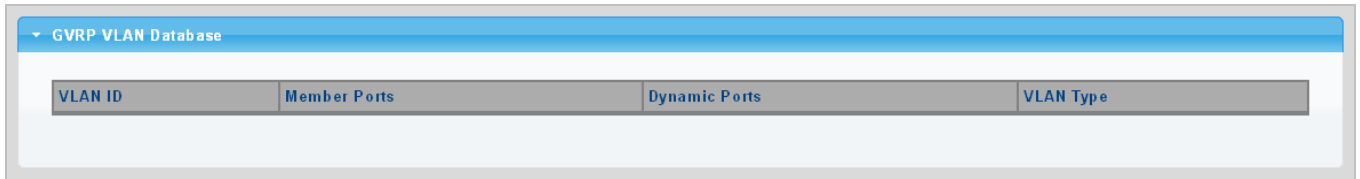


Figure 4-5-17: GVRP VLAN Database Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VLAN ID.
• Member Ports	Display the current member ports.
• Dynamic Ports	Display the current dynamic ports.
• VLAN Type	Display the current VLAN type.

4.5.13 GVRP Statistics

The GVRP Port Statistics and Error Statistics screens in [Figure 4-5-18](#) and [Figure 4-5-19](#) appear.

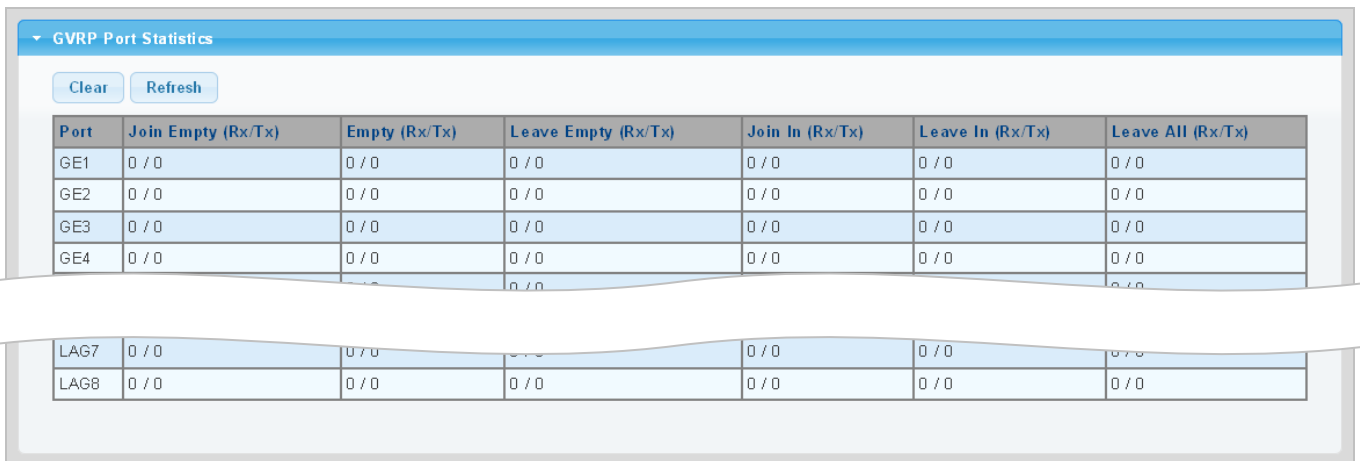


Figure 4-5-18: GVRP Port Statistics Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port
• Join Empty (Rx/Tx)	Display the current join empty (TX/RX) packets
• Empty (Rx/Tx)	Display the current empty (TX/RX) packets

• Leave Empty (Rx/Tx)	Display the current leave empty (TX/RX) packets
• Join In (Rx/Tx)	Display the current join in (TX/RX) packets
• Leave In (Rx/Tx)	Display the current leave in (TX/RX) packets
• LeaveAll (Rx/Tx)	Display the current leaveall (TX/RX) packets

Port	Invalid Protocol ID	Invalid Attribute Type	Invalid Attribute Value	Invalid Attribute Length	Invalid Event
GE1	0	0	0	0	0
GE2	0	0	0	0	0
GE3	0	0	0	0	0
GE4	0	0	0	0	0
LAG6	0	0	0	0	0
LAG7	0	0	0	0	0
LAG8	0	0	0	0	0

Figure 4-5-19: GVRP Port Error Statistics Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Invalid Protocol ID	Display the current invalid protocol ID.
• Invalid Attribute Type	Display the current invalid attribute type.
• Invalid Attribute Value	Display the current invalid attribute value.
• Invalid Attribute Length	Display the current invalid attribute length.
• Invalid Event	Display the current invalid event.

Buttons

Clear: Click to clear the GVRP Error Statistics.

Refresh: Click to refresh the GVRP Error Statistics.

4.5.14 VLAN setting example:

- Separate VLANs
- 802.1Q VLAN Trunk

4.5.14.1 Two separate 802.1Q VLANs

The diagram shows how the Managed Switch handle Tagged and Untagged traffic flow for two VLANs. VLAN Group 2 and VLAN Group 3 are separated VLANs. Each VLAN isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. The screen in [Figure 4-5-20](#) appears and [Table 4-5-2](#) describes the port configuration of the Managed Switches.

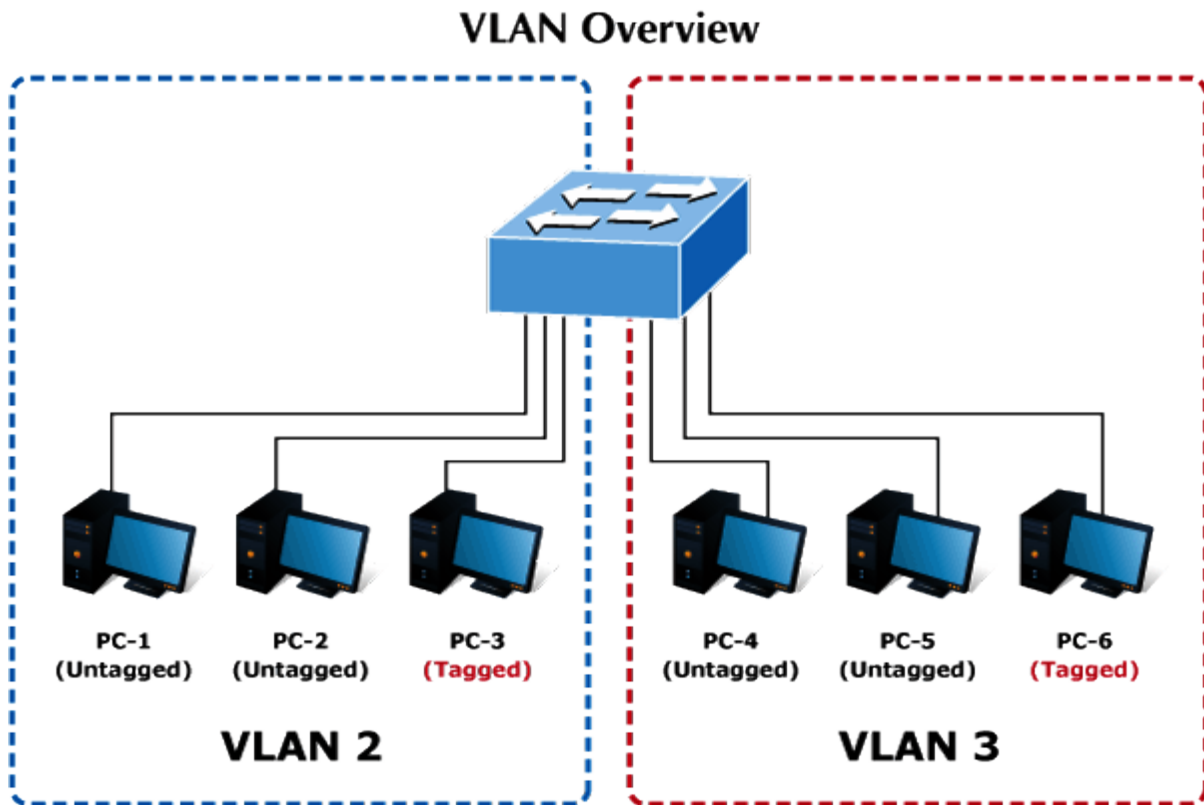


Figure 4-5-20: Two Separate VLAN Diagrams

VLAN Group	VID	Untagged Members	Tagged Members
VLAN Group 1	1	Port-7~Port-8	N/A
VLAN Group 2	2	Port-1,Port-2	Port-3
VLAN Group 3	3	Port-4,Port-5	Port-6

Table 4-5-2: VLAN and Port Configuration

The scenario described as follows:

■ Untagged packet entering VLAN 2

1. While [PC-1] transmit an **untagged** packet enters **Port-1**, the Managed Switch will tag it with a **VLAN Tag=2**. [PC-2] and [PC-3] will received the packet through **Port-2** and **Port-3**.
2. [PC-4],[PC-5] and [PC-6] received no packet.
3. While the packet leaves **Port-2**, it will be stripped away it tag becoming an **untagged** packet.
4. While the packet leaves **Port-3**, it will keep as a **tagged** packet with **VLAN Tag=2**.

■ Tagged packet entering VLAN 2

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

■ Untagged packet entering VLAN 3

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



In this example, VLAN Group 1 is set as default VLAN, but only focuses on VLAN 2 and VLAN 3 traffic flow.

Setup steps

1. Create VLAN Group 2 and 3

Add VLAN group 2 and group 3

VLAN Table		
VLAN ID	VLAN Name	VLAN Type
1	default	Default
2	20002	Static
3	30003	Static

2. Assign VLAN mode and PVID for each port:

Port-1,Port-2 and Port-3 : VLAN Mode = Hybrid, PVID=2

Port-4,Port-5 and Port-6 : VLAN Mode = Hybrid, PVID=3

Port VLAN Status			
Port	Interface VLAN Mode	PVID	Accept Frame Type
GE1	Hybrid	2	ALL
GE2	Hybrid	2	ALL
GE3	Hybrid	2	ALL
GE4	Hybrid	3	ALL
GE5	Hybrid	3	ALL
GE6	Hybrid	3	ALL

3. Assign Tagged/Untagged for each port:

VLAN ID = 2:

Port-1 & 2 = Untagged,

Port-3 = Tagged,

Port -4~6 = Excluded.

Port to VLAN Settings						
VLAN ID : 2						
Port	Interface VLAN Mode	Membership			PVID	
GE1	Hybrid	<input type="radio"/> Forbidden	<input type="radio"/> Excluded	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE2	Hybrid	<input type="radio"/> Forbidden	<input type="radio"/> Excluded	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE3	Hybrid	<input type="radio"/> Forbidden	<input type="radio"/> Excluded	<input checked="" type="radio"/> Tagged	<input type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE4	Hybrid	<input type="radio"/> Forbidden	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>
GE5	Hybrid	<input type="radio"/> Forbidden	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>
GE6	Hybrid	<input type="radio"/> Forbidden	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>

VLAN ID = 3:

Port-4 & 5 = Untagged,

Port -6 = Tagged,

Port-1~3 = Excluded.

Port to VLAN Settings			
VLAN ID: 3			
Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE2	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE3	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE4	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE5	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE6	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input checked="" type="checkbox"/>

4.5.14.2 VLAN Trunking between two 802.1Q aware switch

The most cases are used for “Uplink” to other switches. VLANs are separated at different switches, but they need to access with other switches within the same VLAN group. The screen in [Figure 4-5-21](#) appears.

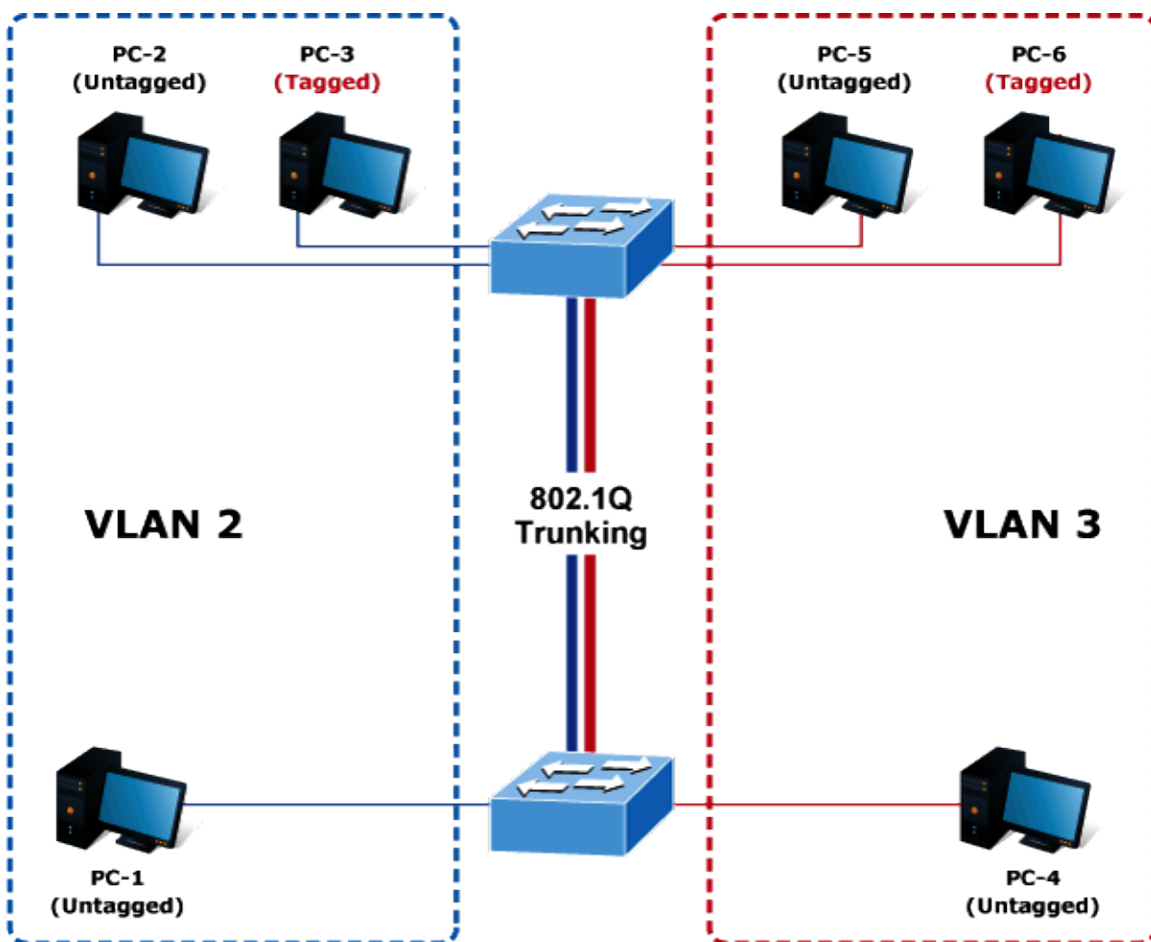


Figure 4-5-21: VLAN Trunking between two 802.1Q Aware Switch Diagrams

Setup steps

1. Create VLAN Group 2 and 3

Add VLAN group 2 and group 3

VLAN Table				
FIRST	PREV	1	NEXT	LAST
VLAN ID	VLAN Name	VLAN Type		
1	default	Default		
2	20002	Static		
3	30003	Static		

2. Assign VLAN mode and PVID for each port:

Port-1,Port-2 and Port-3 : VLAN Mode = Hybrid, PVID=2

Port-4,Port-5 and Port-6 : VLAN Mode = Hybrid, PVID=3

Port-7 : VLAN Mode = Hybrid, PVID=1

Port VLAN Status			
Port	Interface VLAN Mode	PVID	Accept Frame Type
GE1	Hybrid	2	ALL
GE2	Hybrid	2	ALL
GE3	Hybrid	2	ALL
GE4	Hybrid	3	ALL
GE5	Hybrid	3	ALL
GE6	Hybrid	3	ALL
GE7	Hybrid	1	ALL

3. Assign Tagged/Untagged for each port:

VLAN ID = 1:

Port-1~6 = Untagged,

Port -7 = Excluded.

Port to VLAN Settings

VLAN ID: 1

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="checkbox"/>
GE2	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="checkbox"/>
GE3	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="checkbox"/>
GE4	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="checkbox"/>
GE5	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="checkbox"/>
GE6	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="checkbox"/>
GE7	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input checked="" type="checkbox"/>

VLAN ID = 2:

Port-1 & 2 = Untagged,

Port-3 & 7 = Tagged,

Port -4~6 = Excluded.

Port to VLAN Settings

VLAN ID: 2

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE2	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE3	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE4	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE5	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE6	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE7	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>

VLAN ID = 3:

Port-4 & 5 = Untagged,

Port -6 & 7= Tagged,

Port-1~3 = Excluded.

Port to VLAN Settings

VLAN ID: 3

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE2	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE3	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE4	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE5	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE6	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE7	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>

4.6 Spanning Tree Protocol

4.6.1 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

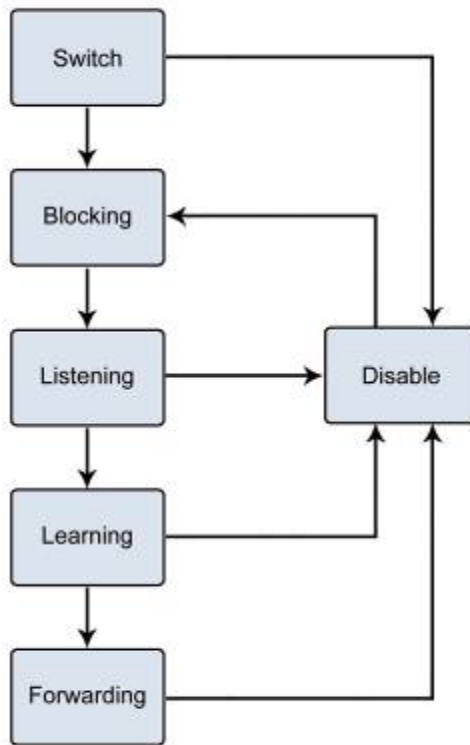



Figure 4-6-1: STP Port State Transitions

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	On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges.
	On the port level, STP sets the Root Port and the Designated Ports.

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

Parameter	Description	Default Value
Bridge Identifier(Not user configurable)	A combination of the User-set priority and the switch's MAC address.	32768 + MAC

except by setting priority below)	The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC	
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

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

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

Default Spanning-Tree Configuration

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

User-Changeable STA Parameters

The Switch's factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory; unless, it is absolutely necessary. The user changeable parameters in the Switch are as follows:

Priority – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.

Hello Time – The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.



The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

Max. Age – The Max Age can be from 6 to 40 seconds. At the end of the Max Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

Forward Delay Timer – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.



Observe the following formulas when setting the above parameters:

Max. Age _ 2 x (Forward Delay - 1 second)

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

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

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

3. Illustration of STP

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

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

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

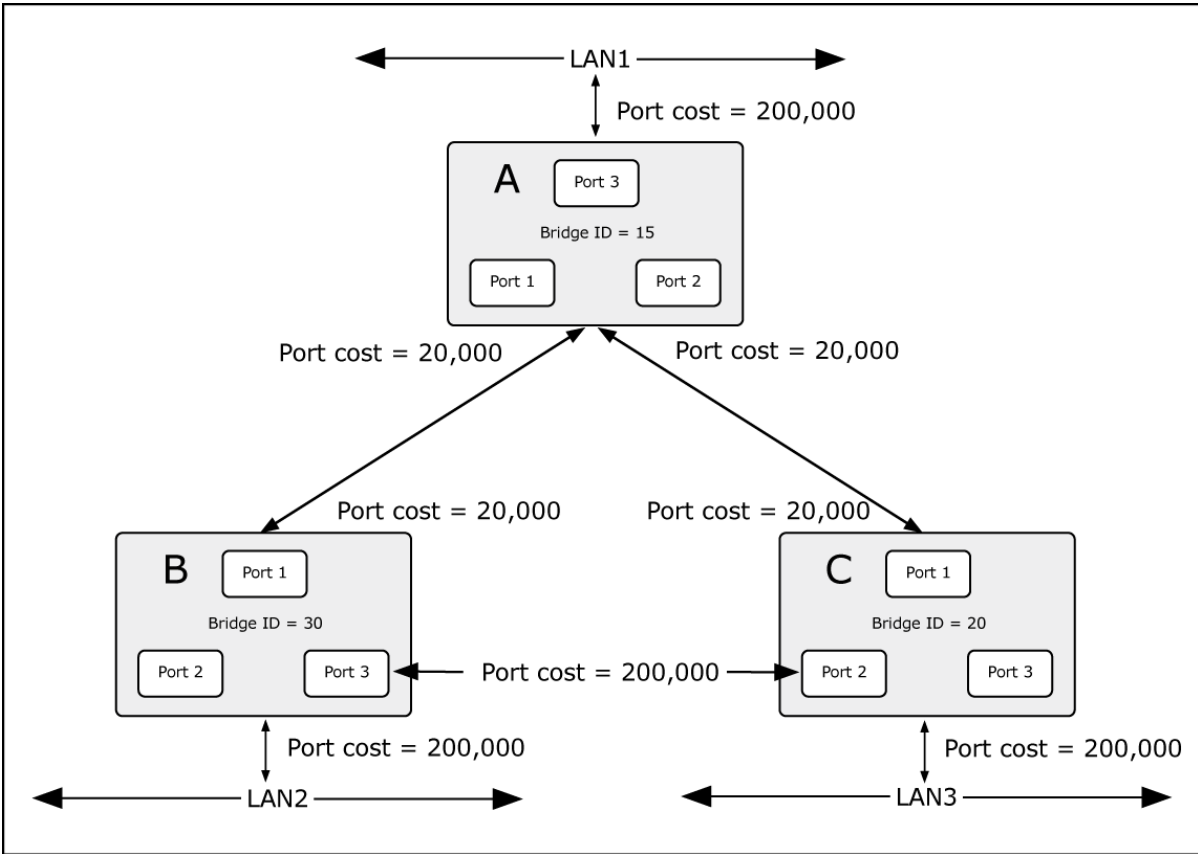


Figure 4-6-2: Before Applying the STA Rules

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

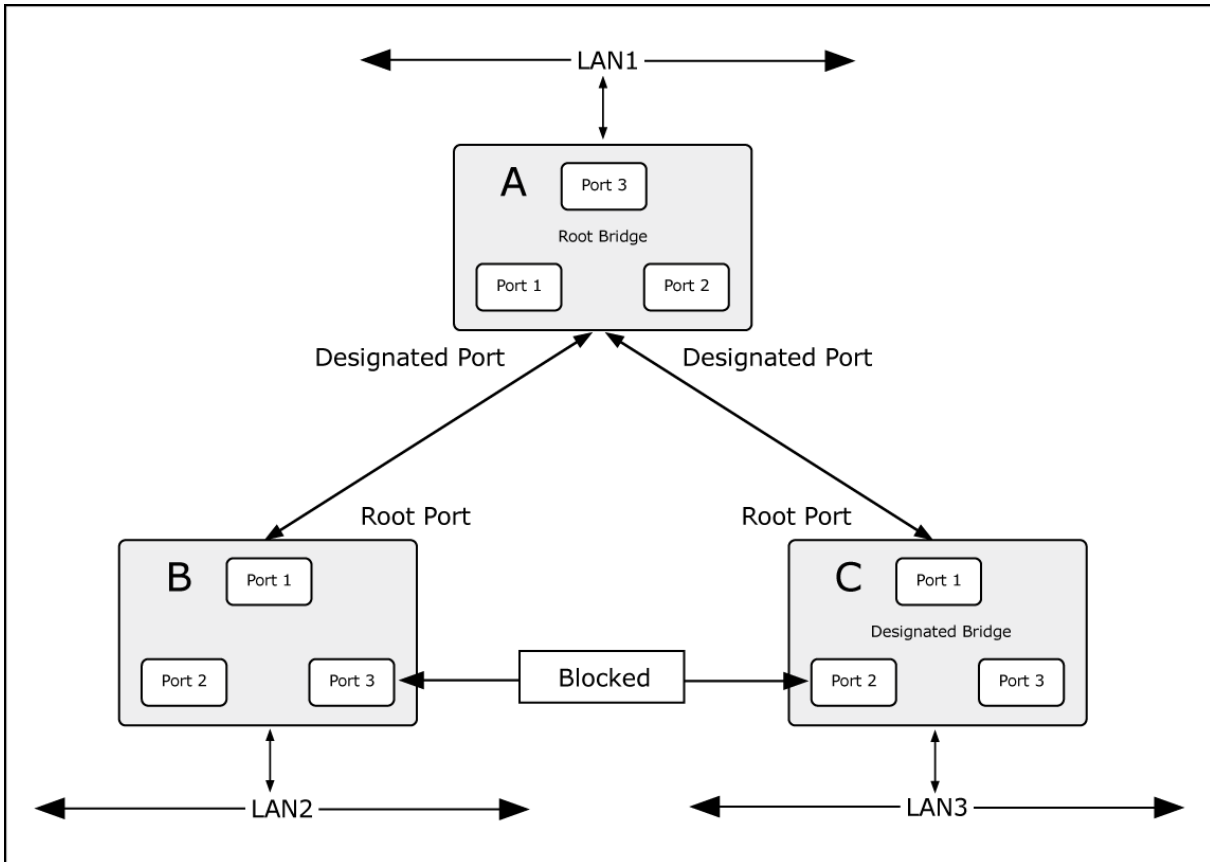


Figure 4-6-3: After Applying the STA Rules

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.

This section has the following items:

- **STP Global Setting** Configures STP system settings.
- **STP Port Setting** Configuration per port STP settings.
- **CIST Instance Setting** Configure system configuration.
- **CIST Port Setting** Configure CIST port setting.
- **MST Instance Setting** Configuration each MST instance settings.
- **MST Port Setting** Configuration per port MST setting.
- **STP Statistics** Display the STP statistics.

4.6.2 STP Global Settings

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch. The Managed Switch support the following Spanning Tree protocols:

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

The STP Global Settings screens in [Figure 4-6-4](#) and [Figure 4-6-5](#) appear.

STP Global Setting	
Global Setting	
Enabled	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
BPDU Forward	<input checked="" type="radio"/> Flooding <input type="radio"/> Filtering
PathCost Method	<input type="radio"/> Short <input checked="" type="radio"/> Long
Force Version	RSTP-Operation ▼
Configuration Name	00:30:4F:AF:FF:81 (Max. 32 character)
Configuration Revision	0 (0 - 65535)

Apply

Figure 4-6-4: Global Settings Page Screenshot

The page includes the following fields:

Object	Description
• Enable	Enable or disable the STP function. The default value is "Disabled".
• BPDU Forward	Set the BPDU forward method.
• PathCost Method	The path cost method is used 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.
• Force Version	The STP protocol version setting. Valid values are STP-Compatible , RSTP-Operation and MSTP-Operation .
• Configuration Name	Identifier used to identify the configuration currently being used.
• Configuration Revision	Identifier used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is 0 .

Button



: Click to apply changes.

STP Information

Information Name	Information Value
STP	Disabled
BPDU Forward	Flooding
Cost Method	Long
Force Version	RSTP-Operation
Configuration Name	00:30:4F:AF:FF:81
Configuration Revision	0

Figure 4-6-5: STP Information Page Screenshot

The page includes the following fields:

Object	Description
• STP	Display the current STP state.
• BPDU Forward	Display the current BPDU forward mode.
• Cost Method	Display the current cost method.
• Force Version	Display the current force version.
• Configuration Name	Display the current configuration name.
• Configuration Revision	Display the current configuration revision.

4.6.3 STP Port Setting

This page allows you to configure per port STP settings. The STP Port Setting screens in [Figure 4-6-6](#) and [Figure 4-6-7](#) appear.

Port Select	External Path Cost (0 = Auto)	Edge Port	BPDU Filter	BPDU Guard	P2P MAC	Migrate
Select Ports ▼	0	No ▼	No ▼	No ▼	Yes ▼	<input type="checkbox"/>

Apply

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

The page includes the following fields:

Object	Description
• Port Select	Select port number for this drop down list.
• External Cost (0 = Auto)	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
• Edge Port	Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized).
• BPDU Filter	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
• BPDU Guard	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
• P2P MAC	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media. (This applies to physical ports only. Aggregations are always <i>forced Point2Point</i>).
• Migrate	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)

Button



: Click to apply changes.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 802.1w standard exceeds 65,535, the default is set to 65,535.

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

Table 4-6-1: Recommended STP Path Cost Range

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

Table 4-6-2: Recommended STP Path Costs

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

Table 4-6-3: Default STP Path Costs

CIST Port Status						
Port	Admin Enable	External Cost	Edge Port	BPDU Filter	BPDU Guard	P2P MAC
GE1	Enable	0	No	No	No	Yes
GE2	Enable	0	No	No	No	Yes
GE3	Enable	0	No	No	No	Yes
GE4	Enable	0	No	No	No	Yes
GE5	Enable	0	No	No	No	Yes
GE6	Enable	0	No	No	No	Yes
GE7	Enable	0	No	No	No	Yes
GE8	Enable	0	No	No	No	Yes
GE9	Enable	0	No	No	No	Yes
GE10	Enable	0	No	No	No	Yes
GE11	Enable	0	No	No	No	Yes
GE12	Enable	0	No	No	No	Yes
GE13	Enable	0	No	No	No	Yes
GE14	Enable	0	No	No	No	Yes
GE15	Enable	0	No	No	No	Yes
GE16	Enable	0	No	No	No	Yes
GE17	Enable	0	No	No	No	Yes
GE18	Enable	0	No	No	No	Yes
GE19	Enable	0	No	No	No	Yes
GE20	Enable	0	No	No	No	Yes
GE21	Enable	0	No	No	No	Yes
GE22	Enable	0	No	No	No	Yes
GE23	Enable	0	No	No	No	Yes
GE24	Enable	0	No	No	No	Yes
GE25	Enable	0	No	No	No	Yes
GE26	Enable	0	No	No	No	Yes
LAG1	Enable	0	No	No	No	Yes
LAG2	Enable	0	No	No	No	Yes
LAG3	Enable	0	No	No	No	Yes
LAG4	Enable	0	No	No	No	Yes
LAG5	Enable	0	No	No	No	Yes
LAG6	Enable	0	No	No	No	Yes
LAG7	Enable	0	No	No	No	Yes
LAG8	Enable	0	No	No	No	Yes

Figure 4-6-7: STP Port Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical STP port.
• Admin Enable	Display the current STP port mode status.
• External Cost	Display the current external cost.
• Edge Port	Display the current edge port status.
• BPDU Filter	Display the current BPDU filter configuration.
• BPDU Guard	Display the current BPDU guard configuration.
• P2P MAC	Display the current P2P MAC status.

4.6.4 CIST Instance Setting

This Page allows you to configure CIST instance settings. The CIST Instance Setting and Information screens in [Figure 4-6-8](#), [Figure 4-6-9](#) and [Figure 4-6-10](#) appear.

CIST Instance Setting

CIST Instance Setting

Priority	<input style="width: 80%;" type="text" value="32768"/>
Max Hops	<input style="width: 40%;" type="text" value="20"/> (1-40)
Forward Delay	<input style="width: 40%;" type="text" value="15"/> (4-30)
Max Age	<input style="width: 40%;" type="text" value="20"/> (6-40)
Tx Hold Count	<input style="width: 40%;" type="text" value="6"/> (1-10)
Hello Time	<input style="width: 40%;" type="text" value="2"/> (1-10)

Figure 4-6-8: CIST Instance Setting Page Screenshot

The Page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Priority 	<p>Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.</p> <p>For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.</p>
<ul style="list-style-type: none"> • Max Hops 	<p>This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 1 to 40 hops.</p>
<ul style="list-style-type: none"> • Forward Delay 	<p>The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds</p> <p>-Default: 15</p> <p>-Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]</p> <p>-Maximum: 30</p>
<ul style="list-style-type: none"> • Max Age 	<p>The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds.</p>

	<p>-Default: 20</p> <p>-Minimum: The higher of 6 or $[2 \times (\text{Hello Time} + 1)]$.</p> <p>-Maximum: The lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$</p>
<ul style="list-style-type: none"> • Tx Hold Count 	<p>The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.</p>
<ul style="list-style-type: none"> • Hello Time 	<p>The time that controls the switch to send out the BPDU packet to check STP current status.</p> <p>Enter a value between 1 through 10.</p>

Button



: Click to apply changes.

▼ CIST Instance Information

Information Name	Information Value
Priority	32768
Max Hops	20
Forward Delay	15
Max Age	20
Tx Hold Count	6
Hello Time	2

Figure 4-6-9: CIST Instance Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Priority 	Display the current CIST priority.
<ul style="list-style-type: none"> • Max Hop 	Display the current Max. hops.
<ul style="list-style-type: none"> • Forward Delay 	Display the current forward delay.
<ul style="list-style-type: none"> • Max Age 	Display the current Max. age.
<ul style="list-style-type: none"> • Tx Hold Count 	Display the current Tx hold count.
<ul style="list-style-type: none"> • Hello Time 	Display the current hello time.

CIST Instance Status	
Information Name	Information Value
Bridge Identifier	32768/ 0/00:30:4F:AF:FF:81
Designated Root Bridge	0/ 0/00:00:00:00:00:00
External Root Path Cost	0
Regional Root Bridge	0/ 0/00:00:00:00:00:00
Internal Root Path Cost	0
Designated Bridge	0/ 0/00:00:00:00:00:00
Root Port	0 / 0
Remaining Hops	0
Last Topology Change	0

Figure 4-6-10: CIST Instance Information Page Screenshot

The page includes the following fields:

Object	Description
• Bridge Identifier	Display the bridge identifier information.
• Designated Root Bridge	Display the designed root bridge information.
• External Root Path Cost	Display the external root path cost information.
• Regional Root Bridge	Display the regional root bridge information.
• Internal Root Path Cost	Display the internal root path cost information.
• Designated Bridge	Display the designated bridge information.
• Root Port	Display the root port information.
• Remaining Hops	Display the remaining hops information.
• Last Topology Change	Display the last topology change information.

4.6.5 CIST Port Setting

This page allows you to configure per port CIST priority and cost. The CIST Port Setting and Status screens in [Figure 4-6-11](#) and [Figure 4-6-12](#) appear.

Port Select	Priority	Internal Path Cost (0 = Auto)
Select Ports	128	0

Apply

Figure 4-6-11: CIST Port Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port Select 	Select port number for this drop down list.
<ul style="list-style-type: none"> • Priority 	<p>Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).</p> <p>Default: 128</p> <p>Range: 0-240, in steps of 16</p>
<ul style="list-style-type: none"> • Internal Path Cost (0 = Auto) 	<p>Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports.</p> <p>Valid values are in the range 1 to 200000000.</p>

Button

: Click to apply changes.

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical STP port.
• Identifier (Priority / Port ID)	Display the current identifier (Priority / Port ID).
• External Path Cost Conf/Oper	Display the current external path cost conf/oper.
• Internal Path Cost Conf/Oper	Display the current internal path cost/oper.
• Designated Root Bridge	Display the current designated root bridge..
• External Root Cost	Display the current external root cost.
• Regional Root Bridge	Display the current regional root bridge.
• Internal Root Cost	Display the current internal root cost.
• Designated Bridge	Display the current designated bridge.
• Internal Port Path Cost	Display the current internal port path cost.
• Edge Port Conf/Oper	Display the current edge port conf/oper.
• P2P MAC Conf/Oper	Display the current P2P MAC conf/oper.
• Port Role	Display the current prot role.
• Port State	Display the current port state.

4.6.6 MST Instance Configuration

This page allows the user to configure MST Instance Configuration. The MST Instance Setting, Information and Status screens in [Figure 4-6-13](#), [Figure 4-6-14](#) and [Figure 4-6-15](#) appear.

MSTI ID (1-15)	VLAN List (1-4094)	Priority
1		32768

Apply

Figure 4-6-13: MST Instance Setting Page Screenshot

The page includes the following fields:

Object	Description
• MSTI ID	Allow assign MSTI ID. The range for the MSTI ID is 1-15.
• VLAN List (1-4094)	Allow assign VLAN list for special MSTI ID. The range for the VLAN list is 1-4094.
• Priority	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Button

: Click to apply changes.

MSTI	Status	VLAN List	VLAN Count	Priority
------	--------	-----------	------------	----------

Figure 4-6-14: MSTI Instance Setting Information Page Screenshot

The page includes the following fields:

Object	Description
• MSTI	Display the current MSTI entry.
• Status	Display the current MSTI status
• VLAN List	Display the current VLAN list.
• VLAN Count	Display the current VLAN count.
• Priority	Display the current MSTI priority

MST Instance Status	
Information Name	Information Value
MSTI ID	1
Regional Root Bridge	--/--
Internal Root Cost	--/--
Designated Bridge	--/--
Root Port	--/--
Max Age	--/--
Forward Delay	--/--
Remaining Hops	--/--
Last Topology Change	--/--

Figure 4-6-15: MST Instance Status Page Screenshot

The page includes the following fields:

Object	Description
• MSTI ID	Display the MSTI ID.
• Regional Root Bridge	Display the current designated root bridge.
• Internal Root Cost	Display the current internal root cost.
• Designated Bridge	Display the current designated bridge.
• Root Port	Display the current root port.
• Max Age	Display the current max. age.
• Forward Delay	Display the current forward delay.
• Remaining Hops	Display the current remaining hops.
• Last Topology Change	Display the current last topology change.

4.6.7 MST Port Setting

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

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

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are global. The MSTI Ports Setting screens in [Figure 4-6-16](#) and [Figure 4-6-17](#) appear.

MST ID	Port Select	Priority	Internal Path Cost (0 = Auto)
1	Select Ports	128	0

Apply

Figure 4-6-16: MST Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• MST ID	Enter the special MST ID to configure path cost & priority.
• Port Select	Select port number for this drop down list.
• Priority	Controls the port priority. This can be used to control priority of ports having identical port cost.
• Internal Path Cost (0 = Auto)	<p>Controls the path cost incurred by the port.</p> <p>The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered.</p> <p>The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports.</p> <p>Valid values are in the range 1 to 200000000.</p>

Button

Apply: Click to apply changes.

MST Port Status									
MSTI ID	Port	Identifier (Priority / Port ID)	Internal Path Cost Conf/Oper	Regional Root Bridge	Internal Root Cost	Designated Bridge	Internal Path Cost	Port Role	Port State
1	GE1	128/1	0/-	-/-	--	-/-	--	--	--
1	GE2	128/2	0/-	-/-	--	-/-	--	--	--
1	GE3	128/3	0/-	-/-	--	-/-	--	--	--
1	GE4	128/4	0/-	-/-	--	-/-	--	--	--
1	GE5	128/5	0/-	-/-	--	-/-	--	--	--
1	GE6	128/6	0/-	-/-	--	-/-	--	--	--
1	GE7	128/7	0/-	-/-	--	-/-	--	--	--
1	GE8	128/8	0/-	-/-	--	-/-	--	--	--
1	GE9	128/9	0/-	-/-	--	-/-	--	--	--
1	GE10	128/10	0/-	-/-	--	-/-	--	--	--
1	GE11	128/11	0/-	-/-	--	-/-	--	--	--
1	GE12	128/12	0/-	-/-	--	-/-	--	--	--
1	GE13	128/13	0/-	-/-	--	-/-	--	--	--
1	GE14	128/14	0/-	-/-	--	-/-	--	--	--
1	GE15	128/15	0/-	-/-	--	-/-	--	--	--
1	GE16	128/16	0/-	-/-	--	-/-	--	--	--
1	GE17	128/17	0/-	-/-	--	-/-	--	--	--
1	GE18	128/18	0/-	-/-	--	-/-	--	--	--
1	GE19	128/19	0/-	-/-	--	-/-	--	--	--
1	GE20	128/20	0/-	-/-	--	-/-	--	--	--
1	GE21	128/21	0/-	-/-	--	-/-	--	--	--
1	GE22	128/22	0/-	-/-	--	-/-	--	--	--
1	GE23	128/23	0/-	-/-	--	-/-	--	--	--
1	GE24	128/24	0/-	-/-	--	-/-	--	--	--
1	GE25	128/25	0/-	-/-	--	-/-	--	--	--
1	GE26	128/26	0/-	-/-	--	-/-	--	--	--
1	LAG1	128/27	0/-	-/-	--	-/-	--	--	--
1	LAG2	128/28	0/-	-/-	--	-/-	--	--	--
1	LAG3	128/29	0/-	-/-	--	-/-	--	--	--
1	LAG4	128/30	0/-	-/-	--	-/-	--	--	--
1	LAG5	128/31	0/-	-/-	--	-/-	--	--	--
1	LAG6	128/32	0/-	-/-	--	-/-	--	--	--
1	LAG7	128/33	0/-	-/-	--	-/-	--	--	--
1	LAG8	128/34	0/-	-/-	--	-/-	--	--	--

Figure 4-6-17: MST Port Status Page Screenshot

The page includes the following fields:

Object	Description
• MSTI ID	Display the current MSTI ID.
• Port	The switch port number of the logical STP port.
• Identifier (Priority / Port ID)	Display the current identifier (priority / port ID).
• Internal Path Cost Conf/Oper	Display the current internal path cost configuration / operation.
• Regional Root Bridge	Display the current regional root bridge.
• Internal Root Cost	Display the current internal root cost.
• Designated Bridge	Display the current designated bridge.

• Internal Path Cost	Display the current internal path cost.
• Port Role	Display the current port role.
• Port State	Display the current port state.

4.6.8 STP Statistics

This page displays STP statistics. The STP statistics screen in [Figure 4-6-18](#) appears.

STP Statistics						
STP Statistics						
Port	Configuration BPDUs Received	TCN BPDUs Received	MSTP BPDUs Received	Configuration BPDUs Transmitted	TCN BPDUs Transmitted	MSTP BPDUs Transmitted
GE1	0	0	0	0	0	0
GE2	0	0	0	0	0	0
GE3	0	0	0	0	0	0
GE4	0	0	0	0	0	0
GE5	0	0	0	0	0	0
GE6	0	0	0	0	0	0
GE7	0	0	0	0	0	0
GE8	0	0	0	0	0	0
GE9	0	0	0	0	0	0
GE10	0	0	0	0	0	0
GE11	0	0	0	0	0	0
GE12	0	0	0	0	0	0
GE13	0	0	0	0	0	0
GE14	0	0	0	0	0	0
GE15	0	0	0	0	0	0
GE16	0	0	0	0	0	0
GE17	0	0	0	0	0	0
GE18	0	0	0	0	0	0
GE19	0	0	0	0	0	0
GE20	0	0	0	0	0	0
GE21	0	0	0	0	0	0
GE22	0	0	0	0	0	0
GE23	0	0	0	0	0	0
GE24	0	0	0	0	0	0
GE25	0	0	0	0	0	0
GE26	0	0	0	0	0	0
LAG1	0	0	0	0	0	0
LAG2	0	0	0	0	0	0
LAG3	0	0	0	0	0	0
LAG4	0	0	0	0	0	0
LAG5	0	0	0	0	0	0
LAG6	0	0	0	0	0	0
LAG7	0	0	0	0	0	0
LAG8	0	0	0	0	0	0

Figure 4-6-18: STP Statistics Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical STP port.
• Configuration BPDUs Received	Display the current configuration BPDUs received.
• TCN BPDUs Received	Display the current TCN BPDUs received.
• MSTP BPDUs Received	Display the current MSTP BPDUs received.
• Configuration BPDUs Transmitted	Display the configuration BPDUs transmitted.

• TCN BPDUs Transmitted	Display the current TCN BPDUs transmitted.
• MSTP BPDUs Transmitted	Display the current BPDUs transmitted.

4.7 Multicast

This section has the following items:

- **Properties** Configures multicast properties.
- **IGMP Snooping** Configures IGMP snooping settings.
- **IGMP Snooping Statistics** Display the IGMP snooping statistics.
- **MLD Snooping** Configures MLD snooping settings.
- **MLD Snooping Statistics** Display the MLD snooping statistics.
- **Multicast Throttling Setting** Configures multicast throttling setting.
- **Multicast Filter** Configures multicast filter.

4.7.1 Properties

This page provides multicast properties related configuration.

The multicast Properties and Information screens in [Figure 4-7-1](#) and [Figure 4-7-2](#) appear.

Properties

Properties Setting

L2 Unknown Multicast Action	<input type="radio"/> Drop <input checked="" type="radio"/> Flood
IP Unknown Multicast Action	<input type="radio"/> Drop <input checked="" type="radio"/> Flood <input type="radio"/> Router Port
IPv6 Unknown Multicast Action	<input type="radio"/> Drop <input checked="" type="radio"/> Flood <input type="radio"/> Router Port
IPv4 Forward Method	<input checked="" type="radio"/> MAC <input type="radio"/> Src-Dst-Ip
IPv6 Forward Method	<input checked="" type="radio"/> MAC <input type="radio"/> Src-Dst-Ip

Figure 4-7-1: Properties Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • L2 Unknow Multicast Action 	Action for L2 unknown multicast traffic: Options are: Drop or flood .
<ul style="list-style-type: none"> • IP Unknown Multicast Action 	Action for IP unknown multicast traffic: Drop , flood or send to router port .
<ul style="list-style-type: none"> • IPv6 Unknown Multicast Action 	Action for IP unknown IPv6 multicast traffic: Drop , flood or send to router port .
<ul style="list-style-type: none"> • IPv4 Forward Method 	Configure the IPv4 multicast forward method.

	Options are: MAC or Src-Dst-Ip.
<ul style="list-style-type: none"> • IPv6 Forward Method 	Configure the IPv6 multicast forward method. Options are: MAC or Src-Dst-Ip.

Button

: Click to apply changes.

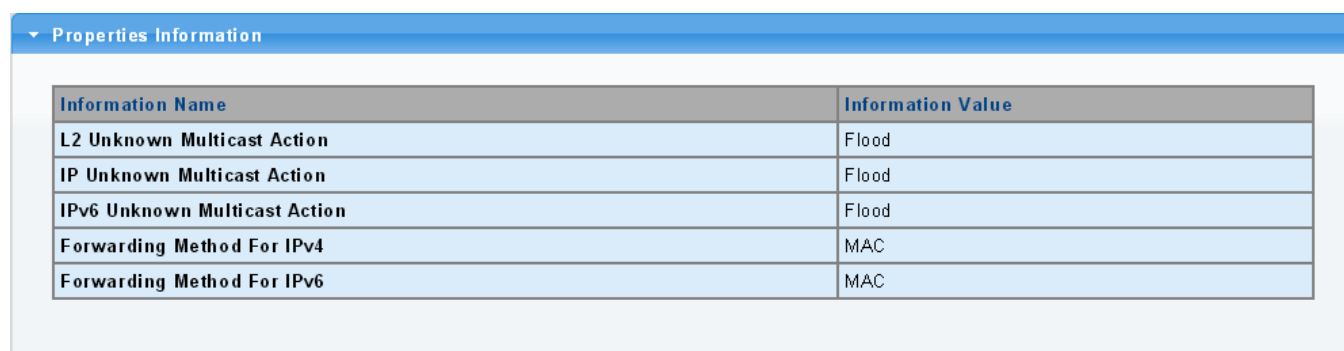


Figure 4-7-2: Properties Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • L2 Unknow Multicast Action 	Display the current L2 unknown multicast action status.
<ul style="list-style-type: none"> • IP Uknown Multicast Action 	Display the current IP unknown multicast action status.
<ul style="list-style-type: none"> • IPv6 Uknown Multicast Action 	Display the current IPv6 unknown multicast action status.
<ul style="list-style-type: none"> • Forward Method For IPv4 	Display the current IPv4 multicast forward method.
<ul style="list-style-type: none"> • Forward Method For IPv6 	Display the current IPv4 multicast forward method.

4.7.2 IGMP Snooping

The **Internet Group Management Protocol (IGMP)** lets host and routers share information about multicast group 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.

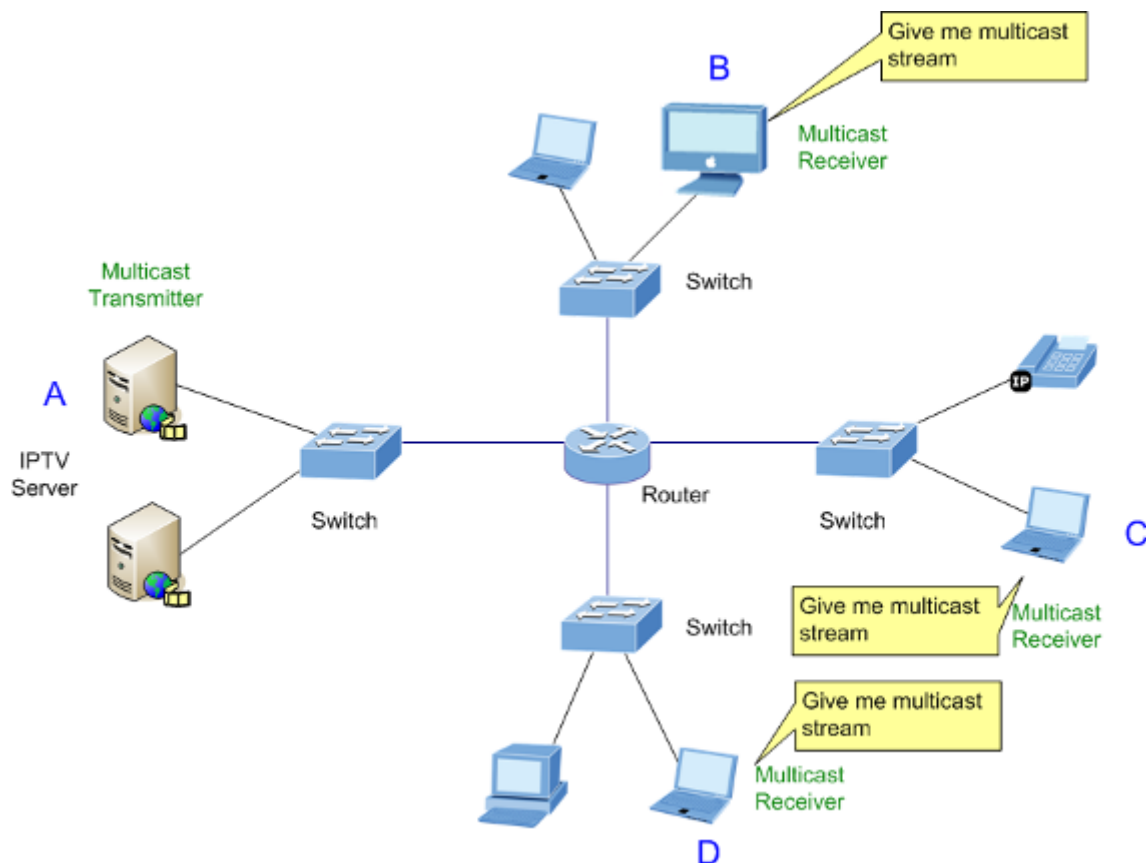


Figure 4-7-3: Multicast Service

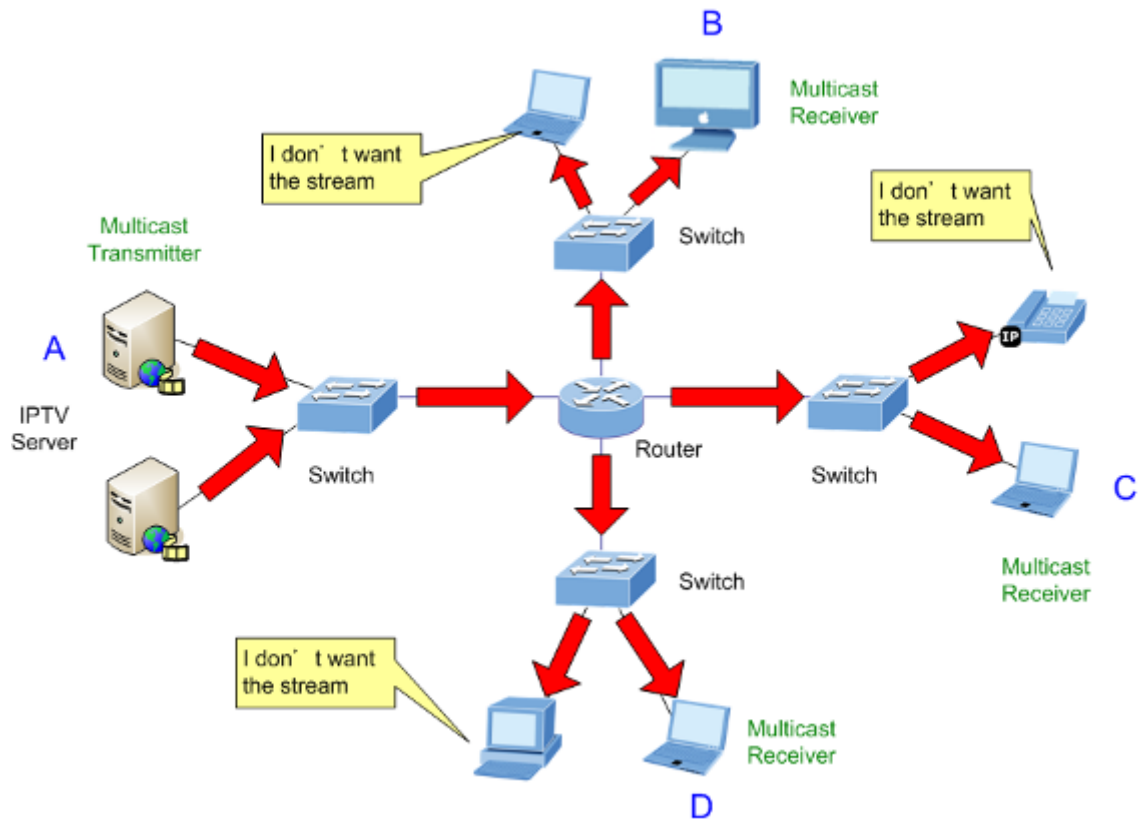


Figure 4-7-4: Multicast Flooding

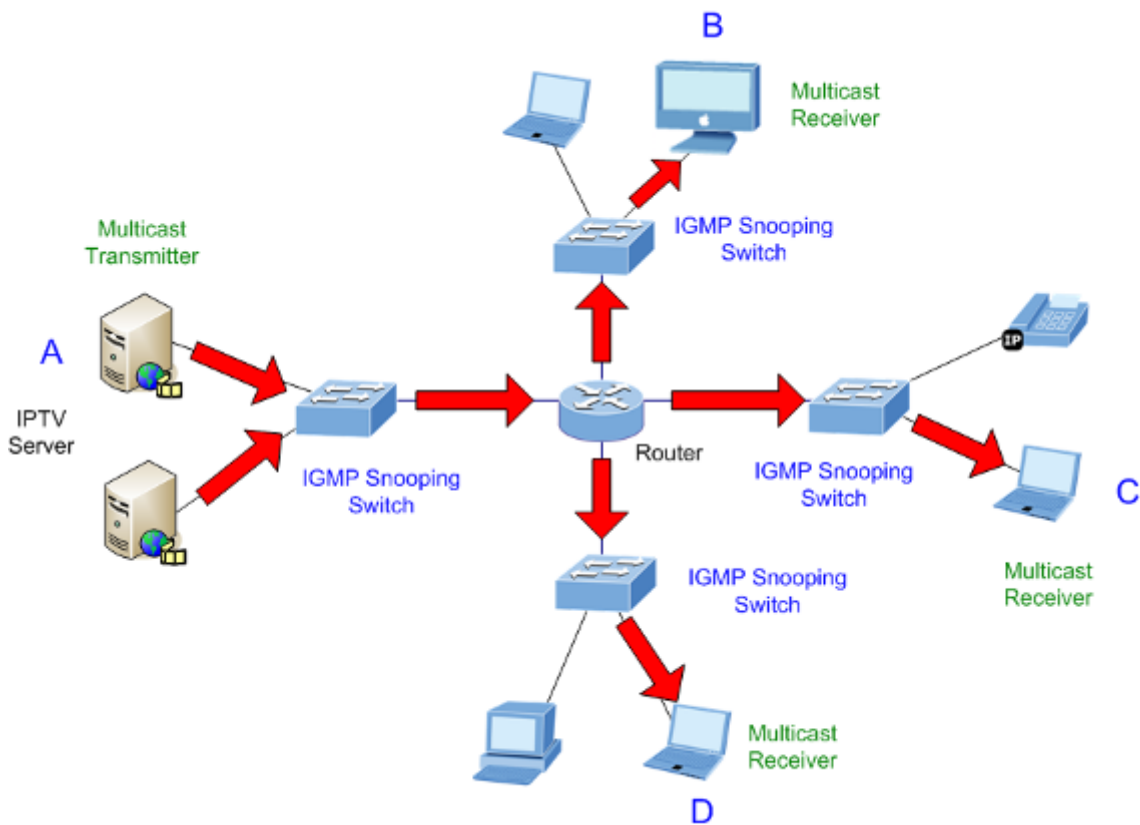


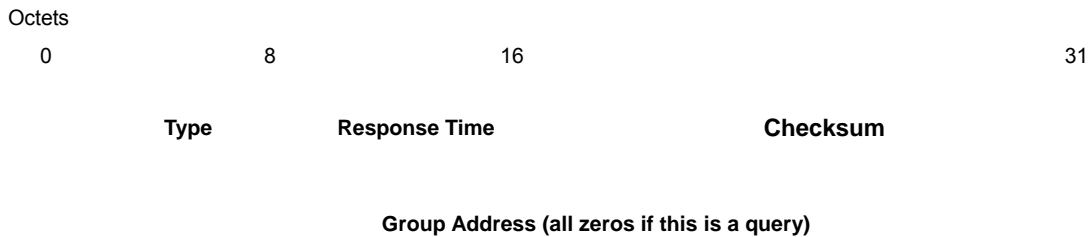
Figure 4-7-5: IGMP Snooping Multicast Stream Control

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

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:

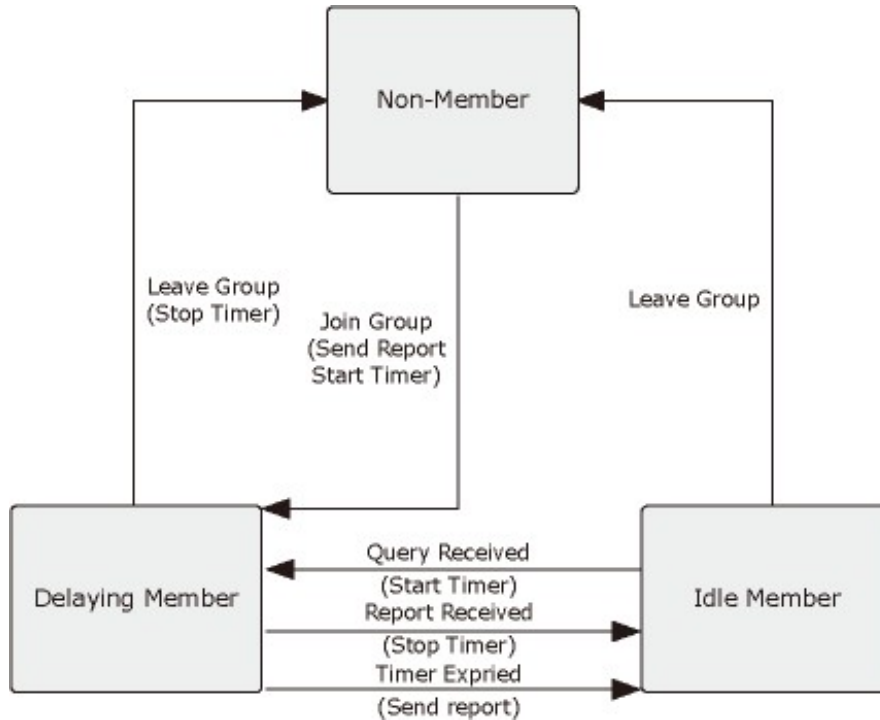
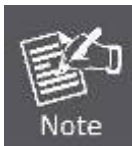


Figure 4-7-6: IGMP State Transitions

■ IGMP Querier –

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



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

4.7.2.1 IGMP Setting

This page provides IGMP Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the current unit, as reflected by the page header. The IGMP Snooping Setting and Information screens in [Figure 4-7-7](#), [Figure 4-7-8](#) and [Figure 4-7-9](#) appear.

IGMP Snooping	
IGMP Snooping Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IGMP Snooping Version	<input checked="" type="radio"/> v2 <input type="radio"/> v3
IGMP Snooping Report Suppression	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Figure 4-7-7: IGMP Snooping Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> IGMP Snooping Status 	Enable or disable the IGMP snooping. The default value is "Disabled".
<ul style="list-style-type: none"> IGMP Snooping Version 	Sets the IGMP Snooping operation version. Possible versions are: <ul style="list-style-type: none"> v2: Set IGMP Snooping supported IGMP version 2. v3: Set IGMP Snooping supported IGMP version 3.
<ul style="list-style-type: none"> IGMP Snooping Report Suppression 	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as is to multicast-capable routers. The default is enabled.

Button

: Click to apply changes.

IGMP Snooping Information	
Information Name	Information Value
IGMP Snooping Status	Enable
IGMP Snooping Version	v2
IGMP Snooping V2 Report Suppression	Enable

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

The page includes the following fields:

Object	Description
• IGMP Snooping Status	Display the current IGMP snooping status.
• IGMP Snooping Version	Display the current IGMP snooping version.
• IGMP Snooping V2 Report Suppression	Display the current IGMP snooping v2 report suppression.

Entry No.	VLAN ID	IGMP Snooping Operation Status	Router Ports Auto Learn	Query Robustness	Query Interval(sec.)	Query Max Response Interval(sec.)	Last Member Query count	Last Member Query Interval(sec)	Immediate Leave	Modify
1	1	Disabled	Enabled	2	125	10	2	1	Disabled	Edit

Figure 4-7-9: IGMP Snooping Information Page Screenshot

The page includes the following fields:

Object	Description
• Entry No.	Display the current entry number.
• VLAN ID	Display the current VLAN ID.
• IGMP Snooping Operation Status	Display the current IGMP snooping operation status.
• Router Ports Auto Learn	Display the current router ports auto learning.
• Query Robustness	Display the current query robustness.
• Query Interval (sec.)	Display the current query interval.
• Query Max Response Interval (sec.)	Display the current query max response interval.
• Last Member Query count	Display the current last member query count.
• Last Member Query Interval (sec)	Display the current last member query interval.
• Immediate Leave	Display the current immediate leave.
• Modify	Click Edit to edit parameter.

4.7.2.2 IGMP Querier Setting

This page provides IGMP Querier Setting. The IGMP Querier Setting screens in [Figure 4-7-10](#) and [Figure 4-7-11](#) appear.

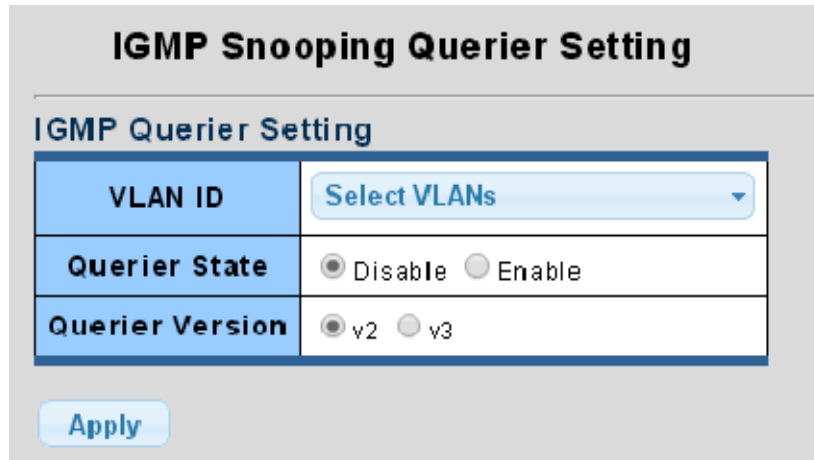


Figure 4-7-10: IGMP VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Select VLAN ID for this drop down list.
• Querier State	Enable or disable the querier state. The default value is "Disabled".
• Querier Version	Sets the querier version for compatibility with other devices on the network. Version: 2 or 3; Default: v2

Button

: Click to apply changes.

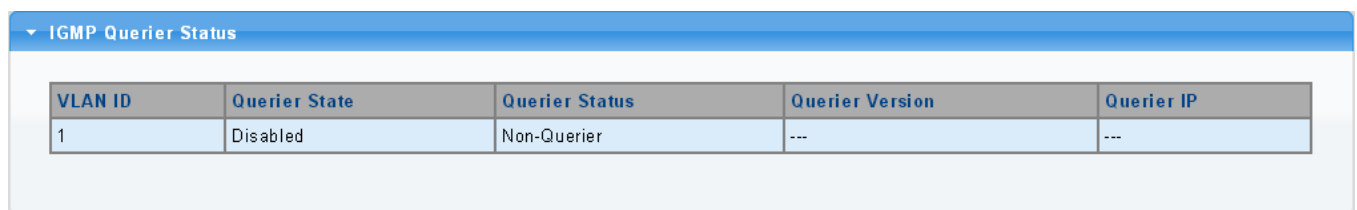


Figure 4-7-11: IGMP Querier Status Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VLAN ID.
• Querier State	Display the current querier state.
• Querier Status	Display the current querier stauts.
• Querier Version	Display the current querier version.
• Querier IP	Display the current querier IP.

4.7.2.3 IGMP Static Group

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in above sections. For certain applications that require tighter control, you may need to statically configure a multicast service on the Managed Switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

The IGMP Static Group configuration screens in [Figure 4-7-12](#) and [Figure 4-7-13](#) appear.

Figure 4-7-12: Add IGMP Static Group Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Select VLAN ID for this drop down list.
• Group IP Address	The IP address for a specific multicast service.
• Member Ports	Select port number for this drop down list.


Button

: Click to add IGMP router port entry.

IGMP Static Groups			
VLAN ID	Group IP Address	Member Ports	Modify

Figure 4-7-13: IGMP Static Groups Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VLAN ID.
• Group IP Address	Display the current group IP address.
• Member Ports	Display the current member ports.
• Modify	Click  to edit parameter.

4.7.2.4 IGMP Group Table

This page provides Multicast Database. The IGMP Group Table screen in [Figure 4-7-14](#) appears.

IGMP Group Table				
VLAN ID	Group IP Address	Member Ports	Type	Life(Sec)

Figure 4-7-14: IGMP Group Table Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VID.
• Group IP Address	Display multicast IP address for a specific multicast service.
• Member Ports	Display the current member port.
• Type	Member types displayed include Static or Dynamic, depending on selected options.
• Life(Sec)	Display the current life.

4.7.2.5 IGMP Router Setting

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your Managed Switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the Managed Switch. The IGMP Router Setting and Status screens in [Figure 4-7-15](#) and [Figure 4-7-16](#) appear.

Figure 4-7-15: Add Router Port Page Screenshot

The page includes the following fields:



Object	Description
<ul style="list-style-type: none"> VLAN ID 	Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
<ul style="list-style-type: none"> Type 	Sets the Router port type. The types of Router port as below: <ul style="list-style-type: none"> ■ Static ■ Forbid
<ul style="list-style-type: none"> Static Ports Select 	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.
<ul style="list-style-type: none"> Forbid Port Select 	Specify which ports un-act as router ports.

Button

: Click to add IGMP router port entry.

Figure 4-7-16: Router Port Status Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VLAN ID.
• Static Ports	Display the current static ports.
• Forbidden Ports	Display the current forbidden ports.
• Modify	Click  to edit parameter. Click  to delete the group ID entry.

4.7.2.6 IGMP Router Table

This page provides Router Table. The Dynamic, Static and Forbidden Router Table screens in [Figure 4-7-17](#), [Figure 4-7-18](#) and [Figure 4-7-19](#) appear.

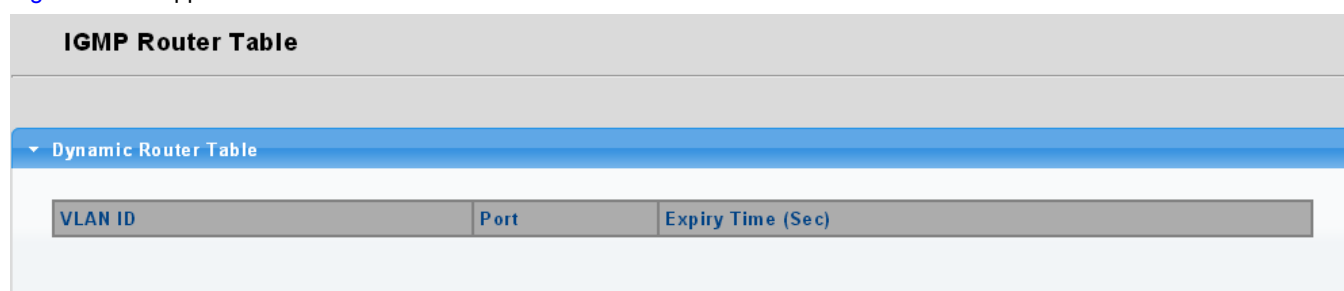


Figure 4-7-17: Dynamic Router Table Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VLAN ID.
• Port	Display the current dynamic router ports.
• Expiry Time (Sec)	Display the current expiry time.

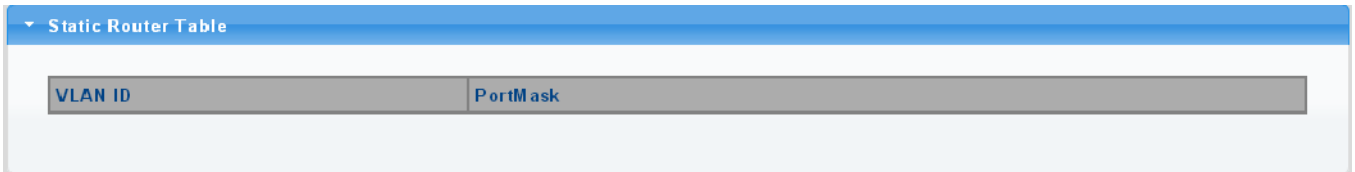


Figure 4-7-18: Static Router Table Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VLAN ID.
• Port Mask	Display the current port mask.

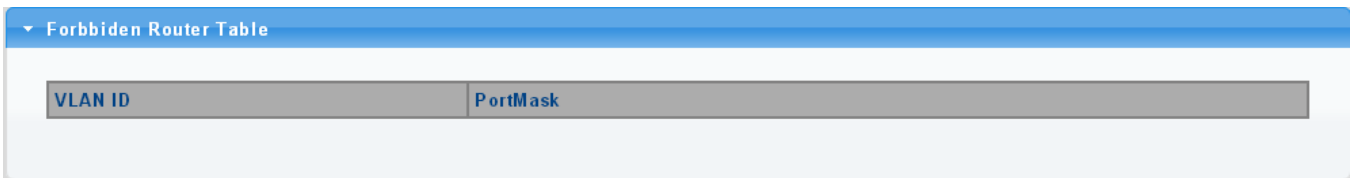


Figure 4-7-19: Forbidden Router Table Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VLAN ID.
• Port Mask	Display the current port mask.

4.7.2.7 IGMP Forward All

This page provides IGMP Forward All. The Forward All screen in [Figure 4-7-20](#) appears.

IGMP Forward All

▼ Forward All

VLAN ID :


Port	Membership
GE1	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE2	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE3	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE4	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE5	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE6	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE7	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE8	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE9	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE10	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE11	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE12	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE13	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE14	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE15	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE16	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE17	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE18	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE19	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE20	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE21	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE22	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE23	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE24	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE25	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE26	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
LAG1	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
LAG2	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
LAG3	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
LAG4	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
LAG5	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
LAG6	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
LAG7	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
LAG8	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None

Figure 4-7-20: Forward All Setting Page Screenshot

The page includes the following fields:

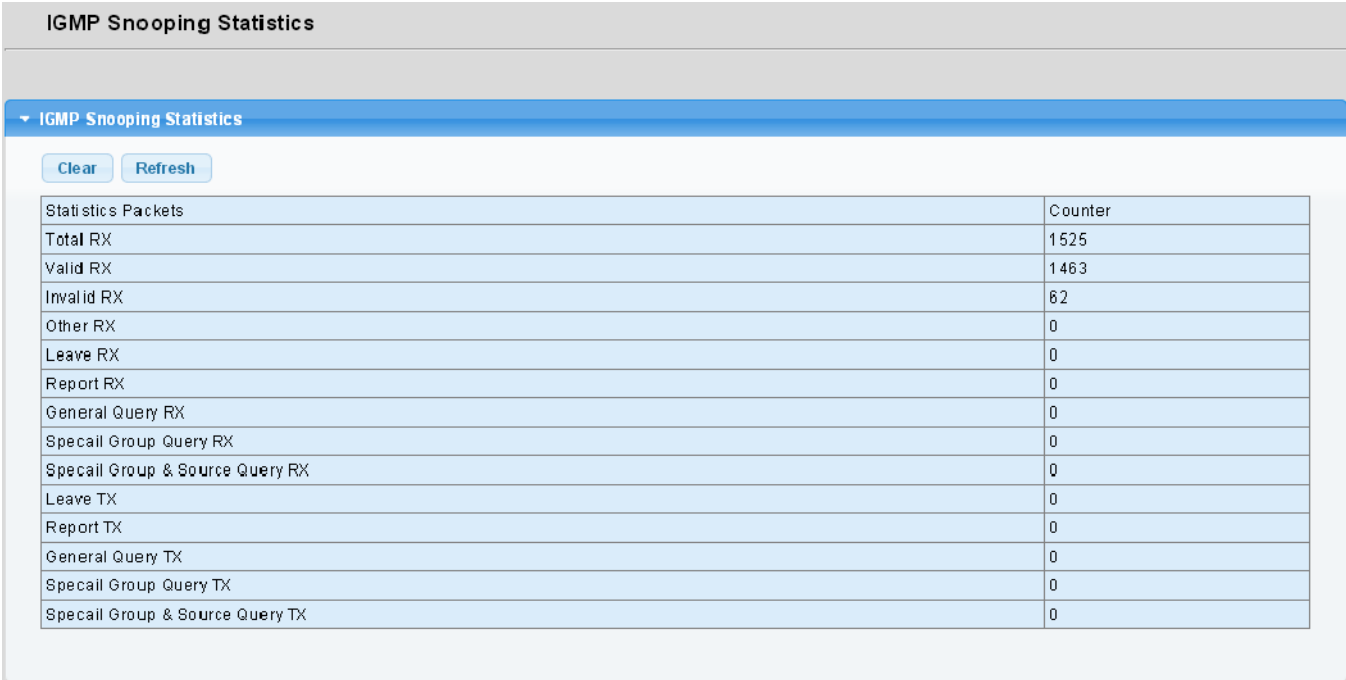
Object	Description	
• VLAN ID	Select VLAN ID for this drop down list to assign IGMP membership.	
• Port	The switch port number of the logical port.	
• Membership	Select IGMP membership for each interface:	
	Static:	Interface is a member of the IGMP.
	Forbidden:	Interface is forbidden from automatically joining the IGMP via MVR.
	None:	Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.

Button

: Click to apply changes.

4.7.3 IGMP Snooping Statics

This page provides IGMP Snooping Statics. The IGMP Snooping Statics screen in [Figure 4-7-21](#) appears.



The screenshot shows the 'IGMP Snooping Statistics' page. At the top, there is a title bar 'IGMP Snooping Statistics'. Below it, a blue header bar contains a dropdown menu 'IGMP Snooping Statistics'. Underneath, there are two buttons: 'Clear' and 'Refresh'. The main content is a table with two columns: 'Statistics Packets' and 'Counter'. The table lists various RX and TX statistics with their corresponding counter values.

Statistics Packets	Counter
Total RX	1525
Valid RX	1463
Invalid RX	62
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Specail Group Query RX	0
Specail Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Specail Group Query TX	0
Specail Group & Source Query TX	0

Figure 4-7-21: Forward All Setting Page Screenshot

The page includes the following fields:

Object	Description
• Total RX	Display current total RX.
• Valid RX	Display current valid RX.
• Invalid RX	Display current invalid RX.
• Other RX	Display current other RX.
• Leave RX	Display current leave RX.
• Report RX	Display current report RX.
• General Query RX	Display current general query RX.
• Special Group Query RX	Display current special group query RX.
• Special Group & Source Query RX	Display current special group & source query RX.
• Leave TX	Display current leave TX.
• Report TX	Display current report TX.
• General Query TX	Display current general query TX.
• Special Group Query TX	Display current special group query TX.
• Special Group & Source Query TX	Display current special group & source query TX.

Buttons

Clear

: Click to clear the IGMP Snooping Statistics.

Refresh

: Click to refresh the IGMP Snooping Statistics.

4.7.4 MLD Snooping

4.7.4.1 MLD Setting

This page provides MLD Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the current unit, as reflected by the page header. The MLD Snooping Setting, Information and Table screens in [Figure 4-7-22](#), [Figure 4-7-23](#) and [Figure 4-7-24](#) appear.

MLD Snooping	
MLD Snooping Settings	
MLD Snooping Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MLD Snooping Version	<input checked="" type="radio"/> v1 <input type="radio"/> v2
MLD Snooping Report Suppression	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/>	

Figure 4-7-22: MLD Snooping Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • MLD Snooping Status 	Enable or disable the MLD snooping. The default value is "Disabled".
<ul style="list-style-type: none"> • MLD Snooping Version 	Sets the MLD Snooping operation version. Possible versions are: <ul style="list-style-type: none"> v1: Set MLD Snooping supported MLD version 1. v2: Set MLD Snooping supported MLD version 2.
<ul style="list-style-type: none"> • MLD Snooping Report Suppression 	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all MLD reports are sent as is to multicast-capable routers. The default is enabled.

Button

: Click to apply changes.

MLD Snooping Information	
Information Name	Information Value
MLD Snooping Status	Disable
MLD Snooping Version	v1
MLD Snooping V2 Report Suppression	Enable

Figure 4-7-23: MLD Snooping information Page Screenshot

The page includes the following fields:

Object	Description
• MLD Snooping Status	Display the current MLD snooping status.
• MLD Snooping Version	Display the current MLD snooping version.
• MLD Snooping V2 Report Suppression	Display the current MLD snooping V2 report suppression.

▼ MLD Snooping Table

Entry No.	VLAN ID	MLD Snooping Operation Status	Router Ports Auto Learn	Query Robustness	Query Interval(sec.)	Query Max Response Interval(sec.)	Last Member Query Count	Last Member Query Interval(sec)	Immediate Leave	Modify
1	1	Disabled	Enabled	2	125	10	2	1	Disabled	Edit

Figure 4-7-24: MLD Snooping Table Page Screenshot

The page includes the following fields:

Object	Description
• Entry No.	Display the current entry number.
• VLAN ID	Display the current VLAN ID.
• MLD Snooping Operation Status	Display the current MLD snooping operation status.
• Router Ports Auto Learn	Display the current router ports auto learning.
• Query Robustness	Display the current query robustness.
• Query Interval (sec.)	Display the current query interval.
• Query Max Response Interval (sec.)	Display the current query max response interval.
• Last Member Query count	Display the current last member query count.
• Last Member Query Interval (sec)	Display the current last member query interval.
• Immediate Leave	Display the current immediate leave.
• Modify	Click Edit to edit parameter.

4.7.4.2 MLD Static Group

The MLD Static Group configuration screens in [Figure 4-7-25](#) and [Figure 4-7-26](#) appear.

Figure 4-7-25: Add MLD Static Group Page Screenshot

The page includes the following fields:


Object	Description
• VLAN ID	Select VLAN ID for this drop down list.
• Group IP Address	The IP address for a specific multicast service.
• Member Ports	Select port number for this drop down list.

Button

: Click to add IGMP router port entry.

Figure 4-7-26: MLD Static Groups Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VLAN ID.
• Group IPv6 Address	Display the current group IPv6 address.
• Member Ports	Display the current member ports.
• Modify	Click  to edit parameter.

4.7.4.3 MLD Group Table

This page provides MLD Group Table. The MLD Group Table screen in [Figure 4-7-27](#) appears.

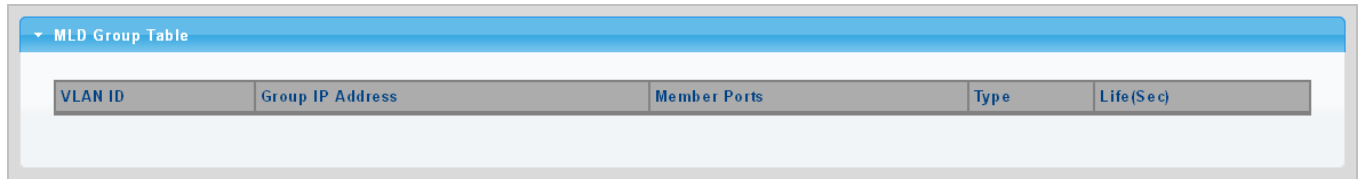


Figure 4-7-27: MLD Group Table Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VID.
• Group IP Address	Display multicast IP address for a specific multicast service.
• Member Port	Display the current member port.
• Type	Member types displayed include Static or Dynamic, depending on selected options.
• Life(Sec)	Display the current life.

4.7.4.4 MLD Router Setting

Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your Managed Switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the Managed Switch.

The MLD Router Setting screens in [Figure 4-7-28](#) and [Figure 4-7-29](#) appear.

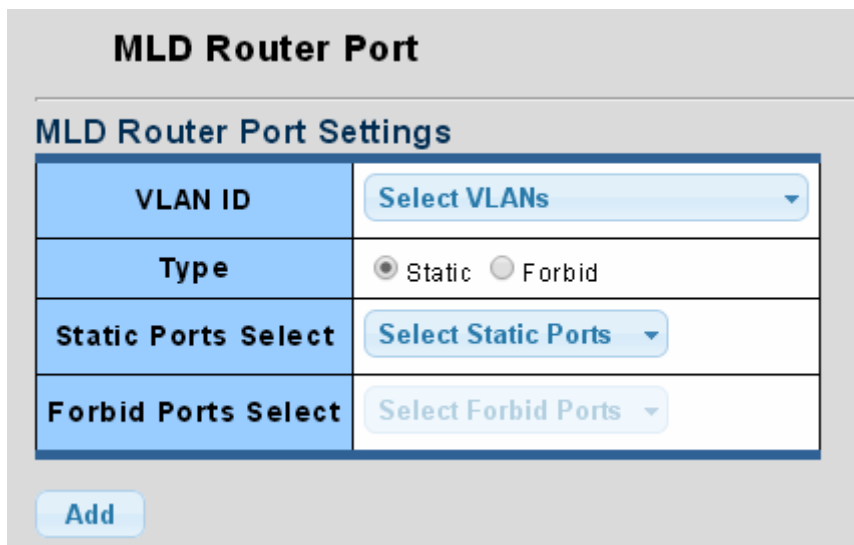


Figure 4-7-28: Add Router Port Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • VLAN ID 	Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
<ul style="list-style-type: none"> • Type 	Sets the Router port type. The types of Router port as below: <div style="margin-left: 20px;"> Static Forbid </div>
<ul style="list-style-type: none"> • Static Ports Select 	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.
<ul style="list-style-type: none"> • Forbid Port Select 	Specify which ports un-act as router ports

Button

Add : Click to add MLD router port entry.

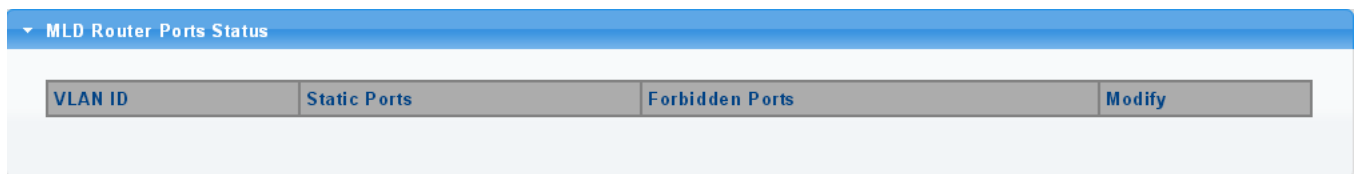


Figure 4-7-29: Router Port Status Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • VLAN ID 	Display the current VLAN ID.
<ul style="list-style-type: none"> • Static Ports 	Display the current static ports.
<ul style="list-style-type: none"> • Forbidden Ports 	Display the current forbidden ports.
<ul style="list-style-type: none"> • Modify 	Click Edit to edit parameter Click Delete to delete the group ID entry

4.7.4.5 MLD Router Table

This page provides Router Table. The Dynamic, Static and Forbidden Router Table screens in [Figure 4-7-30](#), [Figure 4-7-31](#) and [Figure 4-7-32](#) appear.

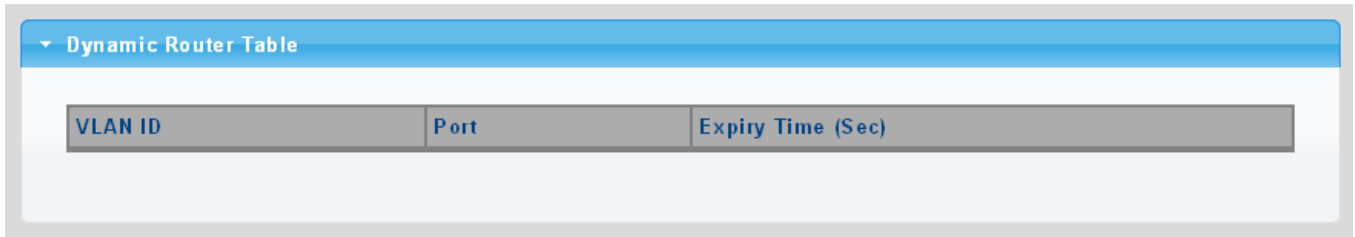


Figure 4-7-30: Dynamic Router Table Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VLAN ID.
• Port	Display the current dynamic router ports.
• Expiry Time (Sec)	Display the current expiry time.

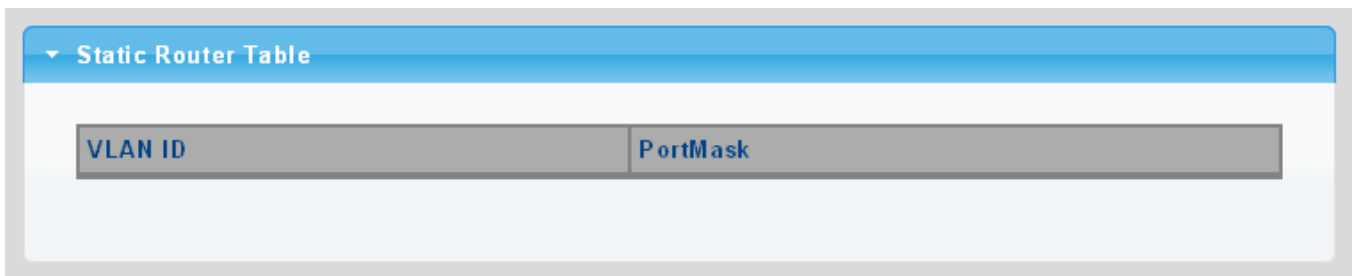


Figure 4-7-31: Static Router Table Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VLAN ID.
• Port Mask	Display the current port mask.

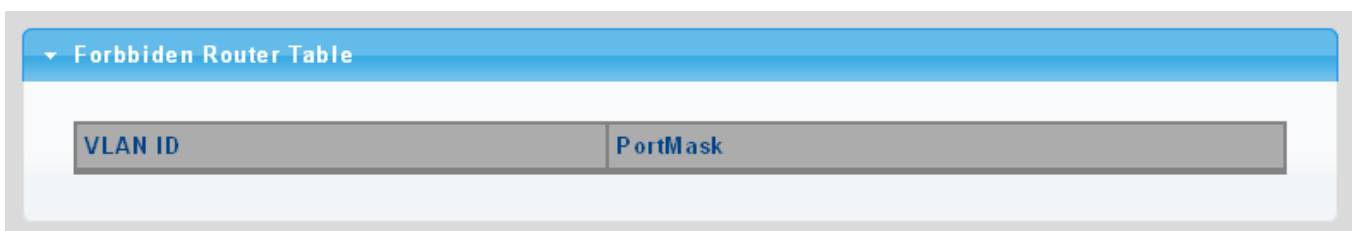


Figure 4-7-32: Forbidden Router Table Page Screenshot

The page includes the following fields:

Object	Description
• VLAN ID	Display the current VLAN ID.
• Port Mask	Display the current port mask.

4.7.4.6 MLD Forward All

This page provides MLD Forward All. The Forward All screen in [Figure 4-7-33](#) appears.

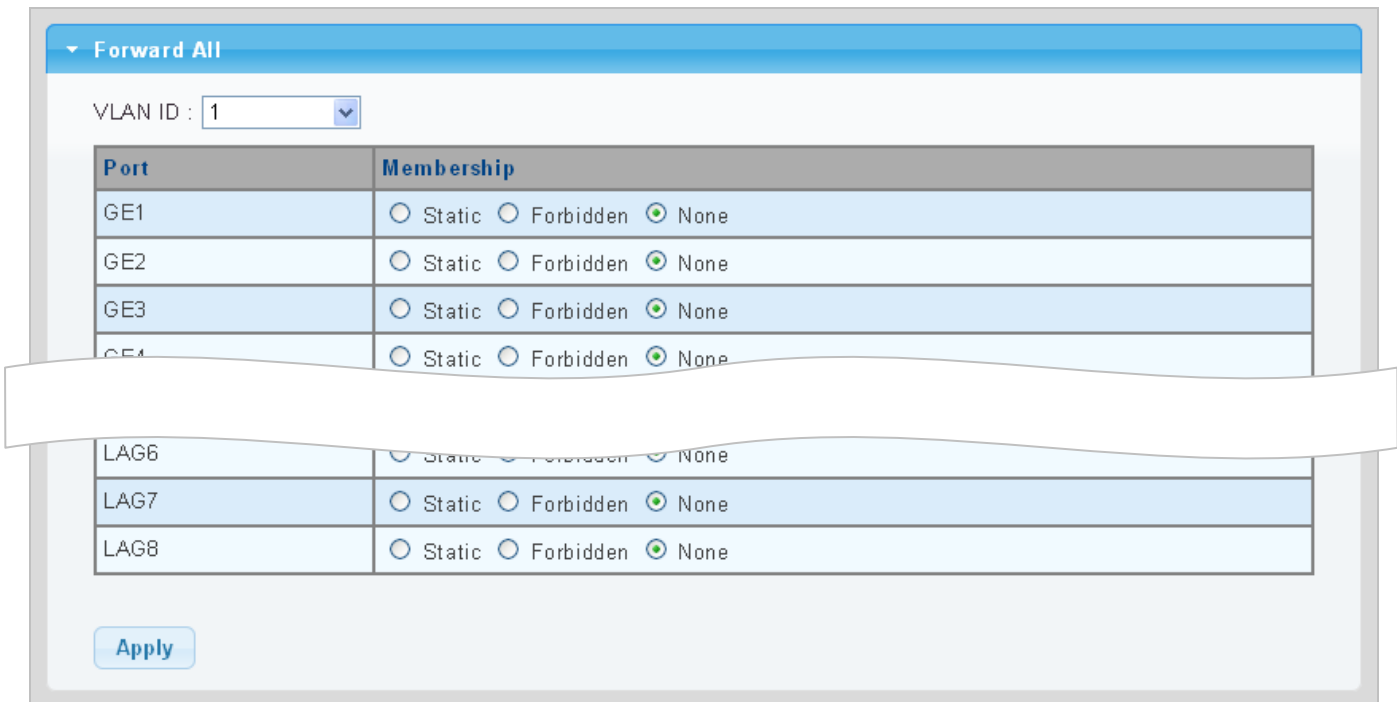


Figure 4-7-33: Forward All Setting Page Screenshot

The page includes the following fields:

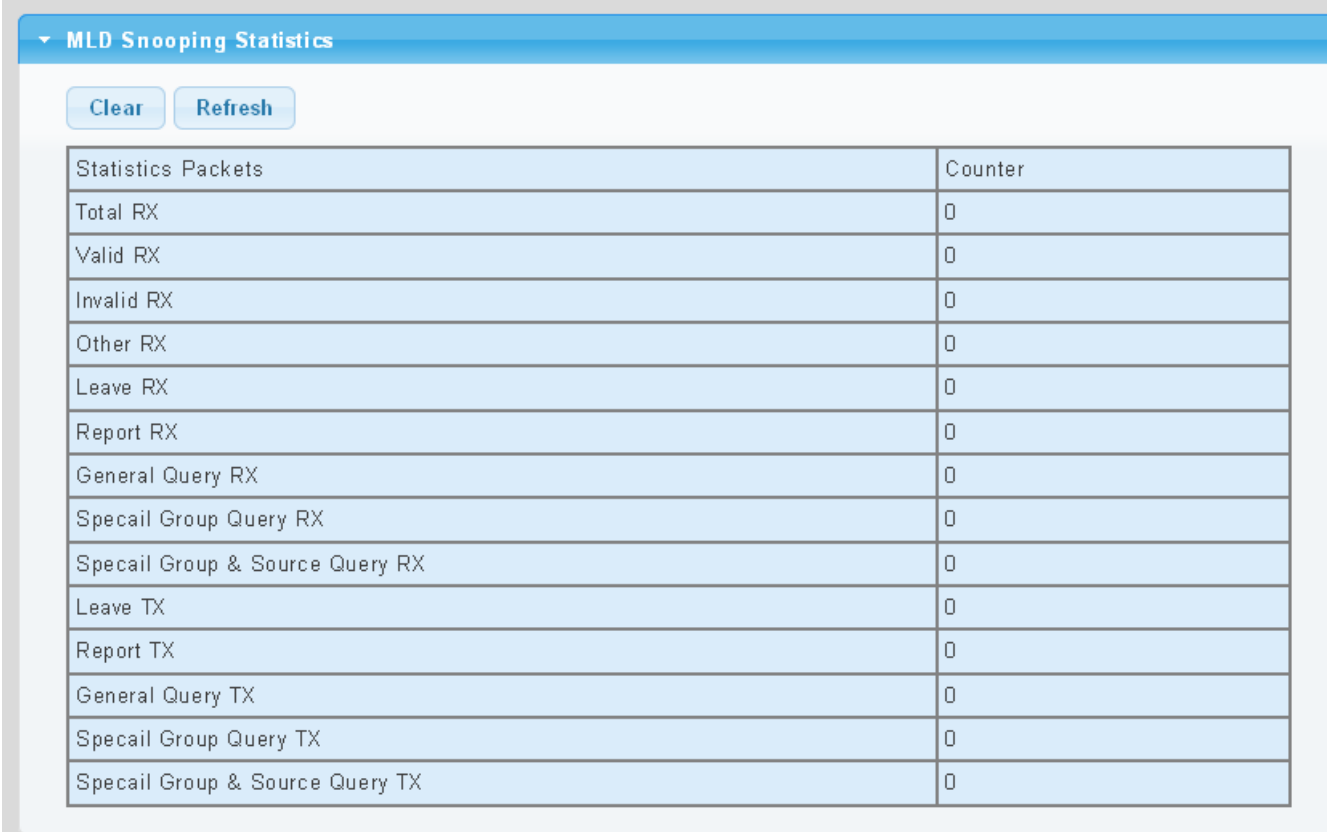
Object	Description	
• VLAN ID	Select VLAN ID for this drop down list to assign MLD membership.	
• Port	The switch port number of the logical port.	
• Membership	Select MLD membership for each interface:	
	Forbidden:	Interface is forbidden from automatically joining the MLD via MVR.
	None:	Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
	Static:	Interface is a member of the MLD.

Button

: Click to apply changes.

4.7.5 MLD Snooping Statics

This page provides MLD Snooping Statics. The MLD Snooping Statics screen in [Figure 4-7-34](#) appears.



Statistics Packets	Counter
Total RX	0
Valid RX	0
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Specail Group Query RX	0
Specail Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Specail Group Query TX	0
Specail Group & Source Query TX	0

Figure 4-7-34: Forward All Setting Page Screenshot

The page includes the following fields:

Object	Description
• Total RX	Display current total RX.
• Valid RX	Display current valid RX.
• Invalid RX	Display current invalid RX.
• Other RX	Display current other RX.
• Leave RX	Display current leave RX.
• Report RX	Display current report RX.
• General Query RX	Display current general query RX.
• Special Group Query RX	Display current special group query RX.
• Special Group & Source Query RX	Display current special group & source query RX.
• Leave TX	Display current leave TX.

• Report TX	Display current report TX.
• General Query TX	Display current general query TX.
• Special Group Query TX	Display current special group query TX.
• Special Group & Source Query TX	Display current special group & source query TX.

Buttons



: Click to clear the MLD Snooping Statistics.



: Click to refresh the MLD Snooping Statistics.

4.7.6 Multicast Throttling Setting

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

Once you have configured multicast profiles, you can assign them to interfaces on the Managed Switch. Also you can set the multicast throttling number to limit the number of multicast groups an interface can join at the same time. The MAX Group and Information screens in [Figure 4-7-35](#) and [Figure 4-7-36](#) appear.

IP Type	Port Select	Max Groups	Action
IPv4	Select Ports	256 (0-256)	<input checked="" type="radio"/> Deny <input type="radio"/> Replace

Apply

Figure 4-7-35: Max Groups and Action Setting Page Screenshot

The page includes the following fields:

Object	Description
• IP Type	Select IPv4 or IPv6 for this drop down list.
• Port Select	Select port number for this drop down list.
• Max Groups	Sets the maximum number of multicast groups an interface can join at the same time. Range: 0-256; Default: 256
• Action	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.

Button

: Click to apply changes.

IGMP Port Max Groups Information

Port	Max Groups	Action
GE1	256	Deny
GE2	256	Deny
GE3	256	Deny
GE4	256	Deny
GE5	256	Deny
GE6	256	Deny
GE7	256	Deny
GE8	256	Deny
GE9	256	Deny
GE10	256	Deny
GE11	256	Deny
GE12	256	Deny
GE13	256	Deny
GE14	256	Deny
GE15	256	Deny
GE16	256	Deny
GE17	256	Deny
GE18	256	Deny
GE19	256	Deny
GE20	256	Deny
GE21	256	Deny
GE22	256	Deny
GE23	256	Deny
GE24	256	Deny
GE25	256	Deny
GE26	256	Deny
LAG1	256	Deny
LAG2	256	Deny
LAG3	256	Deny
LAG4	256	Deny
LAG5	256	Deny
LAG6	256	Deny
LAG7	256	Deny
LAG8	256	Deny

Figure 4-7-36: IGMP Port Max Groups Information Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Max Groups	Display the current Max groups.
• Action	Display the current action.

4.7.7 Multicast Filter

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service is based on a specific subscription plan. The multicast filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port.

Multicast filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. A multicast filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, multicast join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the multicast join report is forwarded as normal. If a requested multicast group is denied, the multicast join report is dropped.

When you have created a Multicast profile number, you can then configure the multicast groups to filter and set the access mode.

Command Usage

- Each profile has only one access mode; either **permit** or **deny**.
- When the access mode is set to **permit**, multicast join reports are processed when a multicast group falls within the controlled range.
- When the access mode is set to **deny**, multicast join reports are only processed when the multicast group is not in the controlled range.

4.7.7.1 Multicast Profile Setting

The Add Profile and Profile Status screens in [Figure 4-7-37](#) and [Figure 4-7-38](#) appear.

Multicast Profile Setting

Add Profile


IP Type	IPv4 ▾
Profile Index	1 (1-128)
Group From	<input type="text"/>
Group To	<input type="text"/>
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny

Figure 4-7-37: Add Profile Setting Page Screenshot

The page includes the following fields:

Object	Description	
• IP Type	Select IPv4 or IPv6 for this drop down list.	
• Profile Index	Indicates the ID of this particular profile, the available range is 1 to 128.	
• Group from	Specifies multicast groups to include in the profile. Specify a multicast group range by entering a start IP address.	
• Group to	Specifies multicast groups to include in the profile. Specify a multicast group range by entering an end IP address.	
• Action	Sets the access mode of the profile; either permit or deny .	
	- Permit	Multicast join reports are processed when a multicast group falls within the controlled range.
	- Deny	When the access mode is set to, multicast join reports are only processed when the multicast group is not in the controlled range.

Button

: Click to add multicast profile entry.

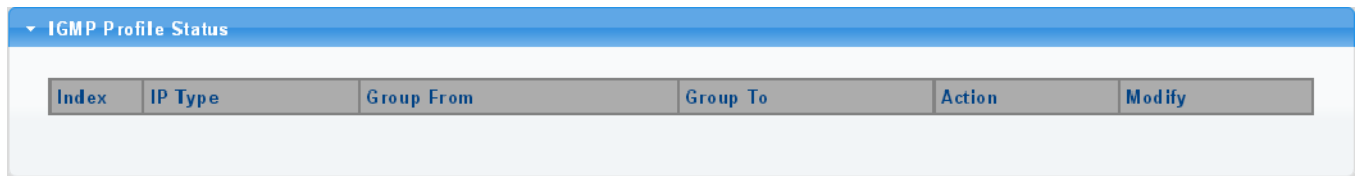




Figure 4-7-38: IGMP/MLD Profile Status Page Screenshot

The page includes the following fields:

Object	Description
• Index	Display the current index.
• IP Type	Display the current IP Type.
• Group From	Display the current group from.
• Group To	Display the current group to.
• Action	Display the current action.
• Modify	Click  to edit parameter.
	Click  to delete the IGMP profile entry.

4.7.7.2 IGMP Filter Setting

The Filter Setting and Status screens in [Figure 4-7-39](#) and [Figure 4-7-40](#) appear.

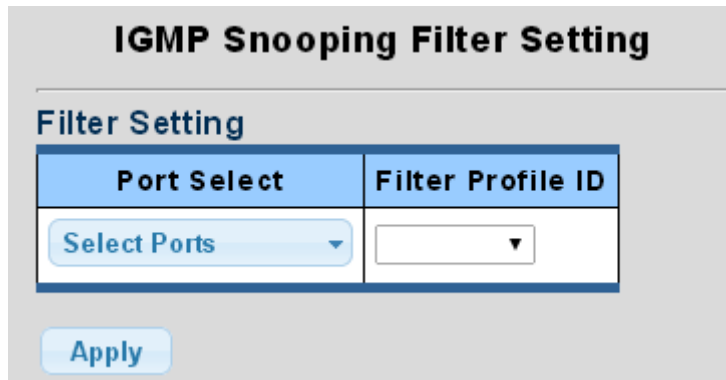



Figure 4-7-39: Filter Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port Select	Select port number for this drop down list.
• Filter Profile ID	Select filter profile ID for this drop down list.

Button

: Click to apply changes.

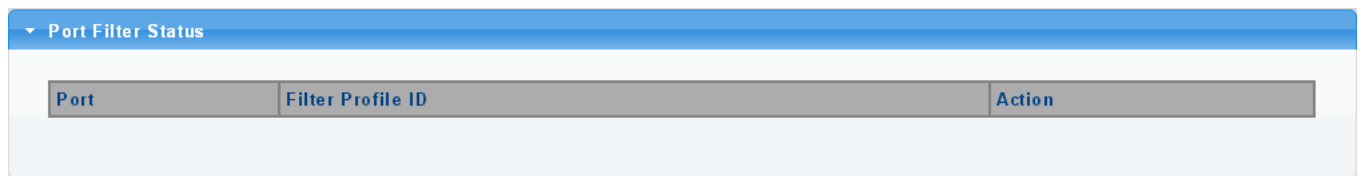




Figure 4-7-40: Port Filter Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	Display the current port
• Filter Profile ID	Display the current filter profile ID
• Action	Click  to display detail profile parameter. Click  to delete the IGMP filter profile entry.

4.7.7.3 MLD Filtering

The MLD Filtering Setting and Status screens in [Figure 4-7-41](#) and [Figure 4-7-42](#) appear.

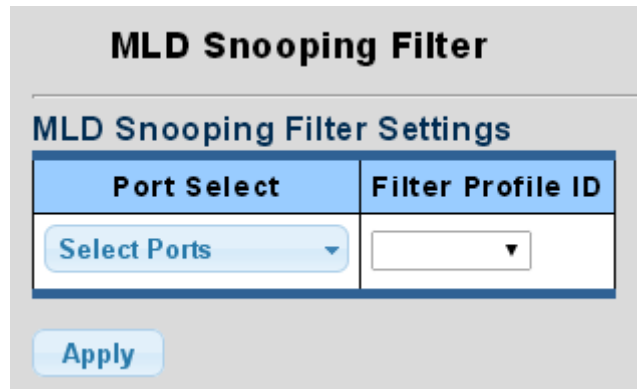



Figure 4-7-41: MLD Filter Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port Select 	Select port number for this drop down list.
<ul style="list-style-type: none"> • Filter Profile ID 	Select filter profile ID for this drop down list.

Button

: Click to apply changes.

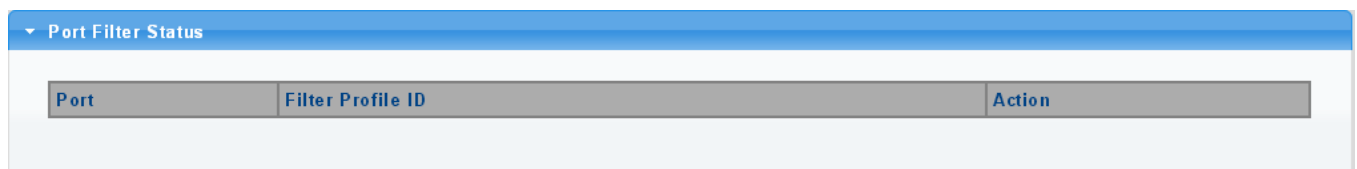




Figure 4-7-42: Port Filter Status Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	Display the current port
<ul style="list-style-type: none"> • Filter Profile ID 	Display the current filter profile ID
<ul style="list-style-type: none"> • Action 	Click  to display detail profile parameter Click  to delete the MLD filter profile entry

4.8 Quality of Service

4.8.1 Understand QoS

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

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

You can use QoS on your system to:

- Control a wide variety of network traffic by:
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

To implement QoS on your network, you need to carry out the following actions:

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

The **QoS** page of the Managed Switch contains three types of QoS mode - the **802.1p** mode, **DSCP** mode or **Port-base** mode can be selected. Both the three mode rely on predefined fields within the packet to determine the output queue.

- **802.1p Tag Priority Mode** –The output queue assignment is determined by the IEEE 802.1p VLAN priority tag.
- **IP DSCP Mode** - The output queue assignment is determined by the TOS or DSCP field in the IP packets.
- **Port-Base Priority Mode** – Any packet received from the specify high priority port will treated as a high priority packet.

The Managed Switch supports **eight priority level** queue, the queue service rate is based on the **WRR(Weight Round Robin)** and **WFQ (Weighted Fair Queuing)** alorithm. The WRR ratio of high-priority and low-priority can be set to "4:1 and 8:1.

4.8.2 General

4.8.2.1 QoS Properties

The QoS Global Setting and Information screens in [Figure 4-8-1](#) and [Figure 4-8-2](#) appear.

Figure 4-8-1: QoS Global Setting Page Screenshot

The page includes the following fields:

Object	Description
• QoS Mode	Enable or disable QoS mode.

Button


: Click to apply changes.

Figure 4-8-2: QoS Information Page Screenshot

The page includes the following fields:

Object	Description
• QoS Mode	Display the current QoS mode.

4.8.2.2 QoS Port Settings

The QoS Port Settings and Status screen in [Figure 4-8-3](#) & [Figure 4-8-4](#) appear.

Port	CoS Value	Remark CoS	Remark DSCP	Remark IP Precedence
Select Ports	0	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input checked="" type="radio"/> Disable <input type="radio"/> Enable


Apply

Figure 4-8-3: QoS Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port Select	Select port number for this drop down list.
• CoS Value	Select CoS value for this drop down list, the available options are 0 to 7.
• Remark CoS	Disable or enable remark CoS
• Remark DSCP	Disable or enable remark DSCP
• Remark IP Precedence	Disable or enable remark IP Precedence

Button

: Click to apply changes.

QoS Port Status				
Port	CoS Value	Remark CoS	Remark DSCP	Remark IP Precedence
GE1	0	Disabled	Disabled	Disabled
GE2	0	Disabled	Disabled	Disabled
GE3	0	Disabled	Disabled	Disabled
GE4	0	Disabled	Disabled	Disabled
GE5	0	Disabled	Disabled	Disabled
GE6	0	Disabled	Disabled	Disabled
GE7	0	Disabled	Disabled	Disabled
GE8	0	Disabled	Disabled	Disabled
GE9	0	Disabled	Disabled	Disabled
GE10	0	Disabled	Disabled	Disabled
GE11	0	Disabled	Disabled	Disabled
GE12	0	Disabled	Disabled	Disabled
GE13	0	Disabled	Disabled	Disabled
GE14	0	Disabled	Disabled	Disabled
GE15	0	Disabled	Disabled	Disabled
GE16	0	Disabled	Disabled	Disabled
GE17	0	Disabled	Disabled	Disabled
GE18	0	Disabled	Disabled	Disabled
GE19	0	Disabled	Disabled	Disabled
GE20	0	Disabled	Disabled	Disabled
GE21	0	Disabled	Disabled	Disabled
GE22	0	Disabled	Disabled	Disabled
GE23	0	Disabled	Disabled	Disabled
GE24	0	Disabled	Disabled	Disabled
GE25	0	Disabled	Disabled	Disabled
GE26	0	Disabled	Disabled	Disabled
LAG1	0	Disabled	Disabled	Disabled
LAG2	0	Disabled	Disabled	Disabled
LAG3	0	Disabled	Disabled	Disabled
LAG4	0	Disabled	Disabled	Disabled
LAG5	0	Disabled	Disabled	Disabled
LAG6	0	Disabled	Disabled	Disabled
LAG7	0	Disabled	Disabled	Disabled
LAG8	0	Disabled	Disabled	Disabled

Figure 4-8-4: QoS Port Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• CoS Value	Display the current CoS value.
• Remark CoS	Display the current remark CoS.
• Remark DSCP	Display the current remark DSCP.
• Remark IP Precedence	Display the current remark IP precedence.

4.8.2.3 Queue Settings

The Queue Table and Information screens in [Figure 4-8-5](#) and [Figure 4-8-6](#) appear.

Queue Settings				
Queue Table				
Queue	Scheduling Method			
	Strict Priority	WRR	Weight	% of WRR Bandwidth
1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="1"/>	
2	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="2"/>	
3	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="3"/>	
4	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="4"/>	
5	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="5"/>	
6	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="9"/>	
7	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="13"/>	
8	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="15"/>	

Figure 4-8-5: Queue Table Page Screenshot

The page includes the following fields:

Object	Description
• Queue	Display the current queue ID.
• Strict Priority	Controls whether the scheduler mode is "Strict Priority" on this switch port.
• WRR	Controls whether the scheduler mode is "Weighted" on this switch port.
• Weight	Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
• % of WRR Bandwidth	Display the current bandwidth for each queue.

Button

: Click to apply changes.

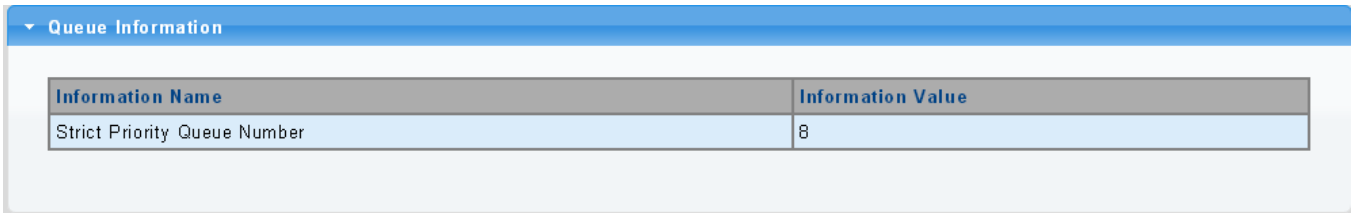


Figure 4-8-6: Queue Information Page Screenshot

The page includes the following fields:

Object	Description
• Information Name	Display the current queue method information.
• Information Value	Display the current queue vlaue information.

4.8.2.4 CoS Mapping

The CoS to Queue and Queue to CoS Mapping screens in Figure 4-8-7 and Figure 4-8-8 appear.

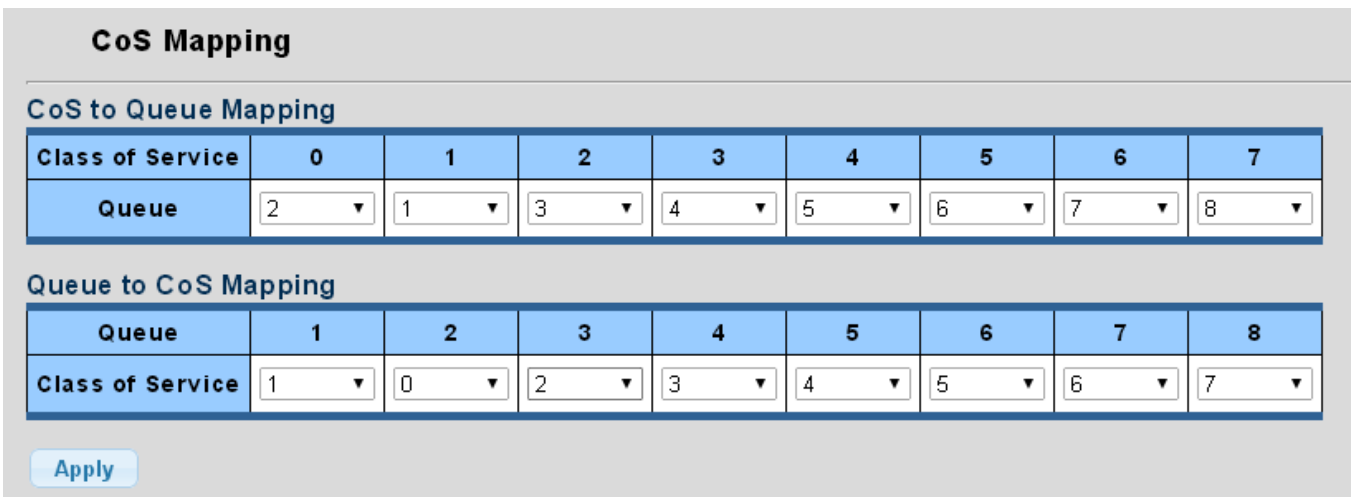


Figure 4-8-7: CoS to Queue and Queue to CoS Mapping Page Screenshot

The page includes the following fields:

Object	Description
• Queue	Select Queue value for this drop down list.
• Class of Service	Select CoS value for this drop down list.

Button



: Click to apply changes.

CoS	Mapping to Queue
0	2
1	1
2	3
3	4
4	5
5	5
6	7
7	5

Queue	Mapping to CoS
1	1
2	0
3	2
4	3
5	4
6	5
7	5
8	7

Figure 4-8-8: CoS Mapping Page Screenshot

The page includes the following fields:

Object	Description
• CoS	Display the current CoS value.
• Mapping to Queue	Display the current mapping to queue.
• Queue	Display the current queue value.
• Mapping to CoS	Display the current mapping to CoS.

4.8.2.5 DSCP Mapping

The DSCP to Queue and Queue to DSCP Mapping screens in [Figure 4-8-9](#) and [Figure 4-8-10](#) appear.

DSCP Mapping

DSCP to Queue Mapping

DSCP	Queue
Select DSCP ▼	1 ▼

Queue to DSCP Mapping

Queue	1	2	3	4	5	6	7	8
DSCP	0 ▼	8 ▼	16 ▼	24 ▼	32 ▼	40 ▼	48 ▼	56 ▼

Figure 4-8-9: DSCP to Queue and Queue to DSCP Mapping Page Screenshot

The page includes the following fields:

Object	Description
• Queue	Select Queue value for this drop down list.
• DSCP	Select DSCP value for this drop down list.

Button



: Click to apply changes.

DSCP Mapping	
DSCP	Mapping to Queue
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	2
9	2
10	2
11	2
12	2
13	2
14	2
15	2
16	3
17	3
18	3
19	3
20	3
21	3
22	3
23	3
24	4
25	4
26	4
27	4
28	4
29	4
30	4
31	4
32	5
33	5
34	5
35	5
36	5
37	5
38	5
39	5
40	6
41	6
42	6
43	6
44	6
45	6
46	6
47	6
48	7
49	7
50	7
51	7
52	7
53	7
54	7
55	7
56	8
57	8
58	8
59	8
60	8
61	8
62	8
63	8

Queue	Mapping to DSCP
1	0
2	8
3	16
4	24
5	32
6	40
7	48
8	56

Figure 4-8-10: DSCP Mapping Page Screenshot

The page includes the following fields:

Object	Description
• DSCP	Display the current CoS value.
• Mapping to Queue	Display the current mapping to queue.
• Queue	Display the current queue value.
• Mapping to DSCP	Display the current mapping to DSCP.

4.8.2.6 IP Precedence Mapping

The IP Precedence to Queue and Queue to IP Precedence Mapping screens in [Figure 4-8-11](#) and [Figure 4-8-12](#) appear.

IP Precedence Mapping

IP Precedence to Queue Mapping

IP Precedence	0	1	2	3	4	5	6	7
Queue	1 ▾	2 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾	8 ▾

Queue to IP Precedence Mapping

Queue	1	2	3	4	5	6	7	8
IP Precedence	0 ▾	1 ▾	2 ▾	3 ▾	4 ▾	5 ▾	6 ▾	7 ▾

Figure 4-8-11: IP Precedence to Queue and Queue to IP Precedence Mapping Page Screenshot

The page includes the following fields:

Object	Description
• Queue	Select Queue value for this drop down list.
• IP Precedence	Select IP Precedence value for this drop down list.

Button

: Click to apply changes.

IP Precedence Mapping	
IP Precedence	Mapping to Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

Queue	Mapping to IP Precedence
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

Figure 4-8-12: IP Precedence Mapping Page Screenshot

The page includes the following fields:

Object	Description
• IP Precedence	Display the current CoS value.
• Mapping to Queue	Display the current mapping to queue.
• Queue	Display the current queue value.
• Mapping to IP Precedence	Display the current mapping to IP Precedence.

4.8.3 QoS Basic Mode

4.8.3.1 Global Settings

The Basic Mode Global Settings and QoS Information screens in [Figure 4-8-13](#) and [Figure 4-8-14](#) appear.

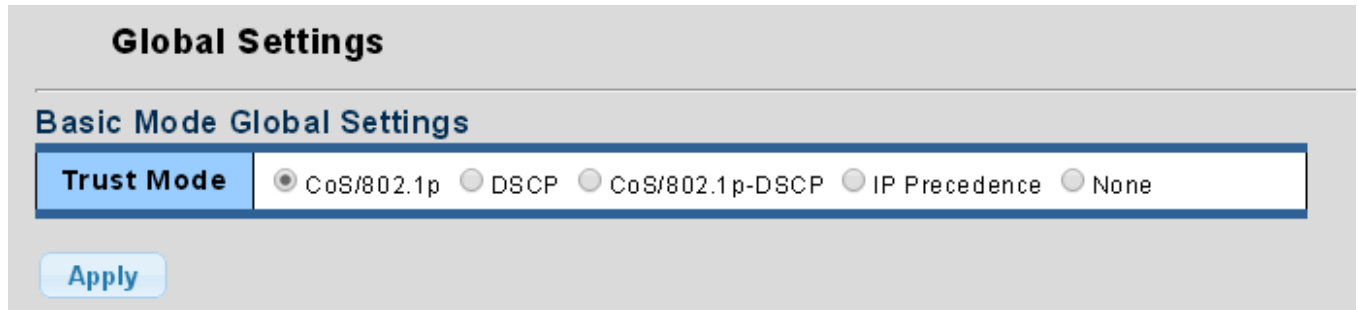


Figure 4-8-13: Basic Mode Global Settings Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Trust Mode 	Set the QoS mode, the optios are shown as below: Cos/802.1p (Default) DSCP CoS/802.1p-DSCP IP Precedence None

Button

Apply: Click to apply changes.

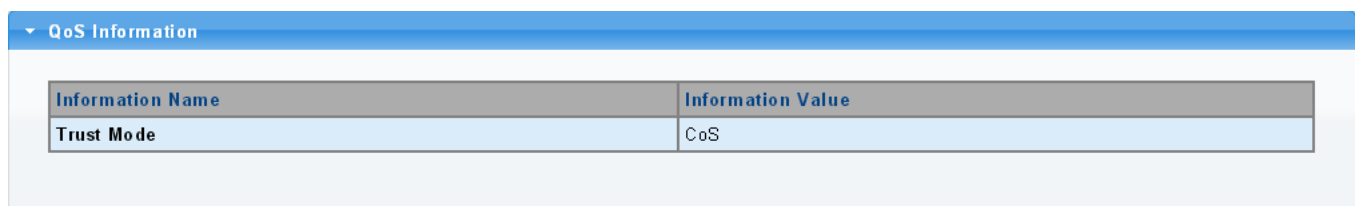


Figure 4-8-14: QoS Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Trust Mode 	Display the current QoS mode.

4.8.3.2 Port Settings

The QoS Port Setting and Status screens in [Figure 4-8-15](#) and [Figure 4-8-16](#) appear.

QoS Port Setting

QoS Port Setting

Port	Trust
Select Ports	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled


Apply

Figure 4-8-15: Basic Mode Global Settings Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port number for this drop down list.
• Trust	Enable or disable the trust mode.

Button

: Click to apply changes.

QoS Port Status	
Port	Trust Type
GE1	Enabled
GE2	Enabled
GE3	Enabled
GE4	Enabled
GE5	Enabled
GE6	Enabled
GE7	Enabled
GE8	Enabled
GE9	Enabled
GE10	Enabled
GE11	Enabled
GE12	Enabled
GE13	Enabled
GE14	Enabled
GE15	Enabled
GE16	Enabled
GE17	Enabled
GE18	Enabled
GE19	Enabled
GE20	Enabled
GE21	Enabled
GE22	Enabled
GE23	Enabled
GE24	Enabled
GE25	Enabled
GE26	Enabled
LAG1	Enabled
LAG2	Enabled
LAG3	Enabled
LAG4	Enabled
LAG5	Enabled
LAG6	Enabled
LAG7	Enabled
LAG8	Enabled

Figure 4-8-16: QoS Port Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Trust Type	Display the current trust type.

4.8.4 QoS Advanced Mode

4.8.4.1 Global Settings

The Advanced Mode Global Settings and QoS Information screens in [Figure 4-8-17](#) and [Figure 4-8-18](#) appear.

The screenshot shows a web interface titled "Global Settings" with a sub-section "Advanced Mode Global Settings". It contains two main settings:

- Trust Mode:** A blue header box with radio button options: CoS/802.1p (selected), DSCP, CoS/802.1p-DSCP, and IP Precedence.
- Default Mode Status:** A blue header box with radio button options: Trusted and Not Trusted (selected).

An "Apply" button is located at the bottom left of the settings area.

Figure 4-8-17: Advanced Mode Global Settings Page Screenshot

The page includes the following fields:

Object	Description
• Trust Mode	Set the QoS mode, the optios are shown as below: Cos/802.1p (Default) DSCP CoS/802.1p-DSCP IP Precedence
• Default Mode Status	Set the default mode as “Trusted” or “Not Trusted” (Default).

Button

: Click to apply changes.

The screenshot shows a "QoS Information" section with a table displaying the current settings:

Information Name	Information Value
Trust Mode	CoS
Default Mode Status	Not Trusted

Figure 4-8-18: QoS Information Page Screenshot

The page includes the following fields:

Object	Description
• Trust Mode	Display the current QoS mode.
• Default Mode Status	Disaply the current default mode status.

4.8.4.2 Class Mapping

The QoS Class Mapping and Class Mapping status screens in [Figure 4-8-19](#) and [Figure 4-8-20](#) appear.

The screenshot shows a 'Class Configuration' form with the following fields:

- Class Name:** A text input field.
- Match ACL Type:** Radio buttons for IP, MAC, and IP or MAC.
- IP:** Checkboxes for IPv4 and IPv6, each followed by a dropdown menu.
- MAC:** A dropdown menu.
- Preferred ACL:** Radio buttons for IP and MAC.

An 'Add' button is located at the bottom left of the form.

Figure 4-8-19: QoS Class Mapping Page Screenshot

The page includes the following fields:

Object	Description
• Class Name	Input the class name and 32 characters allowed.
• Match ACL Type	Choose "IP", "MAC" or "IP or MAC" as match ACL type.
• IP	Choose "IPv4" or "IPv6".
• MAC	Choose specific MAC address.
• Preferred ACL	Choose "IP" or "MAC" for preferred ACL.

Button

Add: Click to add Class Mapping profile entry.

The screenshot shows a table titled 'Class Table' with the following structure:

Class Name	Match	Action
------------	-------	--------

Figure 4-8-20: QoS Class Mapping Table Page Screenshot

The page includes the following fields:

Object	Description
• Class Name	Display the current class name.
• Match	Display the current match information.
• Action	Display the current action information.

4.8.4.3 Aggregate Police


The QoS Aggregate Police and Aggregate Police status screens in [Figure 4-8-21](#) and [Figure 4-8-22](#) appear.

Figure 4-8-21: QoS Aggregate Police Page Screenshot

The page includes the following fields:

Object	Description
• Aggregate Police Name	Input the aggregate police name and 32 characters allowed.
• Ingress Committed Information Rate (CIR)	Allow input a number as ingress committed information rate.
• Ingress Committed Burst Size (CBS)	Allow input a number as ingress committed burst size.
• Exceed Action	Choose “Forward” or “Drop” when the exceed action situation appears.

Button

: Click to add aggregate police profile entry.

Police Name	Ingress CIR	Ingress CBS	Exceed Action	Action
-------------	-------------	-------------	---------------	--------

Figure 4-8-22: QoS Aggregate Police Table Page Screenshot

The page includes the following fields:

Object	Description
• Police Name	Display the current policer name.
• Ingress CIR	Display the current Ingress CIR information.
• Ingress CBS	Display the current Ingress CBS information.
• Exceed Action	Display the current exceed action information.
• Action	Display the current action information.

4.8.4.4 Policy Table

The QoS Policy table and Policy table status screens in [Figure 4-8-23](#) and [Figure 4-8-24](#) appear.

Figure 4-8-23: QoS Policy Table Page Screenshot

The page includes the following fields:

Object	Description
• Policy Name	Input the policy name and 31 characters allowed.

Button




: Click to add policy profile entry.

Policy Name	Delete
-------------	--------

Figure 4-8-24: QoS Policy Table Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Policy Name 	Display the current policy name.
<ul style="list-style-type: none"> • Delete 	Click  to delete the policy name profile entry.

4.8.4.5 Policy Class Maps

The QoS policy class maps and policy class maps status screens in [Figure 4-8-25](#) and [Figure 4-8-26](#) appear.

Policy Class Maps

Policy Class Configuration

Policy Name	<input type="text"/>
Class Name	<input type="text" value="2"/>
Action Type	<input checked="" type="radio"/> Trust None <input type="radio"/> Always Trust <input type="radio"/> Set Queue <input type="text" value="1"/>
Police Type	<input checked="" type="radio"/> None <input type="radio"/> Single <input type="radio"/> Aggregate
Aggregate Police	<input type="text"/>
Ingress Committed Information Rate (CIR)	<input type="text" value="16"/> KBits/s
Ingress Committed Burst Size (CBS)	<input type="text" value="128"/> Bytes
Exceed Action	<input checked="" type="radio"/> Forward <input type="radio"/> Drop

Figure 4-8-25: QoS Policy Class Maps Table Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Policy Name 	Allow choose one specific policy name.
<ul style="list-style-type: none"> • Class Name 	Allow choose one specific class name.
<ul style="list-style-type: none"> • Action Type 	Provide “Trust None”, “Always Trust” and “Set Queue” options.
<ul style="list-style-type: none"> • Police Type 	Provide “None”, “Single” and “Aggregate” options.
<ul style="list-style-type: none"> • Aggregate Police 	Allow choose one specific aggregate police profile.
<ul style="list-style-type: none"> • Ingress Committed 	Allow input a number as ingress committed information rate.

Information Rate (CIR)	
• Ingress Committed Burst Size (CBS)	Allow input a number as ingress committed burst size.
• Exceed Action	Choose "Forward" or "Drop" when the exceed action situation appears.

Button



: Click to add policy class maps profile entry.



Policy Name	Class Name	Action Type			Police Type	Aggregate Police Name	CIR	CBS	Exceed Action	Modify
		Trust	Set Attribute	Set Value						

Figure 4-8-26: QoS Policy Class Map Table Page Screenshot

The page includes the following fields:

Object	Description
• Policy Name	Display the current policy name information.
• Class Name	Display the current class name information.
• Action Type	Display current "Trust", "Set Attribute" and "Set Value" information.
• Police Type	Display current policy type information.
• Aggregate Police Name	Display current Aggregate Police Name information.
• CIR	Display current CIR information.
• CBS	Display current CBS information.
• Exceed Action	Display current exceed action information.
• Modify	<p>Click  to edit parameter.</p> <p>Click  to delete the policy class maps profile entry.</p>

4.8.4.6 Policy Binding

The QoS policy binding and policy binding table screens in [Figure 4-8-27](#) and [Figure 4-8-28](#) appear.


The screenshot shows a web interface for configuring QoS policy binding. At the top, there is a header 'Policy Binding'. Below it, a sub-section 'Policy Binding' contains two columns. The first column is labeled 'Policy Select' and has a dropdown menu. The second column is labeled 'Binding Port' and has a dropdown menu with a 'Select Ports' button next to it. Below these two columns is a blue 'Apply' button.

Figure 4-8-27: QoS Policy Binding Table Page Screenshot

The page includes the following fields:

Object	Description
• Policy Select	Select policy from this drop down list.
• Binding Port	Select one specific port from this drop down list.

Button

: Click to apply changes.

Policy Binding Table	
Port	Policy Name
GE1	
GE2	
GE3	
GE4	
GE5	
GE6	
GE7	
GE8	
GE9	
GE10	
GE11	
GE12	
GE13	
GE14	
GE15	
GE16	
GE17	
GE18	
GE19	
GE20	
GE21	
GE22	
GE23	
GE24	
GE25	
GE26	
LAG1	
LAG2	
LAG3	
LAG4	
LAG5	
LAG6	
LAG7	
LAG8	

Figure 4-8-28: QoS Policy Binding Table Page Screenshot

The page includes the following fields:

Object	Description
• Port	Display per port information.
• Policy Name	Display the current policy name information.

4.8.5 Rate Limit

Configure the switch port rate limit for the switch port on this page.

4.8.5.1 Ingress Bandwidth Control

This page provides to select the ingress bandwidth preamble. The Ingress Bandwidth Control Setting and Status screens in [Figure 4-8-29](#), [Figure 4-8-30](#) and [Figure 4-8-31](#) appear.

Figure 4-8-29: Ingress Bandwidth Control Settings Page Screenshot

The page includes the following fields:

Object	Description
• Burst Size	Allow assigning burst size and the options are 1 to 65535. Unit: Bytes.
• Port	Select port number for this drop down list.
• State	Enable or disable the port rate policer. The default value is "Disabled".
• Rate (Kbps)	Configure the rate for the port policer. The default value is "unlimited". Valid values are in the range 0 to 1000000, must a multiple of 16.

Button

: Click to apply changes.

Figure 4-8-30: Ingress Port Burst Size Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Burst Size	Display current burst size information.

▼ Ingress Bandwidth Control Status

Port	Ingress Rate Limit (Kbps)
GE1	Off
GE2	Off
GE3	Off
GE4	Off
GE5	Off
GE6	Off
GE7	Off
GE8	Off
GE9	Off
GE10	Off
GE11	Off
GE12	Off
GE13	Off
GE14	Off
GE15	Off
GE16	Off
GE17	Off
GE18	Off
GE19	Off
GE20	Off
GE21	Off
GE22	Off
GE23	Off
GE24	Off
GE25	Off
GE26	Off
LAG1	Off
LAG2	Off
LAG3	Off
LAG4	Off
LAG5	Off
LAG6	Off
LAG7	Off
LAG8	Off

Figure 4-8-31: Ingress Bandwidth Control Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Ingress Rate Limit (Kbps)	Display the current ingress rate limit.

4.8.5.2 Ingress VLAN Settings

This page provides to select the VLAN ingress bandwidth preamble. The VLAN Ingress Bandwidth Control Setting and Status screens in [Figure 4-8-32](#) and [Figure 4-8-33](#) appear.

Figure 4-8-32: VLAN Ingress Bandwidth Control Settings Page Screenshot

The page includes the following fields:

Object	Description
• VLAN	Select VLAN number for this drop down list.
• Port	Select port number for this drop down list.
• State	Enable or disable the port rate policer. The default value is "Disabled".
• Rate (Kbps)	Configure the rate for the VLAN ingress bandwidth. The default value is "unlimited". Valid values are in the range 0 to 1000000, must a multiple of 16.

Button

: Click to apply changes.

Figure 4-8-33: VLAN Ingress Bandwidth Control Status Page Screenshot

The page includes the following fields:

Object	Description
• VLAN	Display the VLAN group information.
• Port	The switch port number of the logical port.
• Rate (Kbps)	Display the current ingress rate limit.

4.8.5.3 Egress Bandwidth Control

This page provides to select the egress bandwidth preamble. The Egress Bandwidth Control Setting and Status screens in [Figure 4-8-34](#), [Figure 4-8-35](#) and [Figure 4-8-36](#) appear.

Figure 4-8-34: Egress Bandwidth Control Settings Page Screenshot

The page includes the following fields:

Object	Description
• Burst Size	Allow assigning burst size and the options are 1 to 65535. Unit: Bytes.
• Port	Select port number for this drop down list.
• State	Enable or disable the port rate policer. The default value is "Disabled".
• Rate (Kbps)	Configure the rate for the port policer. The default value is "unlimited". Valid values are in the range 0 to 1000000, must a multiple of 16.

Button

: Click to apply changes.

Egress Port Burst Size Configuration	
Information Name	Information Value
Burst Size	32768 Bytes

Figure 4-8-35: Egress Port Burst Size Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Burst Size	Display current burst size information.

Egress Bandwidth Control Status	
Port	Egress Rate Limit (Kbps)
GE1	Off
GE2	Off
GE3	Off
GE4	Off
GE5	Off
GE6	Off
GE7	Off
GE8	Off
GE9	Off
GE10	Off
GE11	Off
GE12	Off
GE13	Off
GE14	Off
GE15	Off
GE16	Off
GE17	Off
GE18	Off
GE19	Off
GE20	Off
GE21	Off
GE22	Off
GE23	Off
GE24	Off
GE25	Off
GE26	Off
LAG1	Off
LAG2	Off
LAG3	Off
LAG4	Off
LAG5	Off
LAG6	Off
LAG7	Off
LAG8	Off

Figure 4-8-36: Egress Bandwidth Control Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Egress Rate Limit (Kbps)	Display the current egress rate limit.

4.8.5.4 Egress Queue Settings

The Egress Queue Bandwidth Control Settings and Status screens in [Figure 4-8-37](#), [Figure 4-8-38](#) and [Figure 4-8-39](#) appear.

Figure 4-8-37: Egress Queue Bandwidth Settings Page Screenshot

The page includes the following fields:

Object	Description
• Burst Size	Allow assigning burst size and the options are 1 to 65535. Unit: Bytes.
• Port	Select port number for this drop down list.
• Queue	Select queue numbers for this drop down list, options are 1 to 8.
• State	Enable or disable the port rate policer. The default value is "Disabled".
• CIR (Kbps)	Configure the CIR for the port policer. The default value is "unlimited". Valid values are in the range 0 to 1000000, must a multiple of 16.

Button

Apply: Click to apply changes.

Figure 4-8-38: Egress Port Burst Size Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Burst Size 	Display current burst size information.

GE1 Egress Per Queue Status

Queue ID	Rate Limit (Kbps)
1	Off
2	Off
3	Off
4	Off
5	Off
6	Off
7	Off
8	Off

Figure 4-8-39: Egress Queue Status Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Queue ID 	Display the current queue ID.
<ul style="list-style-type: none"> • Rate Limit (Kbps) 	Display the current rate limit.

4.8.6 Voice VLAN

4.8.6.1 Introduction to Voice VLAN

Configure the switch port rate limit for the switch port on this page.

Voice VLAN is specially configured for the user voice data traffic. By setting a Voice VLAN and adding the ports of the connected voice equipments to Voice VLAN, the user will be able to configure QoS (Quality of service) service for voice data, and improve voice data traffic transmission priority to ensure the calling quality.

The switch can judge if the data traffic is the voice data traffic from specified equipment according to the source MAC address field of the data packet entering the port. The packet with the source MAC address complying with the system defined voice equipment **OUI (Organizationally Unique Identifier)** will be considered the voice data traffic and transmitted to the Voice VLAN.

The configuration is based on MAC address, acquiring a mechanism in which every voice equipment transmitting information through the network has got its unique MAC address. VLAN will trace the address belongs to specified MAC. By This means, VLAN allows the voice equipment always belong to Voice VLAN when relocated physically. The greatest advantage of the VLAN is the equipment can be automatically placed into Voice VLAN according to its voice traffic which will be transmitted at specified priority. Meanwhile, when voice equipment is physically relocated, it still belongs to the Voice VLAN without any further configuration modification, which is because it is based on voice equipment other than switch port.



The Voice VLAN feature enables the voice traffic to forward on the Voice VLAN, and then the switch can be classified and scheduled to network traffic. **It is recommended there are two VLANs on a port** -- one for voice, one for data.



Before connecting the IP device to the switch, **the IP phone should configure the voice VLAN ID correctly**. It should be configured through its own GUI.

4.8.6.2 Properties

The Voice VLAN feature enables voice traffic to forward on the Voice VLAN, and then the switch can be classified and scheduled to network traffic. It is recommended that there are two VLANs on a port -- one for voice, one for data.

Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI. This page provides to select the ingress bandwidth preamble. The Ingress Bandwidth Control Setting/Status screens in [Figure 4-8-40](#) and [Figure 4-8-41](#) appears.

Properties	
Properties Settings	
Voice VLAN State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Voice VLAN ID	Default(1) ▼
Remark Cos/802.1p	6 ▼
1p Remark	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Aging Time(30-65536 min)	1440
<input type="button" value="Apply"/>	

Figure 4-8-40: Voice VLAN Properties Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Voice VLAN State 	<p>Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter. Possible modes are:</p> <ul style="list-style-type: none"> ■ Enabled: Enable Voice VLAN mode operation. ■ Disabled: Disable Voice VLAN mode operation
<ul style="list-style-type: none"> • Voice VLAN ID 	<p>Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is conflict configuration if the value equal management VID, MVR VID, PVID, etc.</p> <p>The allowed range is 1 to 4095.</p>
<ul style="list-style-type: none"> • Remark CoS/802.1p 	Select 802.1p value for this drop down list
<ul style="list-style-type: none"> • 1p remark 	Enable or disable 802.1p remark
<ul style="list-style-type: none"> • Aging Time (30-65536 min) 	The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. (\Default: 1440 minutes).

Button

: Click to apply changes.

Voice VLAN State	
Information Name	Information Value
Voice VLAN State	Disabled
Voice VLAN ID	1
Remark Cos/802.1p	6
1p Remark State	Disabled
Aging	1440

Figure 4-8-41: Voice VLAN State Page Screenshot

The page includes the following fields:

Object	Description
• Voice VLAN State	Display the current voice VLAN state.
• Voice VLAN ID	Display the current voice VLAN ID.
• Remark CoS/802.1p	Display the current remark CoS/802.1p.
• 1p remark	Display the current 1p remark.
• Aging	Display the current aging time.

4.8.6.3 Telephony OUI MAC Setting

Configure Voice VLAN OUI table on this Page. The Telephony OUI MAC Setting screens in [Figure 4-8-42](#) and [Figure 4-8-43](#) appear.

Telephony OUI MAC

Voice VLAN OUI MAC Setting


OUI Address	<input style="width: 90%;" type="text" value="00:00:00"/>
Description	<input style="width: 90%;" type="text"/>

Figure 4-8-42: Voice VLAN OUI MAC Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • OUI Address 	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx:xx:xx" (x is a hexadecimal digit).
<ul style="list-style-type: none"> • Description 	User-defined text that identifies the VoIP devices.

Button

: Click to add voice VLAN OUI setting.

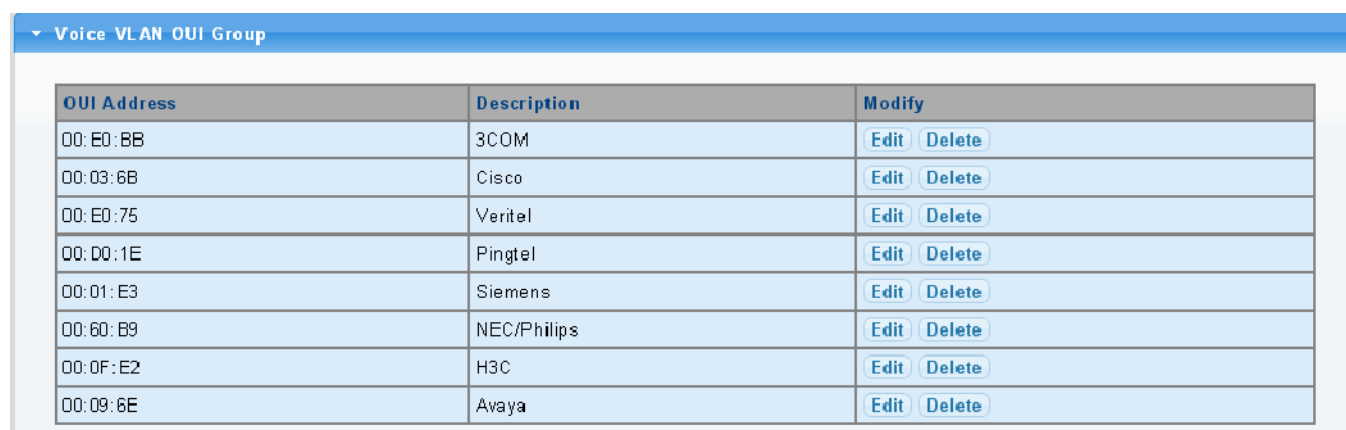




Figure 4-8-43: Voice VLAN OUI Group Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • OUI Address 	Display the current OUI address.
<ul style="list-style-type: none"> • Description 	Display the current description.
<ul style="list-style-type: none"> • Modify 	<p>Click  to edit voice VLAN OUI group parameter.</p> <p>Click  to delete voice VLAN OUI group parameter.</p>

4.8.6.4 Telephony OUI Port Setting

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI. The Telephony OUI MAC Setting screens in [Figure 4-8-44](#) and [Figure 4-8-45](#) appear.

Port	State	Cos Mode
Select Ports	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	<input type="radio"/> All <input checked="" type="radio"/> Src


Apply

Figure 4-8-44: Voice VLAN OUI Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port number for this drop down list.
• State	Enable or disable the voice VLAN port setting. The default value is "Disabled".
• CoS Mode	Select the current CoS mode.

Button

: Click to apply changes.

Port	State	Cos Mode
GE1	Disabled	Src
GE2	Disabled	Src
GE3	Disabled	Src
GE4	Disabled	Src
LAG6		Src
LAG7	Disabled	Src
LAG8	Disabled	Src

Figure 4-8-45: Voice VLAN Port State Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• State	Display the current state.
• CoS Mode	Display the current CoS mode.

4.9 Security

This section is to control the access of the Managed Switch, including the user access and management control.

The Security Page contains links to the following main topics:

- **Strom Control**
- **802.1x**
- **DHCP Snooping**
- **Dynamic ARP Inspection**
- **IP Source Guard**
- **Port Security**
- **DoS**
- **AAA**
- **TACACS+ Server**
- **Radius Server**
- **Access**

4.9.1 Storm Control

Storm control for the switch is configured on this Page.

There is an unknown unicast storm rate control, unknown multicast storm rate control, and a broadcast storm rate control.

These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

4.9.1.1 Global Setting

The Storm Control Global Setting and Information screens in [Figure 4-9-1](#) and [Figure 4-9-2](#) appear.

Storm Control Global

Storm Control Global Setting

Unit	<input checked="" type="radio"/> pps <input type="radio"/> bps
Preamble & IFG	<input checked="" type="radio"/> Excluded <input type="radio"/> Included

Apply

Figure 4-9-1: Storm Control Global Setting Page Screenshot

The page includes the following fields:

Object	Description
• Unit	Controls the unit of measure for the storm control rate as "pps" or "bps". The default value is "bps".
• Preamble & IFG	Set the excluded or included interframe gap

Button

Apply: Click to apply changes.

Storm Control Global Information	
Information Name	Information Value
Unit	bps
Preamble & IFG	Excluded

Figure 4-9-2: Storm Control Global Information Page Screenshot

The page includes the following fields:

Object	Description
• Unit	Display the current unit.
• Preamble & IFG	Display the current preamble & IFG.

4.9.1.2 Port Setting

Storm control for the switch is configured on this page. There are three types of storm rate control:

- **Broadcast** storm rate control
- **Unknown Unicast** storm rate control
- **Unknown Multicast** storm rate control.

The configuration indicates the permitted packet rate for unknown unicast, unknown multicast, or broadcast traffic across the switch. The Storm Control Configuration screens in [Figure 4-9-3](#) and [Figure 4-9-4](#) appear.

Storm Control				
Storm Control Setting				
Port	Port State	Action	Type Enable	Rate (unit:16Kbps)
Select Ports	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	Drop	<input type="checkbox"/> Broadcast	10000
			<input type="checkbox"/> Unknown Multicast	10000
			<input type="checkbox"/> Unknown Unicast	10000

Apply

Figure 4-9-3: Storm Control Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port for this drop down list.
• Port State	Enable or disable the storm control status for the given storm type.
• Action	Configures the action performed when storm control is over rate on a port. Valid values are Shutdown or Drop .
• Type Enable	The settings in a particular row apply to the frame type listed here: <ul style="list-style-type: none"> ■ Broadcast ■ Unknown Multicast ■ Unknown Unicast
• Rate (kbps/pps)	Configure the rate for the storm control. The default value is "10,000" and unit is 16Kbps.

Button

: Click to apply changes.

▼ Storm Control Information

Port	Port State	Broadcast (16Kbps)	Unknown Multicast (16Kbps)	Unknown Unicast (16Kbps)	Action
GE1	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE2	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE3	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE4	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE5	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE6	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE7	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE8	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE9	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE10	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE11	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE12	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE13	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE14	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE15	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE16	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE17	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE18	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE19	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE20	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE21	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE22	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE23	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE24	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE25	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE26	disabled	Off (10000)	Off (10000)	Off (10000)	Drop

Figure 4-9-4: Storm Control Information Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Port State	Display the current port state.
• Broadcast (16Kbps)	Display the current brocast storm control rate.
• Unknown Multicast (16Kbps)	Display the current unknown multicast storm control rate.
• Unknown Unicast (16Kbps)	Display the current unknown unicast storm control rate.
• Action	Display the current action.

4.9.2 802.1X

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.

Overview of User Authentication

It is allowed to configure the Managed Switch to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and Web browser. This Managed Switch provides secure network management access using the following options:

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

4.9.2.1 Understanding IEEE 802.1X Port-based Authentication

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

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

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange
- Ports in Authorized and Unauthorized States

■ Device Roles

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

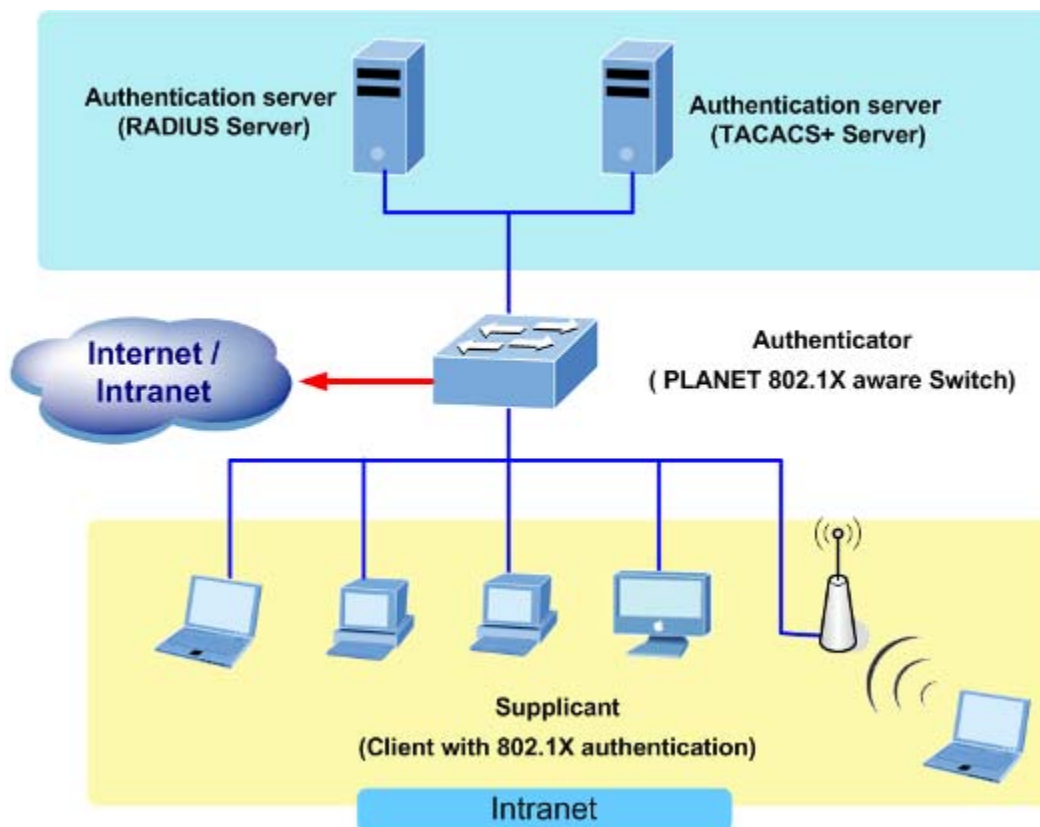


Figure 4-9-5

- **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 4-9-6](#)” shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

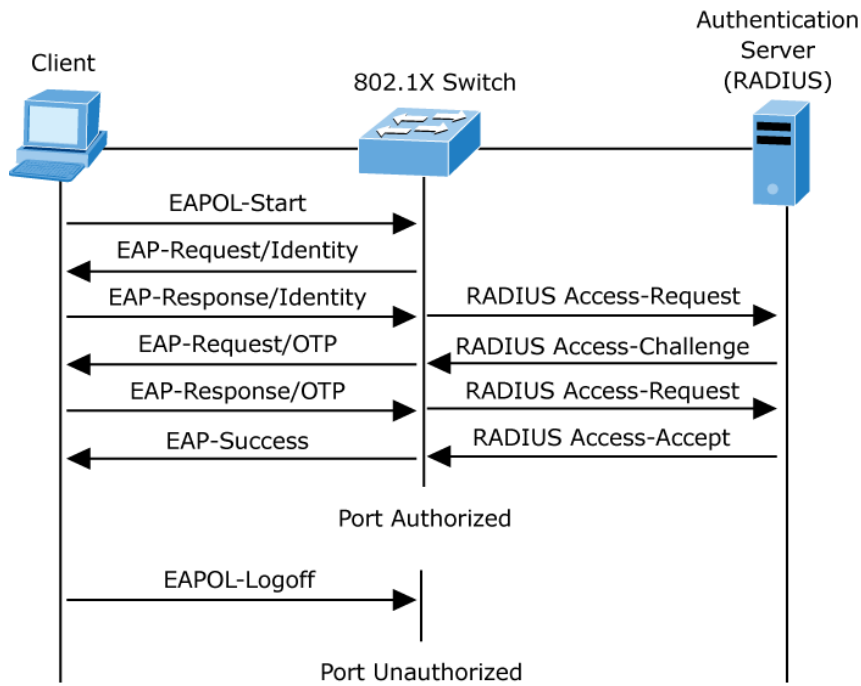


Figure 4-9-6: EAP Message Exchange

■ 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.

4.9.2.2 802.1X Setting

This page allows you to configure the IEEE 802.1X authentication system.

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

The 802.1X Setting and Information screens in [Figure 4-9-7](#) and [Figure 4-9-8](#) appear.

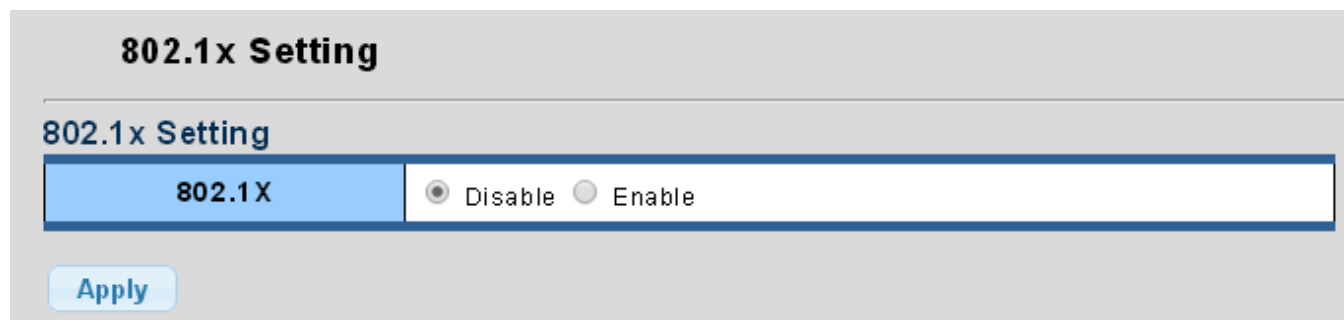


Figure 4-9-7: 802.1X Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> 802.1X 	Enable or disable the 802.1x function and default is "Disable".

Button

: Click to apply changes.

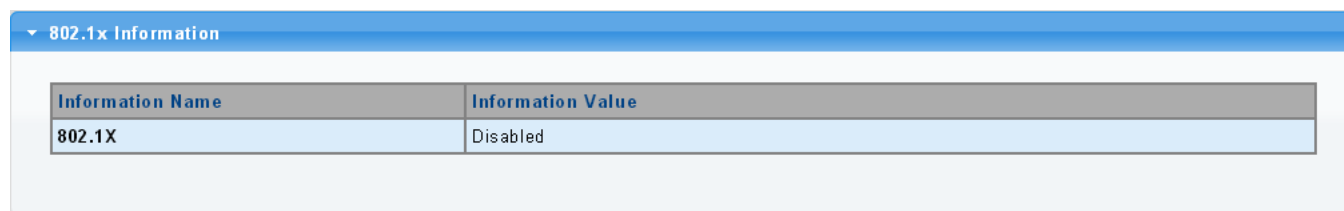


Figure 4-9-8: 802.1X Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> 802.1X 	Display the current 802.1X state.

4.9.2.3 802.1X Port Setting

This page allows you to configure the IEEE 802.1X Port Setting. The 802.1X Port Setting screens in [Figure 4-9-9](#) and [Figure 4-9-10](#) appear.

802.1x Port Setting	
Port	Select Ports
Mode	No Authentication
Reauthentication Enable	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Reauthentication Period	3600 (Range 30 - 65535, Default: 3600)
Quiet Period	60 (Range 0 - 65535, Default: 60)
Supplicant Period	30 (Range 1 - 65535, Default: 30)
Maximum Request Retries	2 (Range 1 - 10, Default: 2)

Apply

Figure 4-9-9: 802.1X Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port for this drop down list.
• Mode	<p>If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:</p> <ul style="list-style-type: none"> ■ No Authentication ■ Authentication ■ Force Unauthorized ■ In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access. ■ Force Authorized ■ In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
• Reauthentication Enable	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a

	switch port or if a supplicant is no longer attached.
<ul style="list-style-type: none"> • Reauthentication Period 	<p>Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked.</p> <p>Valid values are in the range 30 to 65535 seconds.</p>
<ul style="list-style-type: none"> • Quiet Period 	Sets time to keep silent on supplicant authentication failure.
<ul style="list-style-type: none"> • Supplicant Period 	Sets the interval for the supplicant to re-transmit EAP request/identify frame.
<ul style="list-style-type: none"> • Maximun Request Retries 	<p>The number of times that the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting.</p> <p>The value can only be changed if the Guest VLAN option is globally enabled.</p>

Button




: Click to apply changes.

802.1X Port Status								
Port	Mode (pps)	Status (pps)	Periodic Reauthentication	Reauthentication Period	Quiet Period	Supplicant Timeout	Max. EAP Requests	Modify
GE1	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE2	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE3	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE4	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE5	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE6	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE7	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE8	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE9	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE10	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE11	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE12	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE13	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE14	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE15	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE16	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE17	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE18	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE19	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE20	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE21	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE22	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE23	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE24	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE25	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE26	802.1X Disabled	-	Enabled	3600	60	30	2	Edit

Figure 4-9-10 : 802.1X Port Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Mode (pps)	Display the current mode.
• Status (pps)	Display the current status.
• Periodic Reauthentication	Display the current periodic reauthentication.
• Reauthentication Period	Display the current reauthentication period.
• Quiet Period	Display the current quiet period.
• Supplicant Timeout	Display the current supplicant timeout.
• Max. EAP Requests	Display the current Max. EAP requests.
• Modify	Click  to edit 802.1X port setting parameter.

4.9.2.4 Guest VLAN Setting

Overview

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

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

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

The 802.1X Guest VLAN setting screens in [Figure 4-9-11](#) and [Figure 4-9-12](#) appear.

Dot1x Guest VLAN

Guest VLAN Setting

Guest VLAN ID	<input style="width: 80px;" type="text" value="0"/> <input type="checkbox"/> Enable
----------------------	---

Guest VLAN Port Setting

Port Select	Guest VLAN
<input type="text" value="Select Ports"/>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Figure 4-9-11: Guest VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Guest VLAN ID 	<p>This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.</p> <p>Valid values are in the range [1~4094].</p>
<ul style="list-style-type: none"> • Port 	<p>Select port for this drop down list.</p>
<ul style="list-style-type: none"> • Guest VLAN Enabled 	<p>A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.</p> <p>The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality.</p> <ul style="list-style-type: none"> ■ When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. ■ When unchecked, the ability to move to the Guest VLAN is disabled for all ports.

Button



: Click to apply changes.

Guest VLAN Status		
Port Name	Enable State	In Guest VLAN
GE1	Disabled	NO
GE2	Disabled	NO
GE3	Disabled	NO
GE4	Disabled	NO
GE5	Disabled	NO
GE6	Disabled	NO
GE7	Disabled	NO
GE8	Disabled	NO
GE9	Disabled	NO
GE10	Disabled	NO
GE11	Disabled	NO
GE12	Disabled	NO
GE13	Disabled	NO
GE14	Disabled	NO
GE15	Disabled	NO
GE16	Disabled	NO
GE17	Disabled	NO
GE18	Disabled	NO
GE19	Disabled	NO
GE20	Disabled	NO
GE21	Disabled	NO
GE22	Disabled	NO
GE23	Disabled	NO
GE24	Disabled	NO
GE25	Disabled	NO
GE26	Disabled	NO

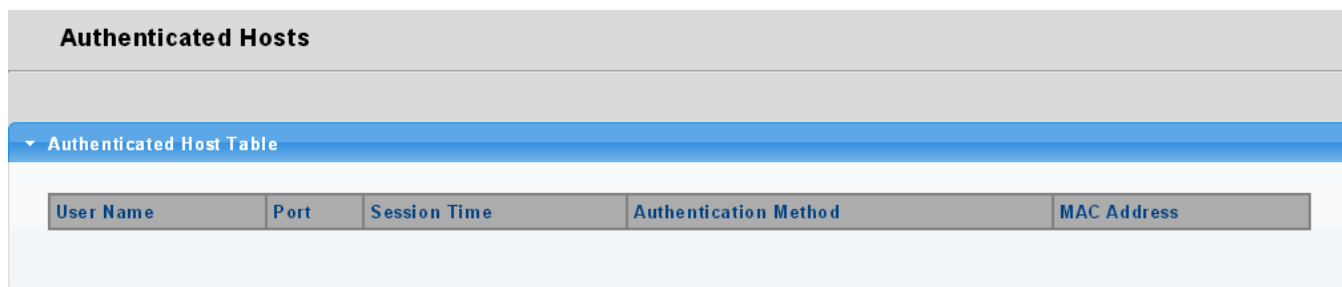
Figure 4-9-12: Guest VLAN Status Page Screenshot

The page includes the following fields:

Object	Description
• Port Name	The switch port number of the logical port.
• Enable State	Display the current state.
• In Guest VLAN	Display the current guest VLAN.

4.9.2.5 Authenticated Host

The Authenticated Host Table screen in [Figure 4-9-13](#) appears.



The screenshot shows a web interface titled "Authenticated Hosts". Below the title is a blue header bar with a dropdown menu labeled "Authenticated Host Table". Underneath is a table with five columns: "User Name", "Port", "Session Time", "Authentication Method", and "MAC Address".

Figure 4-9-13: Authenticated Host Table Page Screenshot

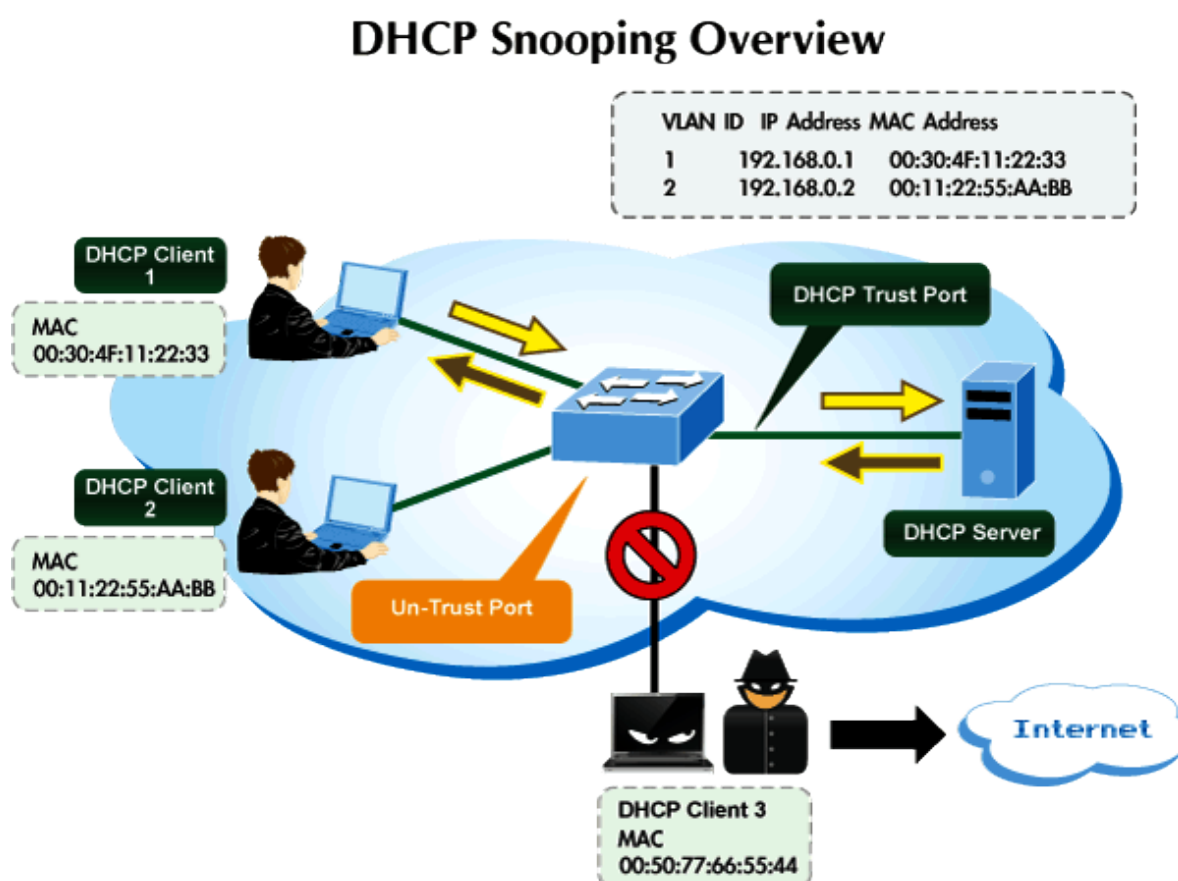
The page includes the following fields:

Object	Description
• User Name	Display the current user name.
• Port	Display the current port number.
• Session Time	Display the current session time.
• Authentication Method	Display the current authentication method.
• MAC Address	Display the current MAC address.

4.9.3 DHCP Snooping

4.9.3.1 DHCP Snooping Overview

The addresses assigned to DHCP clients on unsecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping. DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.



Command Usage

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. **DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or firewall.** When DHCP snooping is enabled globally and enabled on a VLAN interface, **DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped.**
- Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.
- When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- Filtering rules are implemented as follows:
 - If the global DHCP snooping is disabled, all DHCP packets are forwarded.

- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.
- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is not trusted, it is processed as follows:
 - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
 - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
 - If the DHCP packet is from a client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
 - If the DHCP packet is not a recognizable type, it is dropped.
- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.
 - Additional considerations when the switch itself is a DHCP client – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted. Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

4.9.3.2 Global Setting

DHCP Snooping is used to block intruder on the untrusted ports of switch when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server. Configure DHCP Snooping on this page. The DHCP Snooping Setting and Information screens in [Figure 4-9-14](#) and [Figure 4-9-15](#) appear.

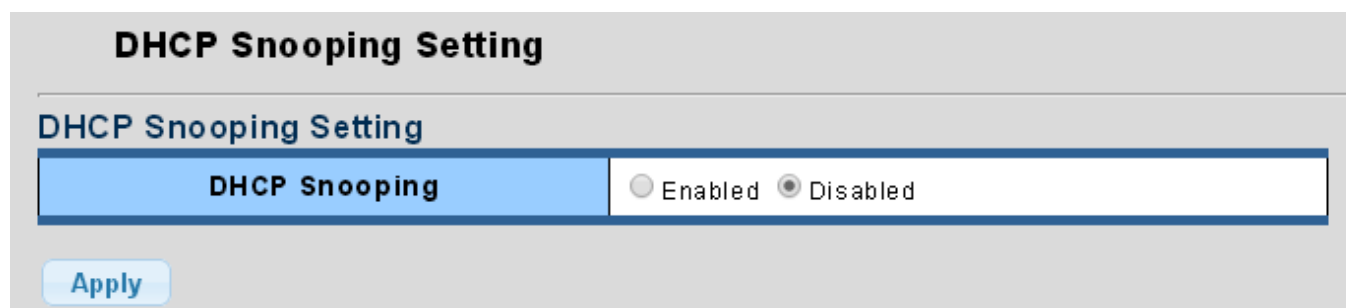



Figure 4-9-14: DHCP Snooping Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> DHCP Snooping 	<p>Indicates the DHCP snooping mode operation. Default mode is Disabled and possible modes are:</p> <ul style="list-style-type: none"> Enabled: Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. Disabled: Disable DHCP snooping mode operation.

Button

: Click to apply changes.

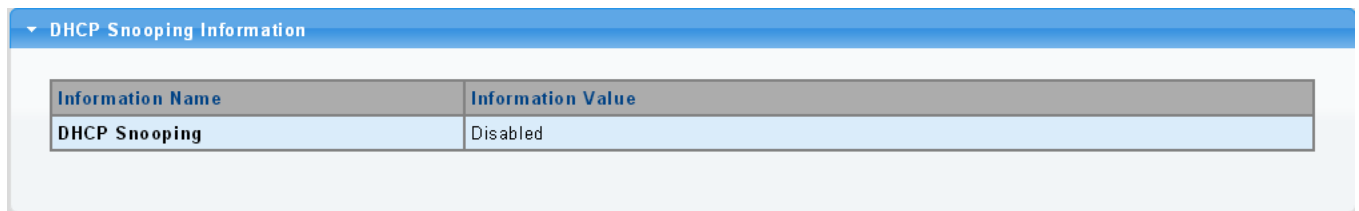


Figure 4-9-15: DHCP Snooping Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> DHCP Snooping 	Display the current DHCP snooping status.

4.9.3.3 VLAN Setting

Command Usage

- 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.
- When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.
- When DHCP snooping is globally enabled, and DHCP snooping is then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

The DHCP Snooping VLAN Setting screens in [Figure 4-9-16](#) and [Figure 4-9-17](#) appear.

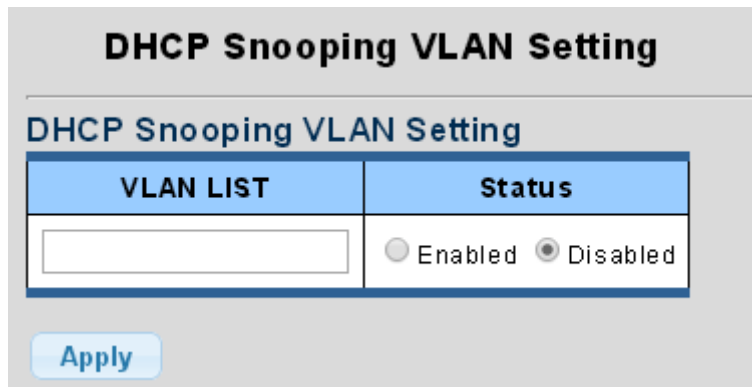



Figure 4-9-16: DHCP Snooping VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • VLAN List 	Indicates the ID of this particular VLAN.
<ul style="list-style-type: none"> • Status 	Indicates the DHCP snooping VLAN mode operation. Default mode is Disabled and possible modes are: <ul style="list-style-type: none"> ■ Enabled: Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. ■ Disabled: Disable DHCP snooping mode operation.

Button

: Click to apply changes.

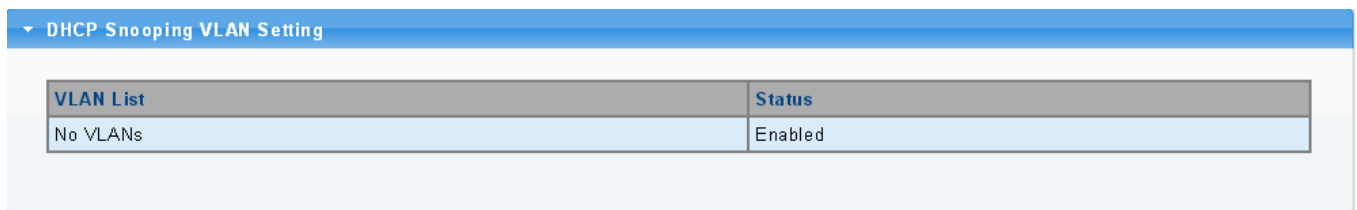


Figure 4-9-17: DHCP Snooping VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • VLAN List 	Display the current VLAN list.
<ul style="list-style-type: none"> • Status 	Display the current DHCP snooping status.

4.9.3.4 Port Setting

Configures switch ports as trusted or untrusted.

Command Usage

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall.
- When DHCP snooping enabled both globally and on a VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- Set all ports connected to DHCP servers within the local network or firewall to trusted state. Set all other ports outside the local network or firewall to untrusted state.

The DHCP Snooping Port Setting screens in [Figure 4-9-18](#) and [Figure 4-9-19](#) appear.

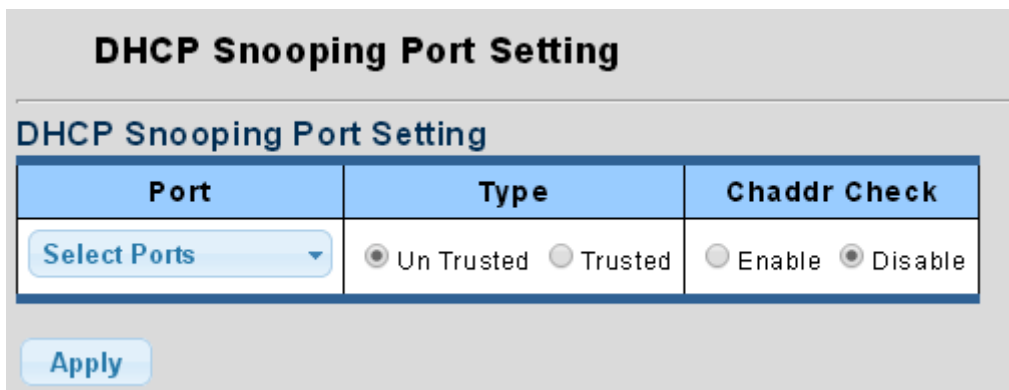


Figure 4-9-18: DHCP Snooping Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port for this drop down list.
• Type	Indicates the DHCP snooping port mode. Default mode is Untrusted and possible modes are: <ul style="list-style-type: none"> ■ Trusted: Configures the port as trusted sources of the DHCP message. ■ Untrusted: Configures the port as untrusted sources of the DHCP message.
• Chaddr Check	Indicates that the Chaddr check function is enabled on selected port. Chaddr: Client hardware address.

Button

: Click to apply changes.

DHCP Snooping Port Setting		
Port	Type	Chaddr Check
GE1	Un Trusted	Disabled
GE2	Un Trusted	Disabled
GE3	Un Trusted	Disabled
GE4	Un Trusted	Disabled
GE5	Un Trusted	Disabled
GE6	Un Trusted	Disabled
GE7	Un Trusted	Disabled
GE8	Un Trusted	Disabled
GE9	Un Trusted	Disabled
GE10	Un Trusted	Disabled
GE11	Un Trusted	Disabled
GE12	Un Trusted	Disabled
GE13	Un Trusted	Disabled
GE14	Un Trusted	Disabled
GE15	Un Trusted	Disabled
GE16	Un Trusted	Disabled
GE17	Un Trusted	Disabled
GE18	Un Trusted	Disabled
GE19	Un Trusted	Disabled
GE20	Un Trusted	Disabled
GE21	Un Trusted	Disabled
GE22	Un Trusted	Disabled
GE23	Un Trusted	Disabled
GE24	Un Trusted	Disabled
GE25	Un Trusted	Disabled
GE26	Un Trusted	Disabled
LAG1	Un Trusted	Disabled
LAG2	Un Trusted	Disabled
LAG3	Un Trusted	Disabled
LAG4	Un Trusted	Disabled
LAG5	Un Trusted	Disabled
LAG6	Un Trusted	Disabled
LAG7	Un Trusted	Disabled
LAG8	Un Trusted	Disabled

Figure 4-9-19: DHCP Snooping Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Type	Display the current type.
• Chaddr Check	Display the current chaddr check.

4.9.3.5 Statistics

The DHCP Snooping Statistics screen in [Figure 4-9-20](#) appears.

DHCP Snooping Statistics					
▼ DHCP Snooping Statistics					
<input type="button" value="Clear"/> <input type="button" value="Refresh"/>					
Port	Forwarded	Chaddr Check Dropped	Untrust Port Dropped	Untrust Port With Option82 Dropped	Invalid Dropped
GE1	0	0	0	0	0
GE2	0	0	0	0	0
GE3	0	0	0	0	0
GE4	0	0	0	0	0
GE5	0	0	0	0	0
GE6	0	0	0	0	0
GE7	0	0	0	0	0
GE8	0	0	0	0	0
GE9	0	0	0	0	0
GE10	0	0	0	0	0
GE11	0	0	0	0	0
GE12	0	0	0	0	0
GE13	0	0	0	0	0
GE14	0	0	0	0	0
GE15	0	0	0	0	0
GE16	0	0	0	0	0
GE17	0	0	0	0	0
GE18	0	0	0	0	0
GE19	0	0	0	0	0
GE20	0	0	0	0	0
GE21	0	0	0	0	0
GE22	0	0	0	0	0
GE23	0	0	0	0	0
GE24	0	0	0	0	0
GE25	0	0	0	0	0
GE26	0	0	0	0	0
LAG1	0	0	0	0	0
LAG2	0	0	0	0	0
LAG3	0	0	0	0	0
LAG4	0	0	0	0	0
LAG5	0	0	0	0	0
LAG6	0	0	0	0	0
LAG7	0	0	0	0	0
LAG8	0	0	0	0	0

Figure 4-9-20: DHCP Snooping Statistics Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Forwarded	Display the current forwarded
• Chaddr Check Dropped	Display the chaddr check dropped
• Untrust Port Dropped	Display untrust port dropped

• Untrust Port with Option82 Dropped	Display untrust port with option82 dropped
• Invaield Dropped	Display invalid dropped

Buttons

Clear: Click to clear the statistics.

Refresh: Click to refresh the statistics.

4.9.3.6 Rate Limit

After enabling DHCP snooping, the switch will monitor all the DHCP messages and implement software transmission. The DHCP Rate Limit Setting and Config screens in [Figure 4-9-21](#) and [Figure 4-9-22](#) appear.

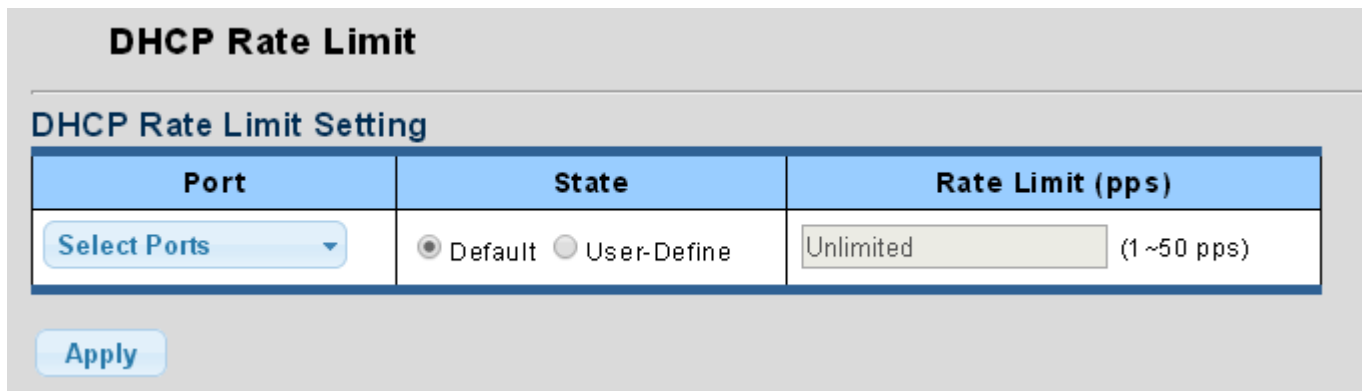


Figure 4-9-21: DHCP Rate Limit Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port for this drop down list.
• State	Set default or user-define.
• Rate Limit (pps)	Configure the rate limit for the port policer. The default value is "unlimited". Valid values are in the range 1 to 50 and unit is pps.

Button

Apply: Click to apply changes.

DHCP Rate Limit Config	
Port Name	Rate Limit (pps)
GE1	Unlimited
GE2	Unlimited
GE3	Unlimited
GE4	Unlimited
GE5	Unlimited
GE6	Unlimited
GE7	Unlimited
GE8	Unlimited
GE9	Unlimited
GE10	Unlimited
GE11	Unlimited
GE12	Unlimited
GE13	Unlimited
GE14	Unlimited
GE15	Unlimited
GE16	Unlimited
GE17	Unlimited
GE18	Unlimited
GE19	Unlimited
GE20	Unlimited
GE21	Unlimited
GE22	Unlimited
GE23	Unlimited
GE24	Unlimited
GE25	Unlimited
GE26	Unlimited
LAG1	Unlimited
LAG2	Unlimited
LAG3	Unlimited
LAG4	Unlimited
LAG5	Unlimited
LAG6	Unlimited
LAG7	Unlimited
LAG8	Unlimited

Figure 4-9-22: DHCP Rate Limit Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port Name	The switch port number of the logical port.
• Rate Limit (pps)	Display the current rate limit.

4.9.3.7 Option82 Global Setting

DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to DHCP servers. Known as **DHCP Option 82**, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients. It is also an effective tool in preventing malicious network attacks from attached clients on DHCP services, such as IP Spoofing, Client Identifier Spoofing, MAC Address Spoofing, and Address Exhaustion.

The **DHCP option 82** enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options:

- Circuit ID (option 1)
- Remote ID (option2).

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

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

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

After enabling DHCP snooping, the switch will monitor all the DHCP messages and implement software transmission. The DHCP Rate Limit Setting and Config screens in [Figure 4-9-23](#) and [Figure 4-9-24](#) appear.

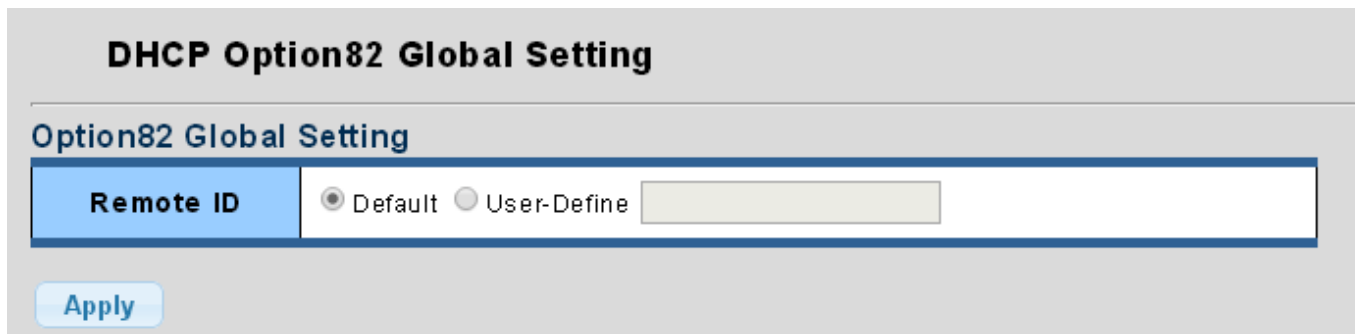


Figure 4-9-23: Option82 Global Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Remote ID 	<p>Set the option2 (remote ID option) content of option 82 added by DHCP request packets.</p> <ul style="list-style-type: none"> ■ Default means the default VLAN MAC format. ■ User-Define means the remote-id content of option 82 specified by users

Button

: Click to apply changes.

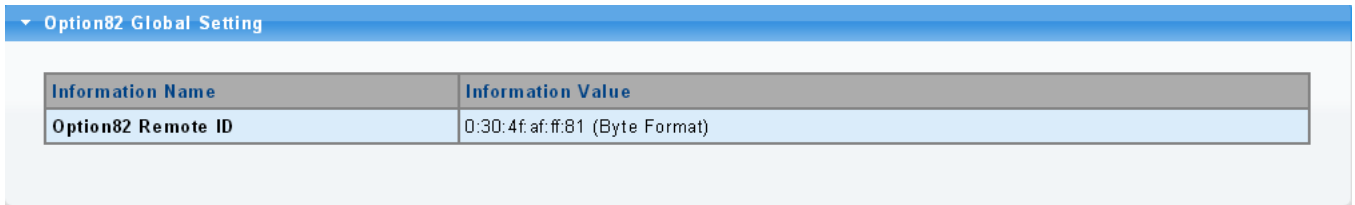


Figure 4-9-24: Option82 Global Setting Page Screenshot

The page includes the following fields:

Object	Description
• Option82 Remote ID	Display the current option82 remite ID.

4.9.3.8 Option82 Port Setting

This function is used to set the retransmitting policy of the system for the received DHCP request message which contains option82. The **drop** mode means that if the message has option82, then the system will drop it without processing; **keep** mode means that the system will keep the original option82 segment in the message, and forward it to the server to process; **replace** mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process. Option82 Port Setting screens in [Figure 4-9-25](#) and [Figure 4-9-26](#) appear.

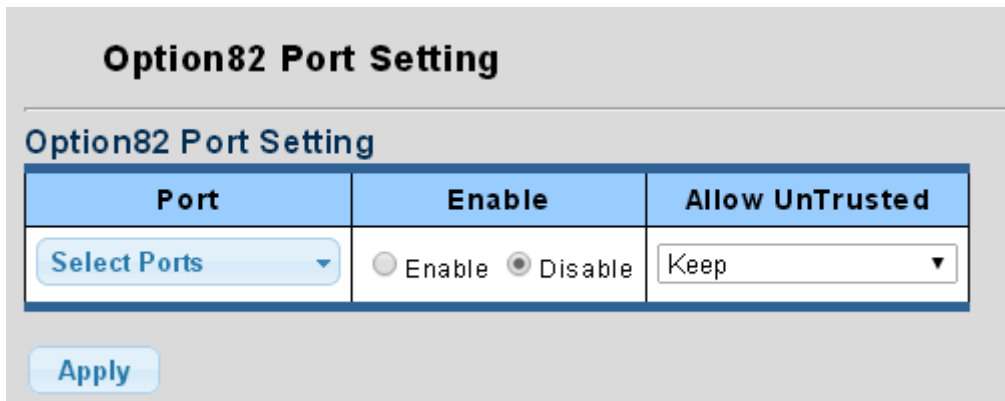


Figure 4-9-25: Option82 Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port for this drop down list.
• Enable	Enable or disable option82 function on port, default mode is Disable.
• Allow UnTrusted	Select modes for this drop down list. The following modes are available: <ul style="list-style-type: none"> ■ Keep (Default mode) ■ Drop ■ Replace

Button



: Click to apply changes.

Option82 Port Setting		
Port	Enable	Allow UnTrusted
GE1	Disabled	Drop
GE2	Disabled	Drop
GE3	Disabled	Drop
GE4	Disabled	Drop
GE5	Disabled	Drop
GE6	Disabled	Drop
GE7	Disabled	Drop
GE8	Disabled	Drop
GE9	Disabled	Drop
GE10	Disabled	Drop
GE11	Disabled	Drop
GE12	Disabled	Drop
GE13	Disabled	Drop
GE14	Disabled	Drop
GE15	Disabled	Drop
GE16	Disabled	Drop
GE17	Disabled	Drop
GE18	Disabled	Drop
GE19	Disabled	Drop
GE20	Disabled	Drop
GE21	Disabled	Drop
GE22	Disabled	Drop
GE23	Disabled	Drop
GE24	Disabled	Drop
GE25	Disabled	Drop
GE26	Disabled	Drop
LAG1	Disabled	Drop
LAG2	Disabled	Drop
LAG3	Disabled	Drop
LAG4	Disabled	Drop
LAG5	Disabled	Drop
LAG6	Disabled	Drop
LAG7	Disabled	Drop
LAG8	Disabled	Drop

Figure 4-9-26: Option82 Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Enable	Display the current status.
• Allow UnTrusted	Display the current untrusted mode.

4.9.3.9 Option82 Circuit-ID Setting

Set creation method for option82, users can define the parameters of circute-id suboption by themselves. Option82 Circuit-ID Setting screens in [Figure 4-9-27](#) and [Figure 4-9-28](#) appear.

Figure 4-9-27: Option82 Port Circuit-ID Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port for this drop down list.
• VLAN	Indicates the ID of this particular VLAN.
• Circuit ID	Set the option1 (Circuit ID) content of option 82 added by DHCP request packets.

Button

Apply: Click to apply changes.

Figure 4-9-28: Option82 Port Circuit-ID Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	Display the current port.
• VLAN	Display the current VLAN.
• Circuit ID	Display the current circuit ID.

4.9.4 Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through DUT. This page provides ARP Inspection related configuration.



A Dynamic ARP prevents the untrusted ARP packets based on the DHCP Snooping Database.

4.9.4.1 Global Setting

DAI Setting and Information screens in [Figure 4-9-29](#) and [Figure 4-9-30](#) appear.

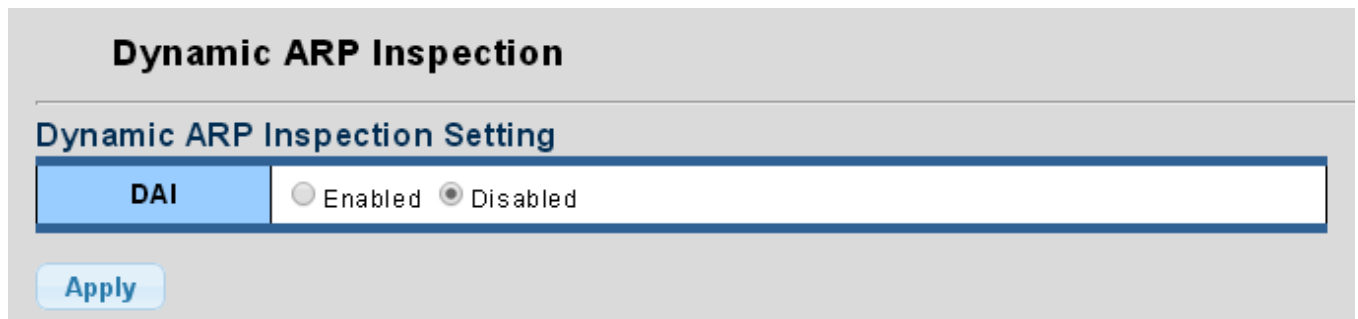


Figure 4-9-29: DAI Setting Page Screenshot

The page includes the following fields:

Object	Description
• DAI	Enable or disable the Dynamic ARP Inspection.

Button

Apply: Click to apply changes.

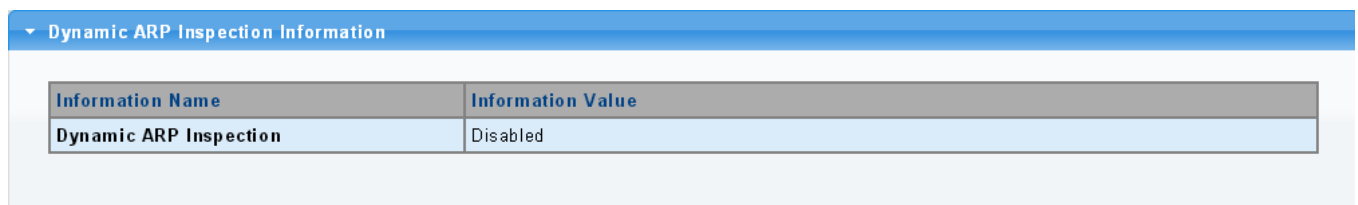


Figure 4-9-30: DAI Information Page Screenshot

The page includes the following fields:

Object	Description
• Dynamic ARP Inspection	Display the current Dynamic ARP Inspection status.

4.9.4.2 VLAN Setting

DAI VLAN Setting screens in [Figure 4-9-31](#) and [Figure 4-9-32](#) appear.

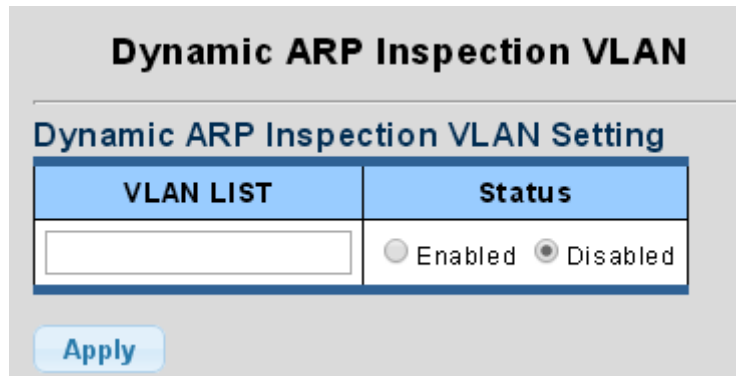



Figure 4-9-31: DAI VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
VLAN List	Indicates the ID of this particular VLAN.
Status	Enables Dynamic ARP Inspection on the specified VLAN Options: <ul style="list-style-type: none"> ■ Enable ■ Disable

Button

: Click to apply changes.

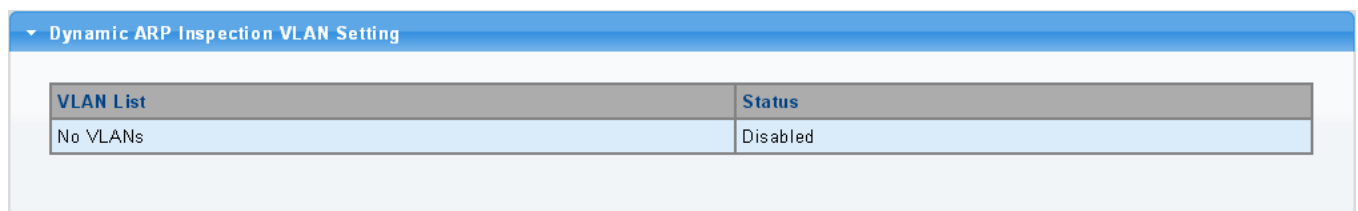


Figure 4-9-32: DAI VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
• VLAN List	Display the current VLAN list.
• Status	Display the current status.

4.9.4.3 Port Setting

Configures switch ports as DAI trusted or untrusted and check mode. DAI Port Setting screens in [Figure 4-9-33](#) and [Figure 4-9-34](#) appear.

Port	Type	Src-MAC Chk	Dst-MAC Chk	IP Chk	IP Allow Zero
Select Ports	<input checked="" type="radio"/> Un Trusted <input type="radio"/> Trusted	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled

Apply

Figure 4-9-33: DAI Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port for this drop down list
• Type	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Default: All interfaces are untrusted.
• Src-Mac Chk	Enable or disable to checks 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. When enabled, packets with different MAC addresses are classified as invalid and are dropped.
• Dst-Mac Chk	Enable or disable to checks the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.
• IP Chk	Enable or disable to checks the source and destination IP addresses of ARP packets. The all-zero, all-one or multicast IP addresses are considered invalid and the corresponding packets are discarded.
• IP Allow Zero	Enable or disable to checks all-zero IP addresses.

Button



: Click to apply changes.

DAI Port Setting					
Port	Type	Src-MAC Chk	Dst-MAC Chk	IP Chk	IP Allow Zero
GE1	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE2	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE3	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE4	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE5	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE6	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE7	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE8	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE9	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE10	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE11	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE12	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE13	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE14	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE15	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE16	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE17	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE18	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE19	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE20	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE21	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE22	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE23	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE24	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE25	Un Trusted	Disabled	Disabled	Disabled	Disabled
GE26	Un Trusted	Disabled	Disabled	Disabled	Disabled
LAG1	Un Trusted	Disabled	Disabled	Disabled	Disabled
LAG2	Un Trusted	Disabled	Disabled	Disabled	Disabled
LAG3	Un Trusted	Disabled	Disabled	Disabled	Disabled
LAG4	Un Trusted	Disabled	Disabled	Disabled	Disabled
LAG5	Un Trusted	Disabled	Disabled	Disabled	Disabled
LAG6	Un Trusted	Disabled	Disabled	Disabled	Disabled
LAG7	Un Trusted	Disabled	Disabled	Disabled	Disabled
LAG8	Un Trusted	Disabled	Disabled	Disabled	Disabled

Figure 4-9-34: DAI Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Type	Display the current port type.
• Src-MAC Chk	Display the current Src-MAC Chk status.
• Dst-MAC Chk	Display the current Dst-MAC Chk status.
• IP Chk	Display the current IP Chk status.
• IP Allow Zero	Display the current IP allow zero status.

4.9.4.4 Statistics

Configures switch ports as DAI trusted or untrusted and check mode. DAI Port Setting screen in [Figure 4-9-35](#) appears.

Port	Forwarded	Source MAC Failures	Dest MAC Failures	SIP Validation Failures	DIP Validation Failures	IP-MAC Mismatch Failures
GE1	0	0	0	0	0	0
GE2	0	0	0	0	0	0
GE3	0	0	0	0	0	0
GE4	0	0	0	0	0	0
LAG6	0	0	0	0	0	0
LAG7	0	0	0	0	0	0
LAG8	0	0	0	0	0	0

Figure 4-9-35: DAI Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Forwarded	Display the current forwarded.
Source MAC Failures	Display the current source MAC failures.
• Dest MAC Failures	Display the current source MAC failures.
• SIP Validation Failures	Display the current SIP Validation failures.
• DIP Validation Failures	Display the current DIP Validation failures.
• IP-MAC Mismatch Failures	Display the current IP-MAC mismatch failures.

Buttons

Clear: Click to clear the statistics.

Refresh: Click to refresh the statistics.

4.9.4.5 Rate Limit


The ARP Rate Limit Setting and Config screens in [Figure 4-9-36](#) and [Figure 4-9-37](#) appear.

Figure 4-9-36: ARP Rate Limit Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port for this drop down list
• State	Set default or user-define
• Rate Limit (pps)	Configure the rate limit for the port policer. The default value is "unlimited".

Button

: Click to apply changes.

Port Name	Rate Limit (pps)
GE1	unlimited
GE2	unlimited
GE3	unlimited
GE4	unlimited
LAG6	unlimited
LAG7	unlimited
LAG8	unlimited

Figure 4-9-37: ARP Rate Limit Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Rate Limit (pps)	Display the current rate limit.

4.9.5 IP Source Guard

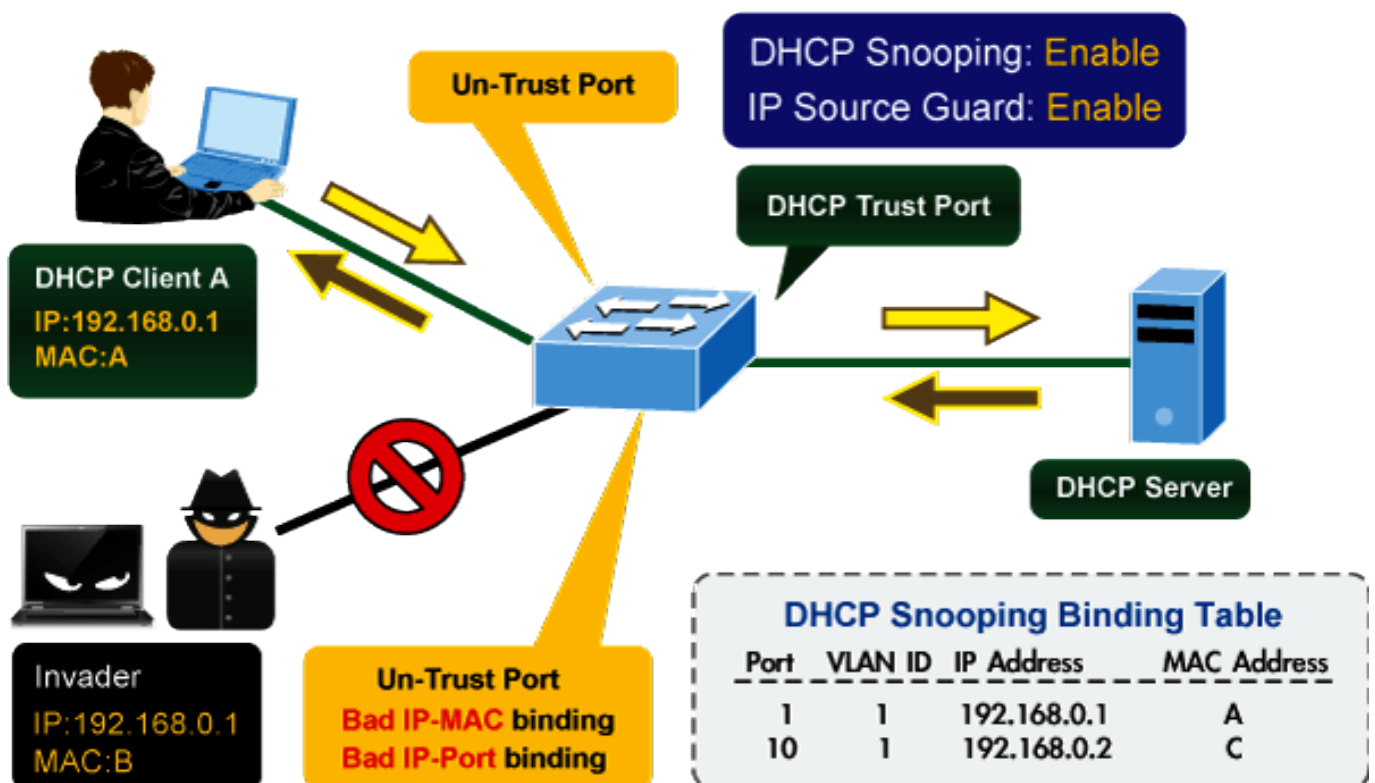
IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

After receiving a packet, the port looks up the key attributes (including IP address, MAC address and VLAN tag) of the packet in the binding entries of the IP source guard. If there is a matching entry, the port will forward the packet. Otherwise, the port will abandon the packet.

IP source guard filters packets based on the following types of binding entries:

- IP-port binding entry
- MAC-port binding entry
- IP-MAC-port binding entry

IP Source Guard Overview



4.9.5.1 Port Settings

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

The IP Source Guard Port Setting and Information screens in [Figure 4-9-38](#) and [Figure 4-9-39](#) appear.

Figure 4-9-38: IP Source Guard Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port for this drop down list.
• Status	Enable or disable the IP source guard.
• Max Binding Entry	The maximum number of IP source guard that can be secured on this port.

Button

: Click to apply changes.

IP Source Guard Port Information			
Port	Status	Max Binding Entry	Current Binding Entry
GE1	Disabled	No-limited	0
GE2	Disabled	No-limited	0
GE3	Disabled	No-limited	0
GE4	Disabled	No-limited	0
GE5	Disabled	No-limited	0
GE6	Disabled	No-limited	0
GE7	Disabled	No-limited	0
GE8	Disabled	No-limited	0
GE9	Disabled	No-limited	0
GE10	Disabled	No-limited	0
GE11	Disabled	No-limited	0
GE12	Disabled	No-limited	0
GE13	Disabled	No-limited	0
GE14	Disabled	No-limited	0
GE15	Disabled	No-limited	0
GE16	Disabled	No-limited	0
GE17	Disabled	No-limited	0
GE18	Disabled	No-limited	0
GE19	Disabled	No-limited	0
GE20	Disabled	No-limited	0
GE21	Disabled	No-limited	0
GE22	Disabled	No-limited	0
GE23	Disabled	No-limited	0
GE24	Disabled	No-limited	0
GE25	Disabled	No-limited	0
GE26	Disabled	No-limited	0
LAG1	Disabled	No-limited	0
LAG2	Disabled	No-limited	0
LAG3	Disabled	No-limited	0
LAG4	Disabled	No-limited	0
LAG5	Disabled	No-limited	0
LAG6	Disabled	No-limited	0
LAG7	Disabled	No-limited	0
LAG8	Disabled	No-limited	0

Figure 4-9-39: IP Source Guard Port Information Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Status	Display the current status.
• Max Binding Entry	Display the current max binding entry.
• Current Binding Entry	Display the current binding entry.

4.9.5.2 Binding Table

The IP Source Guard Static Binding Entry and Table Status screens in [Figure 4-9-40](#) and [Figure 4-9-41](#) appear.

Figure 4-9-40: IP Source Guard Static Binding Entry Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port for this drop down list.
• VLAN ID	Indicates the ID of this particular VLAN.
• MAC Address	Sourcing MAC address is allowed.
• IP Address	Sourcing IP address is allowed.

Button



: Click to add authentication list

Figure 4-9-41: IP Source Guard Binding Table Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	Display the current port.
• VLAN ID	Display the current VLAN.
• MAC Address	Display the current MAC address.
• IP Address	Display the current IP Address.
• Type	Display the current entry type.
• Lease Time	Display the current lease time.
• Action	Click  to delete IP source guard binding table status entry.

4.9.6 Port Security

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

The Limit Control module is one of a range of modules that utilizes a lower-layer module, the Port Security module, which manages MAC addresses, learned on the port.

The Limit Control configuration consists of two sections, a system- and a port-wid. The IP Source Guard Static Binding Entry and Table Status screens in [Figure 4-9-42](#) and [Figure 4-9-43](#) appear.

Port Select	Security	Max L2 Entry	Action	Trap Frequency (sec.)
Select Ports	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	Unlimited	Forward	10

Apply

Figure 4-9-42: Port Security Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port Select 	Select port for this drop down list.
<ul style="list-style-type: none"> • Security 	Enable or disable the port security.
<ul style="list-style-type: none"> • Max L2 Entry 	<p>The maximum number of MAC addresses that can be secured on this port. If the limit is exceeded, the corresponding action is taken.</p> <p>The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.</p>
<ul style="list-style-type: none"> • Action 	<p>If Limit is reached, the switch can take one of the following actions:</p> <ul style="list-style-type: none"> ■ Forward: Do not allow more than Limit MAC addresses on the port, but take no further action. ■ Discard: If Limit + 1 MAC addresses is seen on the port, it will trigger the action that do not learn the new MAC and drop the package. ■ Discard/SNMP/Log: If Limit + 1 MAC addresses is seen on the port, it will trigger the action that do not learn the new MAC and drop the package. Also appears under SNMP and System log.

	<p>■ Discard/SNMP/Log/ Shutdown:</p> <p>If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:</p> <ol style="list-style-type: none"> 1) Disable and re-enable Limit Control on the port or the switch, 2) Click the Reopen button. <p>Also appears under SNMP and System log.</p>
<p>• Trap Frequency (sec.)</p>	<p>Allow to input the seconds for trap frequency.</p>

Button



: Click to apply changes.

▼ Port Security Status				
Port Name	Enable State	L2 Entry Num	Action	Trap Frequency
GE1	Disabled	16383	Forward	-
GE2	Disabled	16383	Forward	-
GE3	Disabled	16383	Forward	-
GE4	Disabled	16383	Forward	-
GE5	Disabled	16383	Forward	-
GE6	Disabled	16383	Forward	-
GE7	Disabled	16383	Forward	-
GE8	Disabled	16383	Forward	-
GE9	Disabled	16383	Forward	-
GE10	Disabled	16383	Forward	-
GE11	Disabled	16383	Forward	-
GE12	Disabled	16383	Forward	-
GE13	Disabled	16383	Forward	-
GE14	Disabled	16383	Forward	-
GE15	Disabled	16383	Forward	-
GE16	Disabled	16383	Forward	-
GE17	Disabled	16383	Forward	-
GE18	Disabled	16383	Forward	-
GE19	Disabled	16383	Forward	-
GE20	Disabled	16383	Forward	-
GE21	Disabled	16383	Forward	-
GE22	Disabled	16383	Forward	-
GE23	Disabled	16383	Forward	-
GE24	Disabled	16383	Forward	-
GE25	Disabled	16383	Forward	-
GE26	Disabled	16383	Forward	-
LAG1	Disabled	16383	Forward	-
LAG2	Disabled	16383	Forward	-
LAG3	Disabled	16383	Forward	-
LAG4	Disabled	16383	Forward	-
LAG5	Disabled	16383	Forward	-
LAG6	Disabled	16383	Forward	-
LAG7	Disabled	16383	Forward	-
LAG8	Disabled	16383	Forward	-

Figure 4-9-43: Port Security Status Page Screenshot

The page includes the following fields:

Object	Description
• Port Name	The switch port number of the logical port.
• Enable State	Display the current per port security status.
• L2 Entry Num	Display the current L2 entry number.
• Action	Display the current aciotn.
• Trap Frequency	Display the current trap frequency.

4.9.7 DoS

The DoS is short for **Denial of Service**, which is a simple but effective destructive attack on the internet. The server under DoS attack will drop normal user data packet due to non-stop processing the attacker's data packet, leading to the denial of the service and worse can lead to leak of sensitive data of the server.

Security feature refers to applications such as protocol check which is for protecting the server from attacks such as DoS. The protocol check allows the user to drop matched packets based on specified conditions. The security features provide several simple and effective protections against Dos attacks while acting no influence on the linear forwarding performance of the switch.

4.9.7.1 Global DoS Setting

The Global DoS Setting and Information screens in [Figure 4-9-44](#) and [Figure 4-9-45](#) appear.

DoS

DoS Global Setting

DMAC = SMAC	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Land	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
UDP Blat	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
TCP Blat	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
POD	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IPv6 Min Fragment	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled Byte: <input style="width: 100px;" type="text" value="1240"/>
ICMP Fragments	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IPv4 Ping Max Size	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IPv6 Ping Max Size	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Ping Max Size Setting	Byte: <input style="width: 100px;" type="text" value="512"/>
Smurf Attack	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled Netmask Length: <input style="width: 100px;" type="text" value="0"/>
TCP Min Hdr Size	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled Bytes: <input style="width: 100px;" type="text" value="20"/>
TCP-SYN(SPORT<1024)	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Null Scan Attack	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
X-Mas Scan Attack	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
TCP SYN-FIN Attack	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
TCP SYN-RST Attack	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
TCP Fragment (Offset = 1)	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Figure 4-9-44: Global DoS Setting Page Screenshot

The page includes the following fields:

Object	Description
• DMAC = SMAC	Enable or disable DoS check mode by DMAC = SMAC.
• Land	Enable or disable DoS check mode by land.
• UDP Blat	Enable or disable DoS check mode by UDP blat.
• TCP Blat	Enable or disable DoS check mode by TCP blat.
• POD	Enable or disable DoS check mode by POD.
• IPv6 Min Fragment	Enable or disable DoS check mode by IPv6 min fragment.
• ICMP Fragments	Enable or disable DoS check mode by ICMP fragment.
• IPv4 Ping Max Size	Enable or disable DoS check mode by IPv4 ping max size.
• IPv6 Ping Max Size	Enable or disable DoS check mode by IPv6 ping max size.
• Ping Max Size Setting	Set the max size for ping.
• Smurf Attack	Enable or disable DoS check mode by smurf attack.
• TCP Min Hdr Size	Enable or disable DoS check mode by TCP min hdr size.
• TCP-SYN (SPORT < 1024)	Enable or disable DoS check mode by TCP-syn (sport < 1024).
• Null Scan Attack	Enable or disable DoS check mode by null scan attack.
• X-Mas Scan Attack	Enable or disable DoS check mode by x-mas scan attack.
• TCP SYN-FIN Attack	Enable or disable DoS check mode by TCP syn-fin attack.
• TCP SYN-RST Attack	Enable or disable DoS check mode by TCP syn-rst attack.
• TCP Fragment (Offset = 1)	Enable or disable DoS check mode by TCP fragment (offset = 1).

Button



: Click to apply changes.

DoS Information	
Information Name	Information Value
DMAC = SMAC	Enabled
Land Attack	Enabled
UDP Blat	Enabled
TCP Blat	Enabled
POD (Ping of Death)	Enabled
IPv6 Min Fragment Size	Enabled (1240 Bytes)
ICMP Fragment Packets	Enabled
IPv4 Ping Max Packet Size	Enabled (512 Bytes)
IPv6 Ping Max Packet Size	Enabled (512 Bytes)
Smurf Attack	Enabled (Netmask Length: 0)
TCP Min Header Length	Enabled (20 Bytes)
TCP Syn (SPORT < 1024)	Enabled
Null Scan Attack	Enabled
X-Mas Scan Attack	Enabled
TCP SYN-FIN Attack	Enabled
TCP SYN-RST Attack	Enabled
TCP Fragment (Offset = 1)	Enabled

Figure 4-9-45: DoS Information Page Screenshot

The page includes the following fields:

Object	Description
• DMAC = SMAC	Display the current DMAC = SMAC status.
• Land Attack	Display the current land attack status.
• UDP Blat	Display the current UDP blat status.
• TCP Blat	Display the current TCP blat status.
• POD	Display the current POD status.
• IPv6 Min Fragment	Display the current IPv6 min fragment status.
• ICMP Fragments	Display the current ICMP fragment status.
• IPv4 Ping Max Size	Display the current IPv4 ping max size status.
• IPv6 Ping Max Size	Display the current IPv6 ping max size status.
• Smurf Attack	Display the current smurf attack status.
• TCP Min Header Length	Display the current TCP min header length.
• TCP-SYN (SPORT < 1024)	Display the current TCP syn status.
• Null Scan Attack	Display the current null scan attack status.
• X-Mas Scan Attack	Display the current x-mas scan attack status.
• TCP SYN-FIN Attack	Display the current TCP syn-fin attack status.
• TCP SYN-RST Attack	Display the current TCP syn-rst attack status.
• TCP Fragment (Offset = 1)	Display the TCP fragment (offset = 1) status

4.9.7.2 DoS Port Setting


The DoS Port Setting and Status screens in [Figure 4-9-46](#) and [Figure 4-9-47](#) appear.

Figure 4-9-46: Port Security Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port Select 	Select port for this drop down list.
<ul style="list-style-type: none"> • DoS Protection 	Enable or disable per port DoS protection.
<ul style="list-style-type: none"> • Gratuitous-ARP 	Enable or disable per port Gratuitous-ARP.

Button

: Click to apply changes.

DoS Port Status		
Port	DoS Protection	Gratuitous-ARP
GE1	Disable	Disable
GE2	Disable	Disable
GE3	Disable	Disable
GE4	Disable	Disable
GE5	Disable	Disable
GE6	Disable	Disable
GE7	Disable	Disable
GE8	Disable	Disable
GE9	Disable	Disable
GE10	Disable	Disable
GE11	Disable	Disable
GE12	Disable	Disable
GE13	Disable	Disable
GE14	Disable	Disable
GE15	Disable	Disable
GE16	Disable	Disable
GE17	Disable	Disable
GE18	Disable	Disable
GE19	Disable	Disable
GE20	Disable	Disable
GE21	Disable	Disable
GE22	Disable	Disable
GE23	Disable	Disable
GE24	Disable	Disable
GE25	Disable	Disable
GE26	Disable	Disable
LAG1	Disable	Disable
LAG2	Disable	Disable
LAG3	Disable	Disable
LAG4	Disable	Disable
LAG5	Disable	Disable
LAG6	Disable	Disable
LAG7	Disable	Disable
LAG8	Disable	Disable

Figure 4-9-47: Port Security Setting Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• DoS Protection	Display the current DoS protection status.
• Gratuitous-ARP	Display the current Gratuitous-ARP status.

4.9.8 AAA

Authentication, authorization, and accounting (AAA) provides a framework for configuring access control on the Managed Switch. The three security functions can be summarized as follows:

- **Authentication** — Identifies users that request access to the network.
- **Authorization** — Determines if users can access specific services.
- **Accounting** — Provides reports, auditing, and billing for services that users have accessed on the network.

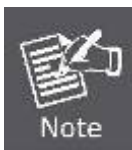
The AAA functions require the use of configured RADIUS or TACACS+ servers in the network. The security servers can be defined as sequential groups that are then applied as a method for controlling user access to specified services. For example, when the switch attempts to authenticate a user, a request is sent to the first server in the defined group, if there is no response the second server will be tried, and so on. If at any point a pass or fail is returned, the process stops.

The Managed Switch supports the following AAA features:

- Accounting for **IEEE 802.1X authenticated users** that access the network through the Managed Switch.
- Accounting for users that access **management interfaces** on the Managed Switch through the console and Telnet.
- Accounting for **commands** that users enter at specific CLI privilege levels. Authorization of users that access management interfaces on the Managed Switch through the console and Telnet.

To configure AAA on the Managed Switch, you need to follow this general process:

1. Configure RADIUS and TACACS+ server access parameters. See "[Configuring Local/Remote Logon Authentication](#)".
2. Define RADIUS and TACACS+ server groups to support the accounting and authorization of services.
3. Define a method name for each service to which you want to apply accounting or authorization and specify the RADIUS or TACACS+ server groups to use. Apply the method names to port or line interfaces.



This guide assumes that RADIUS and TACACS+ servers have already been configured to support AAA. The configuration of RADIUS and TACACS+ server software is beyond the scope of this guide and refers to the documentation provided with the RADIUS or TACACS+ server software.

4.9.8.1 Login List

This page is to login list parameters. The authentication list screens in [Figure 4-9-48](#) and [Figure 4-9-49](#) appear.

Figure 4-9-48: New Authentication List Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • List Name 	Defines a name for the authentication list, the available length is 31 characters.
<ul style="list-style-type: none"> • Method 1-4 	Set the login authentication method: Empty / None / Local / TACACS+ / RADIUS / Enable Default mode is Empty.

Button




: Click to add authentication list.

Figure 4-9-49: Login Authentication List Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • List Name 	Display the current list name.
<ul style="list-style-type: none"> • Method List 	Display the current method list.
<ul style="list-style-type: none"> • Modify 	Click  to edit login authentication list parameter. Click  to delete login authentication list entry.

4.9.8.2 Enable List

This page is to login list parameters. The authentication list screens in [Figure 4-9-50](#) and [Figure 4-9-51](#) appear.

Figure 4-9-50: New Authentication List Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • List Name 	Defines a name for the authentication list, the available length is 31 characters.
<ul style="list-style-type: none"> • Method 1-3 	Set the login authentication method: Empty / None / Enable / TACACS+ / RADIUS

Button




: Click to add authentication list.

Figure 4-9-51: Login Authentication List Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • List Name 	Display the current list name.
<ul style="list-style-type: none"> • Method List 	Display the current method list.
<ul style="list-style-type: none"> • Modify 	Click  to edit login authentication list parameter. Click  to delete login authentication list entry.

4.9.8.3 Accounting List

This page is to accounting list parameters. The authentication list screens in [Figure 4-9-52](#) and [Figure 4-9-53](#) appear.


The screenshot shows a web interface titled "Exec Accounting List". Below the title is a section for "New Accounting List" containing a table with four columns: "List Name", "Record Type", "Method 1", and "Method 2". Each column has a corresponding input field or dropdown menu, all of which are currently set to "None". Below the table is a blue "Add" button.

Figure 4-9-52: New Accounting List Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • List Name 	Defines a name for the accounting list, the available length is 31 characters.
<ul style="list-style-type: none"> • Record Type 	Provide following record type: Start-Stop (Default mode) Stop-Only
<ul style="list-style-type: none"> • Method 1-2 	Set the login accounting method: TACACS+ / RADIUS

Button



: Click to add accounting list.

The screenshot shows a table titled "Exec Accounting Lists" with a single row. The columns are "List Name", "Record Type", "Method 1", "Method 2", and "Modify". The "Default" entry has "None" for Record Type, Method 1, and Method 2. An "Edit" button is visible in the "Modify" column.

Figure 4-9-53: Accounting List Screenshot

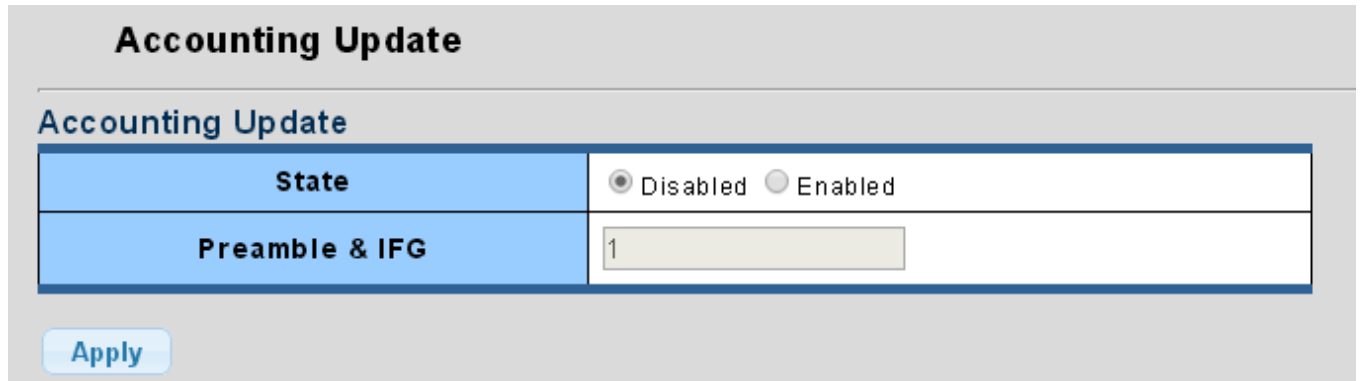
The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • List Name 	Display the current list name.
<ul style="list-style-type: none"> • Record Type 	Display the current record type.
<ul style="list-style-type: none"> • Method List 	Display the current method list.

<ul style="list-style-type: none"> • Modify 	<p>Click  to edit login authentication list parameter.</p> <p>Click  to delete login authentication list entry.</p>
---	---

4.9.8.4 Accounting Update

This page is to accounting update parameters. The authentication list screens in [Figure 4-9-54](#) and [Figure 4-9-55](#) appear.



The screenshot shows a form titled "Accounting Update". It has two main sections: "State" and "Preamble & IFG".

State	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Preamble & IFG	<input type="text" value="1"/>


At the bottom left of the form is an .

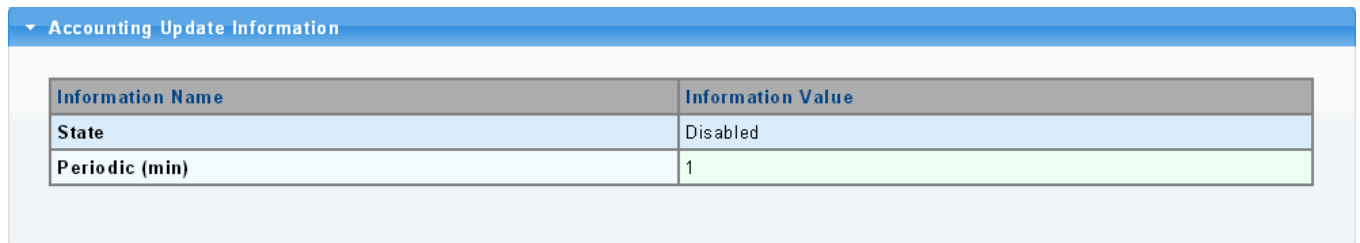
Figure 4-9-54: Accounting Update Screenshot

The page includes the following fields:

Object	Description
• State	Provide Disabled or Enabled this function.
• Preamble & IFG	Provide input the preamble & IFG value.

Button

: Click to apply changes.



The screenshot shows a table titled "Accounting Update Information".

Information Name	Information Value
State	Disabled
Periodic (min)	1

Figure 4-9-55: Accounting Update Screenshot

The page includes the following fields:

Object	Description
• State	Display the current state.
• Periodic (mim)	Display the current periodic value.

4.9.9 TACACS+ Server

This page is to configure the RADIUS server connection session parameters. The RADIUS Settings screens in [Figure 4-9-56](#), [Figure 4-9-57](#) and [Figure 4-9-58](#) appear.

TACACS+ Server Settings	
Use Default Parameters	
IP Version	Version 6 Version 4
Key String	<input type="text"/> (0/128 ASCII Alphanumeric Characters Used)
Timeout for Reply	5 <input type="text"/> sec. (Range 1 - 30, Default: 5)

Figure 4-9-56: TACACS+ Server Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Key String 	The secret key - up to 128 characters long - shared between the TACACS+ server and the switch.
<ul style="list-style-type: none"> • Timeout for Reply 	Retransmit is the number of times, in the range 1 to 30; a TACACS+ request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Button

: Click to apply changes.


New TACACS+ Server	
Server Definition	<input checked="" type="radio"/> By IP address <input type="radio"/> By name
Server IP	<input type="text"/>
Server Port	49 <input type="text"/> (0 - 65535)
Server Key	<input checked="" type="checkbox"/> Use Default <input type="text"/>
Server Timeout	<input checked="" type="checkbox"/> Use Default <input type="text"/> (1-30) secs
Server Priority	1 <input type="text"/> (0 - 65535)

Figure 4-9-57: New TACACS+ Server Page Screenshot

The page includes the following fields:

Object	Description
• Server Definition	Set the server definition.
• Server IP	Address of the TACACS+ server IP/name.
• Server Port	Network (TCP) port of TACACS+ server used for authentication messages. (Range: 0-65535; Default: 49)
• Server Key	The key- shared between the TACACS+ Authentication Server and the switch.
• Server Timeout	The number of seconds the switch waits for a reply from the server before it resends the request. (Range: 1-30 seconds)
• Server Priority	Set the server priority. (Range: 0-65535)

Button

: Click to add TACACS+ Server setting.

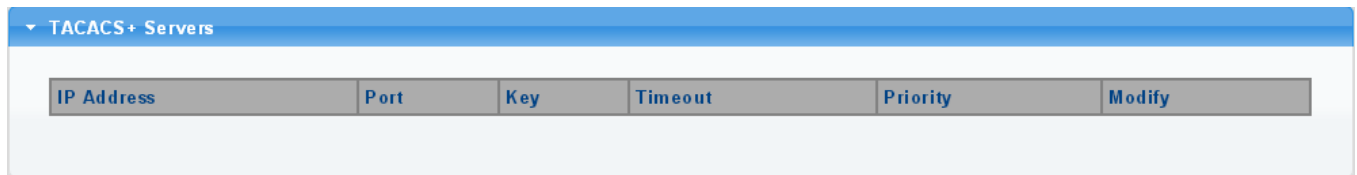




Figure 4-9-58: Login Authentication List Page Screenshot

The page includes the following fields:

Object	Description
• IP Address	Display the current IP address.
• Port	Display the current port.
• Key	Display the current key.
• Timeout	Display the current timeout.
• Priority	Display the current priority
• Modify	Click  to edit login authentication list parameter. Click  to delete login authentication list entry.

4.9.10 RADIUS Server

This page is to configure the RADIUS server connection session parameters. The RADIUS Settings screens in [Figure 4-9-59](#), [Figure 4-9-60](#) and [Figure 4-9-61](#) appear.

Radius Server Settings

Use Default Parameters

IP Version	Version 6 Version 4	
Retries	<input style="width: 80px;" type="text" value="3"/>	(Range 1 - 10, Default: 3)
Timeout for Reply	<input style="width: 80px;" type="text" value="3"/>	sec. (Range 1 - 30, Default: 3)
Dead Time	<input style="width: 80px;" type="text" value="0"/>	min. (Range 0 - 2000, Default: 0)
Key String	<input style="width: 150px;" type="text"/>	(0/1 28 ASCII Alphanumeric Characters Used)

Figure 4-9-59: Radius Server Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Retries 	Timeout is the number of seconds, in the range 1 to 10, to wait for a reply from a RADIUS server before retransmitting the request. Default is 3.
<ul style="list-style-type: none"> • Timeout for Reply 	Retransmit is the number of times, in the range 1 to 30, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead. Default is 3.
<ul style="list-style-type: none"> • Dead Time 	<p>The Dead Time, which can be set to a number between 0 and 2000 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.</p> <p>Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. Default is 0.</p>
<ul style="list-style-type: none"> • Key String 	The secret key - up to 128 characters long - shared between the RADIUS server and the switch.

Button

: Click to apply changes.

New Radius Server

Server Definition	<input checked="" type="radio"/> By IP address <input type="radio"/> By name
Server IP	<input type="text"/>
Authentication Port	<input type="text" value="1812"/> (0 - 65535)
Acct Port	<input type="text" value="1813"/> (0 - 65535)
Key String	<input checked="" type="checkbox"/> Use Default <input type="text"/>
Timeout for Reply	<input checked="" type="checkbox"/> Use Default <input type="text"/> (1-30) secs
Retries	<input checked="" type="checkbox"/> Use Default <input type="text"/> (1 - 10)
Server Priority	<input type="text" value="1"/> (0 - 65535)
Dead Time	<input type="text" value="0"/> (0 - 2000)
Usage Type	<input type="radio"/> Login <input type="radio"/> 802.1X <input checked="" type="radio"/> All


Figure 4-9-60: New Radius Server Page Screenshot

The page includes the following fields:

Object	Description
• Server Definition	Set the server definition.
• Server IP	Address of the Radius server IP/name.
• Authetication Port	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server. (Range: 0-65535)
• Acct Port	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server. (Range: 0-65535)
• Key String	The shared key - shared between the RADIUS Authentication Server and the switch.
• Timeout for Reply	The Timeout, which can be set to a number between 1 and 30 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to

	3 times before it is considered to be dead.
• Retries	Timeout is the number of seconds, in the range 1 to 10, to wait for a reply from a RADIUS server before retransmitting the request.
• Server Priority	Set the server priority. (Range: 0-65535)
• Dead Time	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. (Range: 0-2000)
• Usage Type	Set the usage type. The following modes are available: <ul style="list-style-type: none"> ■ Login ■ 802.1X ■ All

Button

: Click to add Radius server setting.

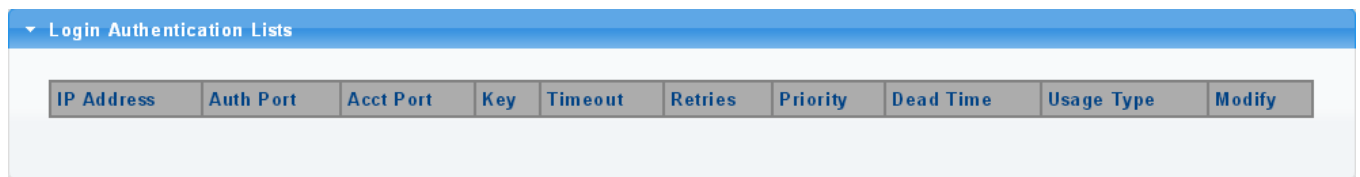




Figure 4-9-61: Login Authentication List Page Screenshot

The page includes the following fields:

Object	Description
• IP Address	Display the current IP address.
• Auth Port	Display the current auth port.
• Acct Port	Display the current acct port.
• Key	Display the current key.
• Timeout	Display the current timeout.
• Retries	Display the current retries times.
• Priority	Display the current priority.
• Dead Time	Display the current dead time
• Usage Type	Display the current usage type.
• Modufy	Click  to edit login authentication list parameter. Click  to delete login authentication list entry.

4.9.11 Access

This section is to control the access of the Managed Switch, including the different access methods – Console, Telnet, HTTP and HTTPS.

4.9.11.1 Console

The Console Settings and Information screens in [Figure 4-9-62](#) and [Figure 4-9-63](#) appear.

Console Settings	
Login Authentication List	Default ▼
Enable Authentication List	Default ▼
EXEC Accounting List	Default ▼
Session Timeout	10 (0-65535) minutes
Password Retry Count	3 (0-120)
Silent Time	0 (0-65535) seconds

Apply

Figure 4-9-62: Console Settings Page Screenshot

The page includes the following fields:

Object	Description
• Login Authentication List	Select login authentication list for this drop down list.
• Enable Authentication List	Select enable authentication list for this drop down list.
• EXEC Accounting List	Select EXEC accounting list for this drop down list.
• Session Timeout	Set the session timeout value. Default is 10 and available range is 0-65535 minutes.
• Password Retry Count	Set the password retry count value. Default is 3 and available range is 0-120.
• Silent Time	Set the silent time value. Default is 0 and available range is 0-65535 seconds.

Button

: Click to apply changes.

Console Information	
Information Name	Information Value
Login Authentication List	Default
Enable Authentication List	Default
EXEC Accounting List	Default
Session Timeout	10
Password Retry Count	3
Silent Time	0

Figure 4-9-63: Console Information Page Screenshot

The page includes the following fields:

Object	Description
• Login Authentication List	Display the current login authentication list information.
• Enable Authentication List	Display the current enable authentication list information.
• EXEC Accounting List	Display the EXEC accounting list information.
• Session Timeout	Display the current session timeout information.
• Password Retry Count	Displays the current password retry count information.
• Silent Time	Display the current silent time information.

4.9.11.2 Telnet

The Telnet Settings and Information screens in [Figure 4-9-64](#) and [Figure 4-9-65](#) appear.

Telnet Settings

Telnet Settings

Telnet Service	Disabled ▼
Login Authentication List	Default ▼
Enable Authentication List	Default ▼
EXEC Accounting List	Default ▼
Session Timeout	10 (0-65535) minutes
Password Retry Count	3 (0-120)
Silent Time	0 (0-65535) seconds

Apply
Disconnect

Figure 4-9-64: Telnet Settings Page Screenshot

The page includes the following fields:

Object	Description
• Telnet Service	Disable or enable telnet service.
• Login Authentication List	Select login authentication list for this drop down list.
• Enable Authentication List	Select enable authentication list for this drop down list.
• EXEC Accounting List	Select EXEC accounting list for this drop down list.
• Session Timeout	Set the session timeout value. Default is 10 and available range is 0-65535 minutes.
• Password Retry Count	Set the password retry count value. Default is 3 and available range is 0-120.
• Silent Time	Set the silent time value. Default is 0 and available range is 0-65535 seconds.

Button

Apply

: Click to apply changes.

Disconnect

: Click to disconnect telnet communication.

Telnet Information	
Information Name	Information Value
Telnet Service	Disabled
Login Authentication List	Default
Enable Authentication List	Default
EXEC Accounting List	Default
Session Timeout	10
Password Retry Count	3
Silent Time	0
Current Telnet Sessions Count	0

Figure 4-9-65: Telnet Information Page Screenshot

The page includes the following fields:

Object	Description
• Telnet Service	Display the current telnet service information.
• Login Authentication List	Display the current login authentication list information.
• Enable Authentication List	Display the current enable authentication list information.
• EXEC Accounting List	Display the EXEC accounting list information.
• Session Timeout	Display the current session timeout information.
• Password Retry Count	Displays the current password retry count information.
• Silent Time	Display the current silent time information.
• Current Telnet Session Count	Display the current telnet session count information.

4.9.11.3 HTTP

The HTTP Settings and Information screens in [Figure 4-9-66](#) and [Figure 4-9-67](#) appear.

Figure 4-9-66: HTTP Settings Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • HTTP Service 	Disable or enable HTTP service. Default is Enabled.
<ul style="list-style-type: none"> • Login Authentication List 	Select login authentication list for this drop down list.
<ul style="list-style-type: none"> • Session Timeout 	Set the session timeout value. Default is 10 and available range is 0-86400 minutes.

Button


: Click to apply changes.

Figure 4-9-67: HTTP Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • HTTP Service 	Display the current HTTP service information.
<ul style="list-style-type: none"> • Login Authentication List 	Display the current login authentication list information.
<ul style="list-style-type: none"> • Session Timeout 	Display the current session timeout information.

4.9.11.4 HTTPS

The HTTPS Settings and Information screens in [Figure 4-9-68](#) and [Figure 4-9-69](#) appear.

Figure 4-9-68: HTTPS Settings Page Screenshot

The page includes the following fields:

Object	Description
• HTTPS Service	Disable or enable HTTPS service. Default is Disabled.
• Login Authentication List	Select login authentication list for this drop down list.
• Session Timeout	Set the session timeout value. Default is 10 and available range is 0-86400 minutes.

Button

: Click to apply changes.

Figure 4-9-69: HTTPS Information Page Screenshot

The page includes the following fields:

Object	Description
• HTTPS Service	Display the current HTTPS service information.
• Login Authentication List	Display the current login authentication list information.
• Session Timeout	Display the current session timeout information.

4.10 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.

ACE is an acronym for **Access Control Entry**. It describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

The ACL page contains links to the following main topics:

- **MAC-Based ACL** Configuration MAC-based ACL setting
- **MAC-Based ACE** Add / Edit / Delete the MAC-based ACE (Access Control Entry) setting
- **IPv4-Based ACL** Configuration IPv4-based ACL setting
- **IPv4-Based ACE** Add / Edit / Delete the IPv4-based ACE (Access Control Entry) setting
- **IPv6-Based ACL** Configuration IPv6-based ACL setting
- **IPv6-Based ACE** Add / Edit / Delete the IPv6-based ACE (Access Control Entry) setting
- **ACL Binding** Configure the ACL parameters (ACE) of each switch port.

4.10.1 MAC-Based ACL

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. MAC-Based ACL screens in [Figure 4-10-1](#) and [Figure 4-10-2](#) appear.



Figure 4-10-1: MAC-Based ACL Page Screenshot

The page includes the following fields:

Object	Description
• ACL Name	Create a named MAC-based ACL list.

Button

: Click to add MAC-Based ACL setting.

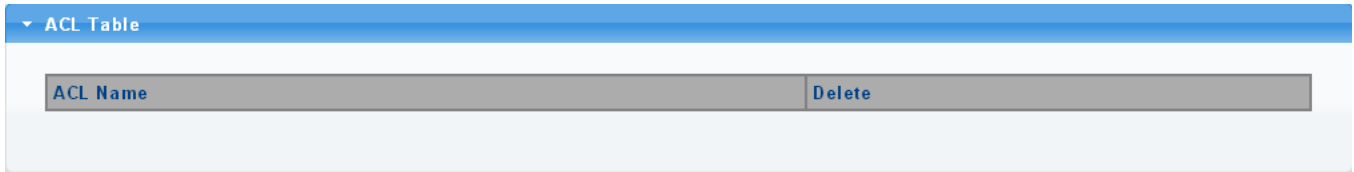



Figure 4-10-2: MAC-Based ACL Table Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Delete 	Click  to delete ACL name entry.

4.10.2 MAC-Based ACE

An ACE consists of several parameters. Different parameter options are displayed depending on the frame type that you selected. The MAC-Based ACE screens in [Figure 4-10-3](#) and [Figure 4-10-4](#) appear.

MAC-Based ACE

MAC-Based ACE

ACL Name	<input type="text"/>
Sequence	<input type="text"/> (Range: 1 - 2147483647, 1 is first processed)
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
DA MAC	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
DA MAC Value	<input type="text"/>
DA MAC Mask	<input type="text"/> (0s for matching, 1s for no matching)
SA MAC	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
SA MAC Value	<input type="text"/>
SA MAC Mask	<input type="text"/> (0s for matching, 1s for no matching)
VLAN ID	<input type="text"/> (Range:1 - 4094)
802.1p	<input type="checkbox"/> Include
802.1p Value	<input type="text"/> (Range:0-7)
802.1p Mask	<input type="text"/>
Ethertype (Range:0x05DD-0xFFFF)	<input type="text"/> (Range:0x05DD-0xFFFF)


Figure 4-10-3: MAC-Based ACE Page Screenshot

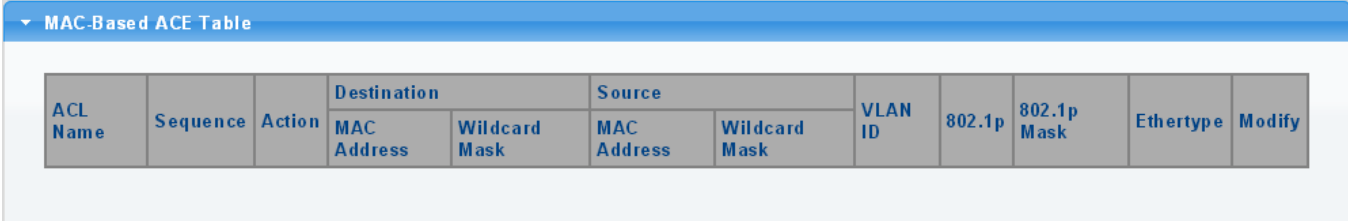
The page includes the following fields:

Object	Description
• ACL Name	Select ACL name for this drop down list.
• Sequence	Set the ACL sequence.
• Action	<p>Indicates the forwarding action of the ACE.</p> <ul style="list-style-type: none"> ■ Permit: Frames matching the ACE may be forwarded and learned. ■ Deny: Frames matching the ACE are dropped.
• DA MAC	<p>Specify the destination MAC filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No DA MAC filter is specified. ■ User Defined: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DA MAC value appears.
• DA MAC Value	When "User Defined" is selected for the DA MAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DA MAC value.

<ul style="list-style-type: none"> • DA MAC Mask 	<p>Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.</p> <ul style="list-style-type: none"> ■ 0: ARP frames where SHA is not equal to the DA MAC address. ■ 1: ARP frames where SHA is equal to the DA MAC address.
<ul style="list-style-type: none"> • SA MAC 	<p>Specify the source MAC filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No SA MAC filter is specified. ■ User Defined: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering a SA MAC value appears.
<ul style="list-style-type: none"> • SA MAC Value 	<p>When "User Defined" is selected for the SA MAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SA MAC value.</p>
<ul style="list-style-type: none"> • SA MAC Mask 	<p>Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.</p> <ul style="list-style-type: none"> ■ 0: ARP frames where SHA is not equal to the SA MAC address. ■ 1: ARP frames where SHA is equal to the SA MAC address.
<ul style="list-style-type: none"> • VLAN ID 	<p>Indicates the ID of this particular VLAN. The available range is 1-4094.</p>
<ul style="list-style-type: none"> • 802.1p 	<p>Include or exclude the 802.1p value.</p>
<ul style="list-style-type: none"> • 802.1p Value 	<p>Set the 802.1p value. The available range is 0-7.</p>
<ul style="list-style-type: none"> • 802.1p Mask 	<ul style="list-style-type: none"> ■ 0: where frame is not equal to the 802.1p value. ■ 1: where frame is equal to the 802.1p value.
<ul style="list-style-type: none"> • Ethertype (Range:0x05DD – 0xFFFF) 	<p>You can enter a specific EtherType value. The allowed range is 0x05DD to 0xFFFF. A frame that hits this ACE matches this EtherType value.</p>

Button



: Click to add MAC-Based ACE setting.



ACL Name	Sequence	Action	Destination		Source		VLAN ID	802.1p	802.1p Mask	Ethertype	Modify
			MAC Address	Wildcard Mask	MAC Address	Wildcard Mask					

Figure 4-10-4: MAC-Based ACE Table Page Screenshot

The page includes the following fields:

Object	Description
• ACL Name	Display the current ACL name.
• Sequence	Display the current sequence.
• Action	Display the current action.
• Destination MAC Address	Display the current destination MAC address.
• Destination Wildcard Mask	Display the current destination wildcard mask.
• Source MAC Address	Display the current source MAC address.
• Source Wildcard Mask	Display the current source wildcard mask.
• VLAN ID	Display the current VLAN ID.
• 802.1p	Display the current 802.1p value.
• 802.1p Mask	Display the current 802.1p mask value.
• Ethertype	Display the current Ethernet type.
• Modify	Click  to edit MAC-Based ACE parameter. Click  to delete MAC-Based ACE entry.

4.10.3 IPv4-based ACL

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. IPv4-Based ACL screens in [Figure 4-10-5](#) and [Figure 4-10-6](#) appear.



Figure 4-10-5: IPv4-based ACL Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> ACL Name 	Create a named IPv4-based ACL list.

Button

: Click to add IPv4-based ACL name list.

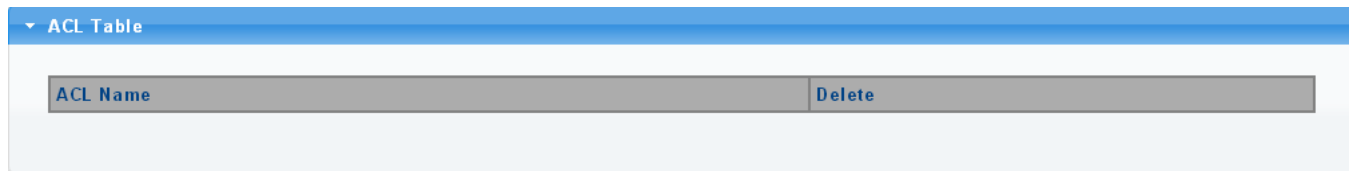



Figure 4-10-6: IPv4-based ACL Table Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Delete 	Click  to delete ACL name entry.

4.10.4 IPv4-based ACE

An ACE consists of several parameters. Different parameter options are displayed depending on the frame type that you selected. The IPv4-Based ACE screens in [Figure 4-10-7](#) and [Figure 4-10-8](#) appear.

IPv4-Based ACE

IPv4-Based ACE

ACL Name	<input type="text"/>
Sequence	<input type="text"/> (Range: 1 - 2147483647, 1 is first processed)
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Protocol	<input checked="" type="radio"/> Any(IP) <input type="radio"/> Select from list <input type="text" value="icmp"/> <input type="radio"/> Protocol ID to match <input type="text" value="1"/>
Source IP Address	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
Source IP Address Value	<input type="text"/>
Source IP Mask	<input type="text"/> (0s for matching, 1s for no matching)
Destination IP Address	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
Destination IP Address Value	<input type="text"/>
Destination IP Mask	<input type="text"/> (0s for matching, 1s for no matching)
Source Port	<input checked="" type="radio"/> Any <input type="radio"/> Single <input type="text"/> (Range: 0 - 65535) <input type="radio"/> Range <input type="text"/> - <input type="text" value="65535"/> (Range: 0 - 65535)
Destination Port	<input checked="" type="radio"/> Any <input type="radio"/> Single (Range: 0 - 65535) <input type="text"/> (Range: 0 - 65535) <input type="radio"/> Range (Range: 0 - 65535) <input type="text"/> - <input type="text" value="65535"/> (Range: 0 - 65535)
TCP Flags	Urg <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Ack <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Psh <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Rst <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Syn <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Fin <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care
Type of Service	<input checked="" type="radio"/> Any <input type="radio"/> DSCP to match <input type="text"/> (Range: 0 - 63) <input type="radio"/> IP Precedence to match <input type="text"/> (Range: 0 - 7)
ICMP	<input checked="" type="radio"/> Any <input type="radio"/> Select from list <input type="text" value="Echo Req"/> <input type="radio"/> Protocol ID to match <input type="text"/> (Range: 0 - 255)
ICMP Code	<input checked="" type="radio"/> Any <input type="radio"/> User Defined <input type="text"/> (Range: 0 - 255)

Figure 4-10-7: IPv4-based ACE Page Screenshot


The page includes the following fields:

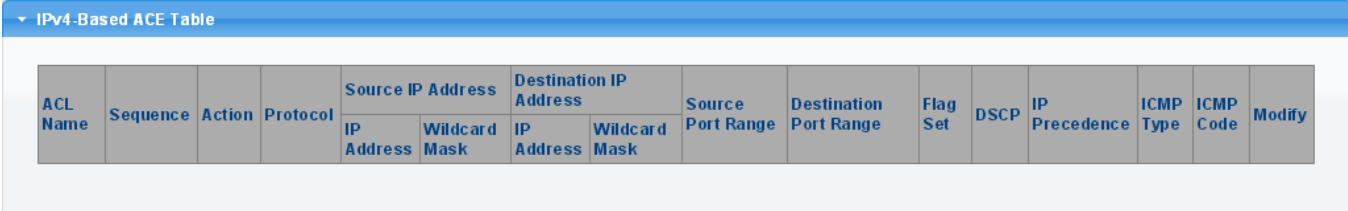
Object	Description
• ACL Name	Select ACL name for this drop down list.
• Sequence	Set the ACL sequence.
• Action	Indicates the forwarding action of the ACE. <ul style="list-style-type: none"> ■ Permit: Frames matching the ACE may be forwarded and learned. ■ Deny: Frames matching the ACE are dropped.
• Protocol	Specify the protocol filter for this ACE. <ul style="list-style-type: none"> ■ Any(IP): No protocol filter is specified. ■ Select from list: If you want to filter a specific protocol with this ACE, choose this value and select protocol for this drop down list. ■ Protocol ID to match: If you want to filter a specific protocol with this ACE, choose this value and set correct protocol ID.
• Source IP Address	Specify the Source IP address filter for this ACE. <ul style="list-style-type: none"> ■ Any: No source IP address filter is specified. ■ User Defined: If you want to filter a specific source IP address with this ACE, choose this value. A field for entering a source IP address value appears.
• Source IP Address Value	When "User Defined" is selected for the source IP address filter, you can enter a specific source IP address. The legal format is "xxx.xxx.xxx.xxx". A frame that hits this ACE matches this source IP address value.
• Source IP Mask	When "User Defined" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
• Destination IP Address	Specify the Destination IP address filter for this ACE. <ul style="list-style-type: none"> ■ Any: No destination IP address filter is specified. ■ User Defined: If you want to filter a specific destination IP address with this ACE, choose this value. A field for entering a source IP address value appears.
• Destination IP Address Value	When "User Defined" is selected for the destination IP address filter, you can enter a specific destination IP address. The legal format is "xxx.xxx.xxx.xxx". A frame that hits this ACE matches this destination IP address value.
• Destination IP Mask	When "User Defined" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.
• Source Port	Specify the source port for this ACE. <ul style="list-style-type: none"> ■ Any: No specific source port is specified (source port status is "don't-care"). ■ Single: If you want to filter a specific source port with this ACE, you can enter a specific source port value. A field for entering a source port value appears. The allowed range is 0 to 65535. A frame that hits this ACE matches this source port value.

	<ul style="list-style-type: none"> ■ Range: If you want to filter a specific source port range filter with this ACE, you can enter a specific source port range value. A field for entering a source port value appears. The allowed range is 0 to 65535. A frame that hits this ACE matches this source port value. 	
<ul style="list-style-type: none"> • Destination Port 	<p>Specify the destination port for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No specific destination port is specified (destination port status is "don't-care"). ■ Single: If you want to filter a specific destination port with this ACE, you can enter a specific destination port value. A field for entering a destination port value appears. The allowed range is 0 to 65535. A frame that hits this ACE matches this destination port value. ■ Range: If you want to filter a specific destination port range filter with this ACE, you can enter a specific destination port range value. A field for entering a destination port value appears. 	
<ul style="list-style-type: none"> • TCP Flags 	Urg	<p>Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the Urg field is set must be able to match this entry. ■ Unset: TCP frames where the Urg field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care").
	Ack	<p>Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the Ack field is set must be able to match this entry. ■ Unset: TCP frames where the Ack field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care").
	Psh	<p>Specify the TCP "Push Function" (PSH) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the Psh field is set must be able to match this entry. ■ Unset: TCP frames where the Psh field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care").
	Rst	<ul style="list-style-type: none"> ■ Specify the TCP "Reset the connection" (RST) value for this ACE. ■ Set: TCP frames where the Rst field is set must be able to match this entry. ■ Unset: TCP frames where the Rst field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care").

	Syn	<p>Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the Syn field is set must be able to match this entry. ■ Unset: TCP frames where the Syn field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care").
	Fin	<p>Specify the TCP "No more data from sender" (FIN) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the Fin field is set must be able to match this entry. ■ Unset: TCP frames where the Fin field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care").
<ul style="list-style-type: none"> • Type of Service 	<p>Specify the type of service for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No specific type of service is specified (destination port status is "don't-care"). ■ DSCP to match: If you want to filter a specific DSCP with this ACE, you can enter a specific DSCP value. A field for entering a DSCP value appears. The allowed range is 0 to 63. A frame that hits this ACE matches this DSCP value. ■ IP Precedence to match: If you want to filter a specific IP precedence with this ACE, you can enter a specific IP precedence value. A field for entering an IP precedence value appears. The allowed range is 0 to 7. A frame that hits this ACE matches this IP precedence value. 	
<ul style="list-style-type: none"> • ICMP 	<p>Specify the ICMP for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No specific ICMP is specified (destination port status is "don't-care"). ■ Select from List: If you want to filter a specific list with this ACE, you can select a specific list value. ■ Protocol ID to match: If you want to filter a specific protocol ID filter with this ACE, you can enter a specific protocol ID value. A field for entering a protocol ID value appears. The allowed range is 0 to 255. A frame that hits this ACE matches this protocol ID value. 	
<ul style="list-style-type: none"> • ICMP Code 	<p>Specify the ICMP code filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No ICMP code filter is specified (ICMP code filter status is "don't-care"). ■ User Defined: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value. 	

Button



 : Click to add IPv4-based ACE list.



ACL Name	Sequence	Action	Protocol	Source IP Address		Destination IP Address		Source Port Range	Destination Port Range	Flag Set	DSCP	IP Precedence	ICMP Type	ICMP Code	Modify
				IP Address	Wildcard Mask	IP Address	Wildcard Mask								

Figure 4-10-8: IPv4-based ACE Table Page Screenshot

The page includes the following fields:

Object	Description
• ACL Name	Display the current ACL name.
• Sequence	Display the current sequence.
• Action	Display the current action.
• Protocol	Display the current protocol.
• Source IP Address	Display the current source IP address.
• Source IP Address Wildcard Mask	Display the current source IP address wildcard mask.
• Destination IP Address	Display the current destination IP address.
• Destination IP Address Wildcard Mask	Display the current destination IP address wildcard mask.
• Source Port Range	Display the current source port range.
• Destiantion Port Range	Display the current destination port range.
• Flag Set	Display the current flag set.
• DSCP	Display the current DSCP.
• IP Precedence	Display the current IP precedence.
• ICMP Type	Display the current ICMP Type.
• ICMP Code	Display the current ICMP code.
• Modify	Click  to edit IPv4-based ACL parameter. Click  to delete IPv4-Based ACL entry.

4.10.5 IPv6-based ACL

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. IPv6-Based ACL screens in [Figure 4-10-9](#) and [Figure 4-10-10](#) appear.



Figure 4-10-9: IPv6-based ACL Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • ACL Name 	Create a named IPv6-based ACL list.

Button



: Click to add IPv6-based ACL name list.

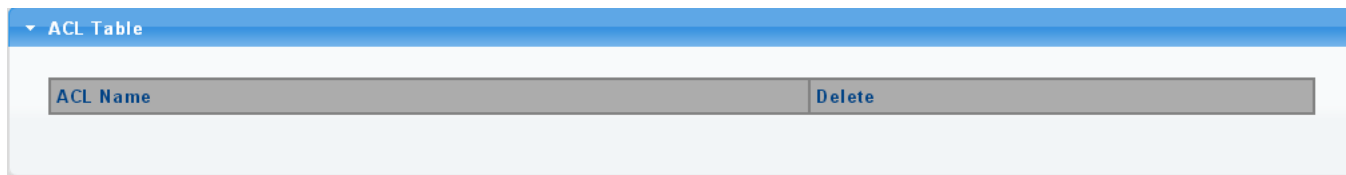



Figure 4-10-10: IPv6-based ACL Table Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Delete 	Click  to delete ACL name entry

4.10.6 IPv6-based ACE

An ACE consists of several parameters. Different parameter options are displayed depending on the frame type that you selected. The IPv6-Based ACE screens in [Figure 4-10-11](#) and [Figure 4-10-12](#) appear.

IPv6-Based ACE	
IPv6-Based ACE	
ACL Name	<input type="text"/>
Sequence	<input type="text"/> (Range: 1 - 2147483647, 1 is first processed)
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Protocol	<input checked="" type="radio"/> Any(IP) <input type="radio"/> Select from list <input type="text" value="tcp"/> <input type="radio"/> Protocol ID to match <input type="text" value="1"/>
Source IP Address	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
Source IP Address Value	<input type="text"/>
Source IP Prefix Length	<input type="text"/> (Range: 0 - 128)
Destination IP Address	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
Destination IP Address Value	<input type="text"/>
Destination IP Refix Length	<input type="text"/> (0s for matching, 1s for no matching)
Source Port	<input checked="" type="radio"/> Any <input type="radio"/> Single <input type="text"/> (Range: 0 - 65535) <input type="radio"/> Range <input type="text"/> - <input type="text" value="65535"/> (Range: 0 - 65535)
Destination Port	<input checked="" type="radio"/> Any <input type="radio"/> Single (Range: 0 - 65535) <input type="text"/> (Range: 0 - 65535) <input type="radio"/> Range (Range: 0 - 65535) <input type="text"/> - <input type="text" value="65535"/> (Range: 0 - 65535)
TCP Flags	Urg <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Ack <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Psh <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Rst <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Syn <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Fin <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care
Type of Service	<input checked="" type="radio"/> Any <input type="radio"/> DSCP to match <input type="text"/> (Range: 0 - 63) <input type="radio"/> IP Precedence to match <input type="text"/> (Range: 0 - 7)
ICMP	<input checked="" type="radio"/> Any <input type="radio"/> Select from list <input type="text" value="destinatic"/> <input type="radio"/> Protocol ID to match <input type="text"/> (Range: 0 - 255)
ICMP Code	<input checked="" type="radio"/> Any <input type="radio"/> User Defined <input type="text"/> (Range: 0 - 255)

Figure 4-10-11: IPv6-based ACE Page Screenshot


The page includes the following fields:

Object	Description
• ACL Name	Select ACL name for this drop down list.
• Sequence	Set the ACL sequence.
• Action	Indicates the forwarding action of the ACE <ul style="list-style-type: none"> ■ Permit: Frames matching the ACE may be forwarded and learned. ■ Deny: Frames matching the ACE are dropped. ■ Shutdown: Port shutdown is disabled for the ACE.
• Protocol	Specify the protocol filter for this ACE <ul style="list-style-type: none"> ■ Any (IP): No protocol filter is specified. ■ Select from list: If you want to filter a specific protocol with this ACE, choose this value and select protocol for this drop down list.
• Source IP Address	Specify the Source IP address filter for this ACE <ul style="list-style-type: none"> ■ Any: No source IP address filter is specified. ■ User Defined: If you want to filter a specific source IP address with this ACE, choose this value. A field for entering a source IP address value appears.
• Source IP Address Value	When "User Defined" is selected for the source IP address filter, you can enter a specific source IP address. The legal format is "xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx". A frame that hits this ACE matches this source IP address value.
• Source IP Prefix Length	When "User Defined" is selected for the source IP filter, you can enter a specific SIP prefix length in dotted decimal notation.
• Destination IP Address	Specify the Destination IP address filter for this ACE. <ul style="list-style-type: none"> ■ Any: No destination IP address filter is specified. ■ User Defined: If you want to filter a specific destination IP address with this ACE, choose this value. A field for entering a source IP address value appears.
• Destination IP Address Value	When "User Defined" is selected for the destination IP address filter, you can enter a specific destination IP address. The legal format is " xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx ". A frame that hits this ACE matches this destination IP address value.
• Destination IP Prefix Length	When "User Defined" is selected for the destination IP filter, you can enter a specific DIP prefix length in dotted decimal notation.
• Source Port	Specify the source port for this ACE. <ul style="list-style-type: none"> ■ Any: No specific source port is specified (source port status is "don't-care"). ■ Single: If you want to filter a specific source port with this ACE, you can enter a specific source port value. A field for entering a source port value appears. The allowed range is 0 to 65535. A frame that hits this ACE

	<p>matches this source port value.</p> <ul style="list-style-type: none"> ■ Range: If you want to filter a specific source port range filter with this ACE, you can enter a specific source port range value. A field for entering a source port value appears. The allowed range is 0 to 65535. A frame that hits this ACE matches this source port value. 								
<ul style="list-style-type: none"> • Destination Port 	<p>Specify the destination port for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No specific destination port is specified (destination port status is "don't-care"). ■ Single: If you want to filter a specific destination port with this ACE, you can enter a specific destination port value. A field for entering a destination port value appears. The allowed range is 0 to 65535. A frame that hits this ACE matches this destination port value. ■ Range: If you want to filter a specific destination port range filter with this ACE, you can enter a specific destination port range value. A field for entering a destination port value appears. 								
<ul style="list-style-type: none"> • TCP Flags 	<table border="1"> <tr> <td data-bbox="531 887 624 1211">URG</td> <td data-bbox="624 887 1410 1211"> <p>Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the URG field is set must be able to match this entry. ■ Unset: TCP frames where the URG field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care"). </td> </tr> <tr> <td data-bbox="531 1211 624 1547">ACK</td> <td data-bbox="624 1211 1410 1547"> <p>Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the ACK field is set must be able to match this entry. ■ Unset: TCP frames where the ACK field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care"). </td> </tr> <tr> <td data-bbox="531 1547 624 1839">PSH</td> <td data-bbox="624 1547 1410 1839"> <p>Specify the TCP "Push Function" (PSH) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the PSH field is set must be able to match this entry. ■ Unset: TCP frames where the PSH field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care"). </td> </tr> <tr> <td data-bbox="531 1839 624 2074">RST</td> <td data-bbox="624 1839 1410 2074"> <p>Specify the TCP "Reset the connection" (RST) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the RST field is set must be able to match this entry. ■ Unset: TCP frames where the RST field is set must not be able to match this entry. </td> </tr> </table>	URG	<p>Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the URG field is set must be able to match this entry. ■ Unset: TCP frames where the URG field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care"). 	ACK	<p>Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the ACK field is set must be able to match this entry. ■ Unset: TCP frames where the ACK field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care"). 	PSH	<p>Specify the TCP "Push Function" (PSH) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the PSH field is set must be able to match this entry. ■ Unset: TCP frames where the PSH field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care"). 	RST	<p>Specify the TCP "Reset the connection" (RST) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the RST field is set must be able to match this entry. ■ Unset: TCP frames where the RST field is set must not be able to match this entry.
URG	<p>Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the URG field is set must be able to match this entry. ■ Unset: TCP frames where the URG field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care"). 								
ACK	<p>Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the ACK field is set must be able to match this entry. ■ Unset: TCP frames where the ACK field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care"). 								
PSH	<p>Specify the TCP "Push Function" (PSH) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the PSH field is set must be able to match this entry. ■ Unset: TCP frames where the PSH field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care"). 								
RST	<p>Specify the TCP "Reset the connection" (RST) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the RST field is set must be able to match this entry. ■ Unset: TCP frames where the RST field is set must not be able to match this entry. 								

	<ul style="list-style-type: none"> ■ Don't Care: Any value is allowed ("don't-care").
SYN	<p>Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the SYN field is set must be able to match this entry. ■ Unset: TCP frames where the SYN field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care").
FIN	<p>Specify the TCP "No more data from sender" (FIN) value for this ACE.</p> <ul style="list-style-type: none"> ■ Set: TCP frames where the FIN field is set must be able to match this entry. ■ Unset: TCP frames where the FIN field is set must not be able to match this entry. ■ Don't Care: Any value is allowed ("don't-care").
<ul style="list-style-type: none"> • Type of Service 	<p>Specify the type of service for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No specific type of service is specified (destination port status is "don't-care"). ■ DSCP: If you want to filter a specific DSCP with this ACE, you can enter a specific DSCP value. A field for entering a DSCP value appears. The allowed range is 0 to 63. A frame that hits this ACE matches this DSCP value. ■ IP Precedence: If you want to filter a specific IP precedence with this ACE, you can enter a specific IP precedence value. A field for entering an IP precedence value appears. The allowed range is 0 to 7. A frame that hits this ACE matches this IP precedence value.
<ul style="list-style-type: none"> • ICMP 	<p>Specify the ICMP for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No specific ICMP is specified (destination port status is "don't-care"). ■ List: If you want to filter a specific list with this ACE, you can select a specific list value. ■ Protocol ID: If you want to filter a specific protocol ID filter with this ACE, you can enter a specific protocol ID value. A field for entering a protocol ID value appears. The allowed range is 0 to 255. A frame that hits this ACE matches this protocol ID value.
<ul style="list-style-type: none"> • ICMP Code 	<p>Specify the ICMP code filter for this ACE.</p> <ul style="list-style-type: none"> ■ Any: No ICMP code filter is specified (ICMP code filter status is "don't-care"). ■ User Defined: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.

Button

 : Click to add IPv6-based ACE list

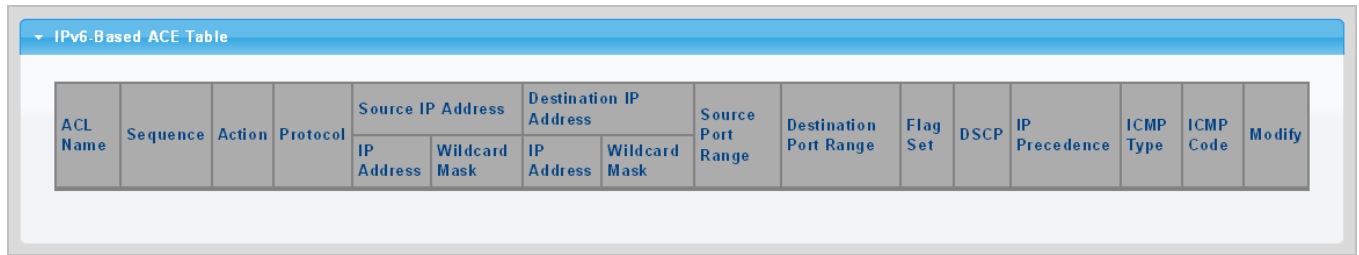




Figure 4-10-12: IPv6-based ACE Table Page Screenshot

The page includes the following fields:

Object	Description
• ACL Name	Display the current ACL name.
• Sequence	Display the current sequence.
• Action	Display the current action.
• Protocol	Display the current protocol.
• Source IP Address	Display the current source IP address.
• Source IP Address Wildcard Mask	Display the current source IP address wildcard mask.
• Destination IP Address	Display the current destination IP address.
• Destination IP Address Wildcard Mask	Display the current destination IP address wildcard mask.
• Source Port Range	Display the current source port range.
• Destination Port Range	Display the current destination port range.
• Flag Set	Display the current flag set.
• DSCP	Display the current DSCP.
• IP Precedence	Display the current IP precedence.
• ICMP Type	Display the current ICMP Type.
• ICMP Code	Display the current ICMP code.
• Modify	Click  to edit IPv6-based ACL parameter. Click  to delete IPv6-based ACL entry.

4.10.7 ACL Binding

This page allows you to bind the Policy content to the appropriate ACLs. The ACL Policy screens in [Figure 4-10-13](#) & [Figure 4-10-14](#) appears.

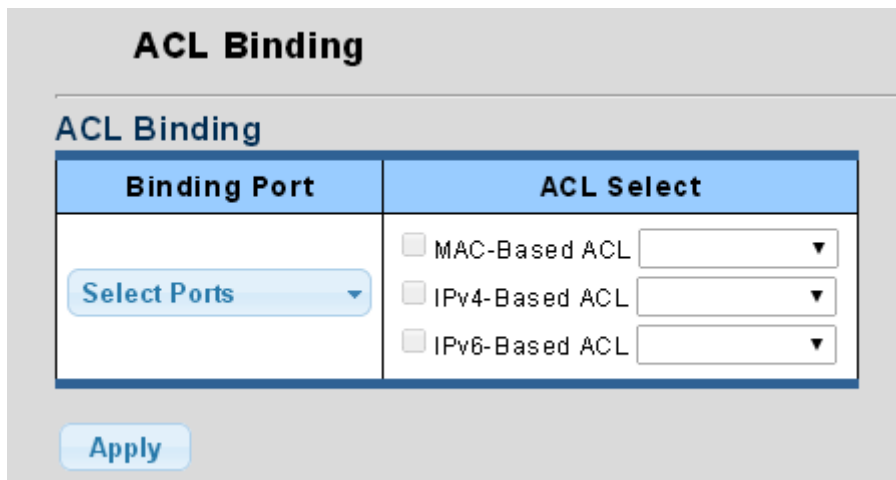



Figure 4-10-13: ACL Binding Page Screenshot

The page includes the following fields:

Object	Description
• Binding Port	Select port for this drop down list.
• ACL Select	Select ACL list for this drop down list.

Button

: Click to apply changes.

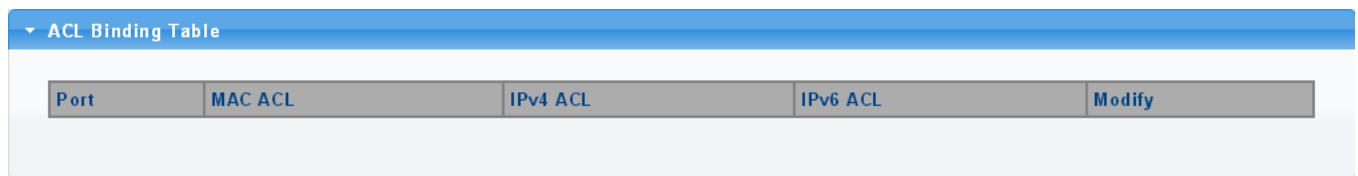




Figure 4-10-14: ACL Binding Table Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• MAC ACL	Display the current MAC ACL
• IPv4 ACL	Display the current IPv4 ACL
• IPv6 ACL	Display the current IPv6 ACL
• Modify	Click  to edit ACL binding table parameter. Click  to delete ACL binding entry.

4.11 MAC Address Table

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

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frames with the corresponding SMAC address have been seen after a configurable age time.

4.11.1 Static MAC Setting

The static entries in the MAC table are shown in this table. The MAC table is sorted first by VLAN ID and then by MAC address. The Static MAC Setting screens in [Figure 4-11-1](#) and [Figure 4-11-2](#) appear.

MAC Address	Port	VLAN
00:00:00:00:00:00	GE1	Default(1)


Add

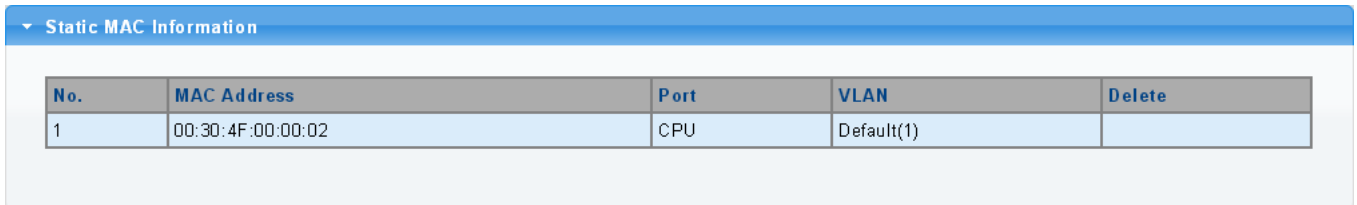
Figure 4-11-1: Static MAC Setting Page Screenshot

The page includes the following fields:

Object	Description
• MAC Address	Physical address associated with this interface.
• Port	Select port for this drop down list.
• VLAN	Select VLAN for this drop down list.

Button


: Click to add new static MAC address.



No.	MAC Address	Port	VLAN	Delete
1	00:30:4F:00:00:02	CPU	Default(1)	

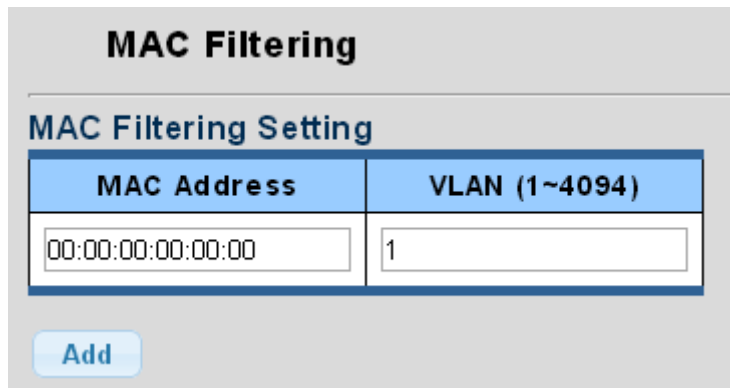
Figure 4-11-2: Static MAC Status Page Screenshot

The page includes the following fields:

Object	Description
• No.	This is the number for entries.
• MAC Address	The MAC address for the entry.
• Port	Display the current port.
• VLAN	The VLAN ID for the entry.
• Delete	Click  to delete static MAC status entry.

4.11.2 MAC Filtering

By filtering MAC address, the switch can easily filter the per-configured MAC address and reduce the un-safety. The Static MAC Setting screens in [Figure 4-11-3](#) and [Figure 4-11-4](#) appear.



MAC Filtering

MAC Filtering Setting

MAC Address	VLAN (1~4094)
00:00:00:00:00:00	1

Figure 4-11-3: MAC Filtering Setting Page Screenshot

The page includes the following fields:

Object	Description
• MAC Address	Physical address associated with this interface.
• VLAN (1~4094)	Indicates the ID of this particular VLAN.

Button

 : Click to add new MAC filtering setting.

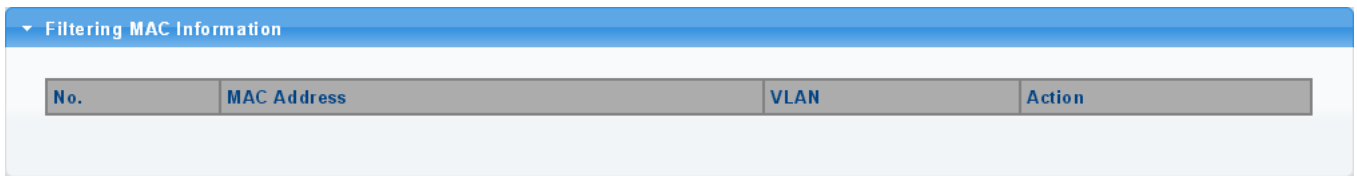



Figure 4-11-4: MAC Filter Information Page Screenshot

The page includes the following fields:

Object	Description
• No.	This is the number for entries
• MAC Address	The MAC address for the entry.
• VLAN	The VLAN ID for the entry.
• Action	Click  to delete static MAC status entry.

4.11.3 Dynamic Address Setting

By default, dynamic entries are removed from the MAC table after 300 seconds. The Dynamic Address Setting/Status screens in [Figure 4-11-5](#) and [Figure 4-11-6](#) appear.

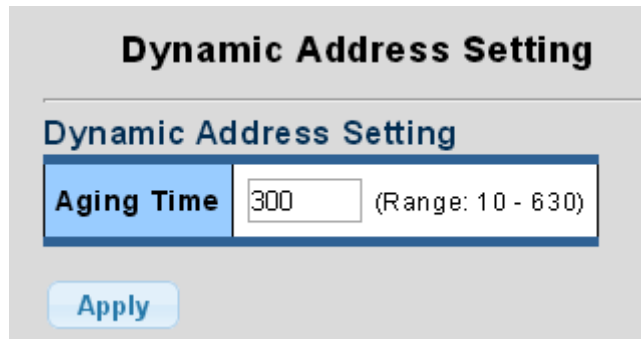


Figure 4-11-5: Dynamic Addresses Setting Page Screenshot

The page includes the following fields:

Object	Description
• Aging Time	The time after which a learned entry is discarded. (Range: 10-630 seconds; Default: 300 seconds)

Button



: Click to apply changes.

Dynamic Address Status	
Information Name	Information Value
Aging time	300

Figure 4-11-6: Dynamic Address Status Page Screenshot

The page includes the following fields:

Object	Description
• Aging Time	Display the current aging time setting information.

4.11.4 Dynamic Learned

Dynamic MAC Table

Dynamic Learned MAC Table are shown on this page. The MAC Table is sorted first by VLAN ID, then by MAC address. The Dynamic Learned screens in [Figure 4-11-7](#) and [Figure 4-11-8](#) appear.

Dynamic Learned

Port GE1 ▼
 VLAN Default ▼
 MAC Address 00:00:00:00:00:00

View
Clear

Figure 4-11-7: Dynamic Learned Page Screenshot

The page includes the following fields:

Object	Description
• Port	Select port for this drop down list.
• VLAN	Select VLAN for this drop down list.
• MAC Address	Physical address associated with this interface.

Buttons

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

Clear: Flushes all dynamic entries.

MAC Address	VLAN	Type	Port
C8:9C:DC:EC:D6:DD	Default(1)	Dynamic	GE24

Total Entries:1

Figure 4-11-8: MAC Address Information Page Screenshot

Object	Description
• MAC Address	The MAC address of the entry.
• VLAN	The VLAN ID of the entry.
• Type	Indicates whether the entry is a static or dynamic entry.
• Port	The ports that are members of the entry.

Button

: Click to add dynamic MAC address to static MAC address.

4.11.5 RMA Setting**Reserved MAC Addresses**

Reserved MAC Addresses setting are shown on this page. This page provides “**Peer**”, “**Bridge**” and “**Discard**” in Action mode for specific MAC address. The Reserved MAC Addresses setting screens in [Figure 4-11-9](#) and [Figure 4-11-10](#) appear.


Reserved MAC Addresses Setting				
<table border="1"> <tr> <td>MAC Address</td> <td>Select MAC Address</td> </tr> <tr> <td>Action</td> <td> <input type="radio"/> Peer <input checked="" type="radio"/> Bridge <input type="radio"/> Discard </td> </tr> </table>	MAC Address	Select MAC Address	Action	<input type="radio"/> Peer <input checked="" type="radio"/> Bridge <input type="radio"/> Discard
MAC Address	Select MAC Address			
Action	<input type="radio"/> Peer <input checked="" type="radio"/> Bridge <input type="radio"/> Discard			
Apply				

Figure 4-11-9: Reserved MAC Addresses Page Screenshot

The page includes the following fields:

Object	Description
• MAC Address	Select MAC Address from this drop down list.
• Action	Select “ Peer ”, “ Bridge ” and “ Discard ” for specific MAC address.

Button

: Click to apply changes.

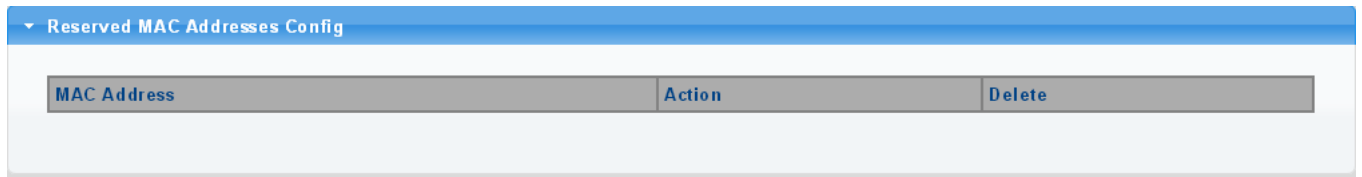



Figure 4-11-10: Reserved MAC Addresses StatusPage Screenshot

Object	Description
<ul style="list-style-type: none"> • MAC Address 	The MAC address of the entry.
<ul style="list-style-type: none"> • Action 	Display current Action mode.
<ul style="list-style-type: none"> • Delete 	Click  to delete Reserved MAC Addresses status entry.

4.12 LLDP

4.12.1 Link Layer Discovery Protocol

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

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

4.12.2 LLDP Global Setting

This page allows the user to inspect and configure the current LLDP port settings. The LLDP Global Setting and Config screens in [Figure 4-12-1](#) and [Figure 4-12-2](#) appear.

LLDP Global Setting

LLDP Global Settings

Enabled	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
LLDP PDU Disable Action	<input type="radio"/> Filtering <input type="radio"/> Bridging <input checked="" type="radio"/> Flooding
Transmission Interval	<input type="text" value="30"/> (5-32768)
Check-Change Interval	<input type="text" value="4"/> (2-10)
Reinitialization Delay	<input type="text" value="2"/> (1-10)
Transmit Delay	<input type="text" value="2"/> (1-8192)
LLDP-MED Fast Start Repeat Count	<input type="text" value="3"/> (1-10)

Figure 4-12-1: LLDP Global Setting Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Enable 	<p>Enable or disable LLDP globally function.</p>
<ul style="list-style-type: none"> • LLDP PDU Disable Action 	<p>Set LLDP PDU disable action: include "Filtering", "Bridging" and "Flooding".</p> <ul style="list-style-type: none"> ■ Filtering: discard all LLDP PDU. ■ Bridging: transmit LLDP PDU in the same VLAN. ■ Flooding: transmit LLDP PDU for all port.
<ul style="list-style-type: none"> • Transmission Interval 	<p>The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Transmission Interval value. Valid values are restricted to 5 - 32768 seconds.</p> <p>Default: 30 seconds</p> <p>This attribute must comply with the following rule:</p> <p>$(\text{Transmission Interval} * \text{Hold Time Multiplier}) \leq 65536$, and $\text{Transmission Interval} \geq (4 * \text{Delay Interval})$</p>
<ul style="list-style-type: none"> • Check-Change Interval 	<p>Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Holdtime multiplied by Transmission Interval seconds. Valid values are restricted to 2 - 10 times.</p> <p>TTL in seconds is based on the following rule:</p> <p>$(\text{Transmission Interval} * \text{Holdtime Multiplier}) \leq 65536$.</p> <p>Therefore, the default TTL is $4 * 30 = 120$ seconds.</p>
<ul style="list-style-type: none"> • Reinitialization Delay 	<p>When a port is disabled, LLDP is disabled or the switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.</p>
<ul style="list-style-type: none"> • Transmit Delay 	<p>If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Transmit Delay seconds. Transmit Delay cannot be larger than 1/4 of the Transmission Interval value. Valid values are restricted to 1 - 8192 seconds.</p> <p>This attribute must comply with the rule:</p> <p>$(4 * \text{Delay Interval}) \leq \text{Transmission Interval}$</p>
<ul style="list-style-type: none"> • LLDP-MED Fast Start Repeat Count 	<p>Configures the amount of LLDP MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism.</p> <p>Range: 1-10 packets;</p>

	<p>Default: 3 packets</p> <p>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. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.</p>
--	---

Button



: Click to apply changes.

LLDP Global Config

Config Name	Config Value
LLDP Enabled	Disabled
LLDP PDU Disable Action	Flooding
Transmission Interval	30 Secs
Check-Change Interval	4
Reinitialization Delay	2 Secs
Transmit Delay	2 Secs
LLDP-MED Fast Start Repeat Count	3 PDUs

Figure 4-12-2: LLDP Global Config Page Screenshot

The page includes the following fields:

Object	Description
• LLDP Enable	Display the current LLDP status.
• LLDP PDU Disable Action	Displays the current LLDP PDU disable action.
• Transmission Interval	Display the current transmission interval informaiton.
• Check-Change Interval	Display the current check-change interval informaiton.
• Reinitialization Delay	Display the current reinitialization delay informaiton.
• Transmit Delay	Displays the current transmit delay informaiton.
• LLDP-MED Fast Start Repeat Count	Display the current LLDP-MED Fast Start Repeat Count informaiton.

4.12.3 LLDP Port Setting

Use the LLDP Port Setting to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received. The LLDP Port Configuration and Status screens in [Figure 4-12-3](#) and [Figure 4-12-4](#) appear.

Figure 4-12-3: LLDP Port Configuration and Optional TLVs Selection Page Screenshot

The page includes the following fields:

Object	Description
• Port Select	Select port for this drop down list.
• State	Enables LLDP messages transmit and receive modes for LLDP Protocol Data Units. Options: <ul style="list-style-type: none"> ■ Disable (Default) ■ Rx ONLY ■ Tx ONLY ■ TX & RX
• Port Select	Select port for this drop down list.
• Optional TLV Select	Configures the information included in the TLV field of advertised messages. <ul style="list-style-type: none"> ■ System Name: When checked the "System Name" is included in LLDP information transmitted. ■ Port Description: When checked the "Port Description" is included in LLDP information transmitted. ■ System Description: When checked the "System Description" is included in LLDP information transmitted.

	<ul style="list-style-type: none"> ■ System Capability: When checked the "System Capability" is included in LLDP information transmitted. ■ 802.3 MAC-PHY: When checked the "802.3 MAC-PHY" is included in LLDP information transmitted. ■ 802.3 Link Aggregation: When checked the "802.3 Link Aggregation" is included in LLDP information transmitted. ■ 802.3 Maximun Frame Size: When checked the "802.3 Maximun Frame Size" is included in LLDP information transmitted. ■ 802.1 PVID: When checked the "802.1 PVID" is included in LLDP information transmitted.
--	---

Button



: Click to apply changes.

LLDP Port Status

Port	State	Selected Optional TLVs
GE1	TX & RX	802.1 PVID
GE2	TX & RX	802.1 PVID
GE3	TX & RX	802.1 PVID
GE4	TX & RX	802.1 PVID
GE5	TX & RX	802.1 PVID
GE6	TX & RX	802.1 PVID
GE7	TX & RX	802.1 PVID
GE8	TX & RX	802.1 PVID
GE9	TX & RX	802.1 PVID
GE10	TX & RX	802.1 PVID
GE11	TX & RX	802.1 PVID
GE12	TX & RX	802.1 PVID
GE13	TX & RX	802.1 PVID
GE14	TX & RX	802.1 PVID
GE15	TX & RX	802.1 PVID
GE16	TX & RX	802.1 PVID
GE17	TX & RX	802.1 PVID
GE18	TX & RX	802.1 PVID
GE19	TX & RX	802.1 PVID
GE20	TX & RX	802.1 PVID
GE21	TX & RX	802.1 PVID
GE22	TX & RX	802.1 PVID
GE23	TX & RX	802.1 PVID
GE24	TX & RX	802.1 PVID
GE25	TX & RX	802.1 PVID
GE26	TX & RX	802.1 PVID

Figure 4-12-4 : LLDP Port Status Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	The switch port number of the logical port.
<ul style="list-style-type: none"> • State 	Display the current LLDP status.
<ul style="list-style-type: none"> • Selected Optional TLVs 	Display the current selected optional TLVs setting.

The VLAN Name TLV VLAN Selection and LLDP Port VLAN TLV Status screens in [Figure 4-12-5](#) and [Figure 4-12-6](#) appear.

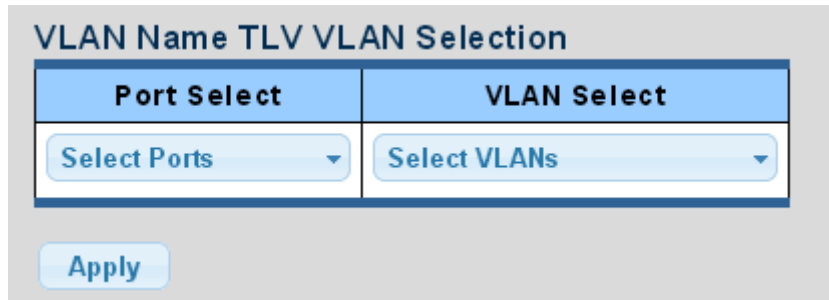


Figure 4-12-5: VLAN Name TLV VLAN Selection Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port Select 	Select port from this drop down list.
<ul style="list-style-type: none"> • VLAN Select 	Select VLAN from this drop down list.

Button

: Click to apply changes.

LLDP Port VLAN TLV Status	
Port	Selected VLAN
GE1	
GE2	
GE3	
GE4	
GE5	
GE6	
GE7	
GE8	
GE9	
GE10	
GE11	
GE12	
GE13	
GE14	
GE15	
GE16	
GE17	
GE18	
GE19	
GE20	
GE21	
GE22	
GE23	
GE24	
GE25	
GE26	

Figure 4-12-6: LLDP Port VLAN TLV Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Selected VLAN	Display the current selected VLAN.

4.12.4 LLDP Local Device

Use the LLDP Local Device Information screen to display information about the switch, such as its **MAC address**, **chassis ID**, **management IP address**, and **port information**. The Local Device Summary and Port Status screens in [Figure 4-12-7](#) and [Figure 4-12-8](#) appear.

LLDP Local Device	
Local Device Summary	
Chassis ID Subtype	MAC Address
Chassis ID	00:30:4F:AF:FF:81
System Name	GS-4210-24P2S
System Description	V1
Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Interface name

Figure 4-12-7: Local Device Summary Page Screenshot

The page includes the following fields:

Object	Description
• Chassis ID Subtype	Display the current chassis ID subtype.
• Chassis ID	Display the current chassis ID.
• System Name	Display the current system name.
• System Description	Display the current system description.
• Capabilities Supported	Display the current capabilities supported.
• Capabilities Enabled	Display the current capabilities enabled.
• Port ID Subtype	Display the current port ID subtype.

	Interface	LLDP Status	LLDP Med Status	
<input type="radio"/>	GE1	TX & RX	Enabled	N/A
<input type="radio"/>	GE2	TX & RX	Enabled	N/A
<input type="radio"/>	GE3	TX & RX	Enabled	N/A
<input type="radio"/>	GE4	TX & RX	Enabled	N/A
<input type="radio"/>	GE5	TX & RX	Enabled	N/A
<input type="radio"/>	GE6	TX & RX	Enabled	N/A
<input type="radio"/>	GE7	TX & RX	Enabled	N/A
<input type="radio"/>	GE8	TX & RX	Enabled	N/A
<input type="radio"/>	GE9	TX & RX	Enabled	N/A
<input type="radio"/>	GE10	TX & RX	Enabled	N/A
<input type="radio"/>	GE11	TX & RX	Enabled	N/A
<input type="radio"/>	GE12	TX & RX	Enabled	N/A
<input type="radio"/>	GE13	TX & RX	Enabled	N/A

Figure 4-12-8: Port Status Page Screenshot

The page includes the following fields:

Object	Description
• Interface	The switch port number of the logical port.
• LLDP Status	Display the current LLDP status
• LLDP MED Status	Display the current LLDP MED Status

Detail: press the “**Detail**” button then the following detail LLDP Local Device Detail information appears. Press “**Back**” button for back to previous Port Status screen. The Global Information screen in Figure 4-12-9 appears.

Global	
Chassis ID Subtype	MAC address
Chassis ID	00:30:4F:AF:FF:81
System Name	GS-4210-24P2S
System Description	
Supported System Capabilities	Bridge
Enabled System Capabilities	Bridge
Port ID Subtype	Interface name
Port ID	gi1
Port Description	
Management Address	

Figure 4-12-9: Global Information Page Screenshot

The page includes the following fields:

Object	Description
• Chassis ID Subtype	Display current chassis ID Subtype information.
• Chassis ID	Display the current chassis ID information.
• System Name	Display the current system name.
• System Description	Display the current system description.
• Supported System Capabilities	Display the current supported system capabilities information.
• Enabled System Capabilities	Display the current enabled system capabilities information.
• Port ID Subtype	Display the current port ID Subtype information.
• Port ID	Display the current port ID information.
• Port Description	Display the current port description information.
• Management Address	Display the current management address information.

The MAC/PHY Details Information screen in [Figure 4-12-10](#) appears.

MAC/PHY Details	
Auto-Negotiation Supported	N/A
Auto-Negotiation Enabled	N/A
Auto-Negotiation Advertised Capabilities	N/A
Operational MAU Type	N/A

Figure 4-12-10: MAC/PHY Details Information Page Screenshot

The page includes the following fields:

Object	Description
• Auto-Negotiation Supported	Display current auto-negotiation supported information.
• Auto-Negotiation Enabled	Display the current auto-negotiation enabled information.
• Auto-Neogitaion Advertised Capailities	Display the current auto-neogitaion advertised capailities information.
• Operational MAU Type	Display the current operational MAU type information.

The 802.3 Details Information screen in [Figure 4-12-11](#) appears.

802.3 Details	
802.3 Maximum Frame Size	N/A

Figure 4-12-11: 802.3 Details Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> 802.3 Maximum Frame Size 	Display current 802.3 maximum frame size information.

The 802.3 Link Aggregation Information screen in [Figure 4-12-12](#) appears.

802.3 Link Aggregation	
Aggregation Capability	N/A
Aggregation Status	N/A
Aggregation Port ID	N/A

Figure 4-12-12: 802.3 Link Aggregation Information Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Aggregation Capability 	Display current aggregation capability information.
<ul style="list-style-type: none"> Aggregation Status 	Display current aggregation status information.
<ul style="list-style-type: none"> Aggregation Port ID 	Display current aggregation port ID information.

The MED Details Information screen in [Figure 4-12-13](#) appears.

MED Details	
Capabilities Supported	Capabilities, Network Policy
Current Capabilities	Capabilities, Network Policy
Device Class	Network Connectivity
PoE Device Type	N/A
PoE Power Source	N/A
PoE Power Priority	N/A
PoE Power Value	N/A
Hardware Revision	N/A
Firmware Revision	N/A
Software Revision	N/A
Serial Number	N/A
Manufacturer Name	N/A
Model Name	N/A
Asset ID	N/A

Figure 4-12-13: MED Detailed Information Page Screenshot

The page includes the following fields:

Object	Description
• Capabilities Supported	Display current capabilities supported information.
• Current Capabilities	Display current capabilities information.
• Device Class	Display current device class information.
• PoE Device Type *	Display current PoE device type information.
• PoE Power Source*	Display current PoE power source information.
• PoE Power Priority*	Display current PoE power priority information.
• PoE Power Value*	Display current PoE power value information.
• Hardware Revision	Display current hardware revision information.
• Firmware Revision	Display current firmware revision information.
• Software Revision	Display current software revision information.
• Serial Number	Display current serial number information.
• Manufacturer Name	Display current manufacturer name information.
• Model Name	Display current model name information.
• Asset ID	Display current asset ID information.



The items with * mark are only available at GS-4210-24P2S.

The 802.1 VLAN and Protocol Information screen in [Figure 4-12-14](#) appears.

802.1 VLAN and Protocol	
PVID	N/A
VLAN Names	N/A

Figure 4-12-14: 802.1 VLAN and Protocol Information Page Screenshot

The page includes the following fields:

Object	Description
• PVID	Display current PVID information.
• VLAN Names	Display current VLAN Names information.

The Location Information screen in [Figure 4-12-15](#) appears.

Location Information	
Civic	N/A
Coordinates	N/A
ECS ELIN	N/A

Figure 4-12-15: Location Information Page Screenshot

The page includes the following fields:

Object	Description
• Civic	Display current civic information.
• Coordinates	Display current coordinates information.
• ECS ELIN	Display current ECS ELIN information.

The Network Policy Table screen in [Figure 4-12-16](#) appears.

Network Policy Table				
Application Type	VLAN ID	VLAN Type	User Priority	DSCP
Voice	1	Tagged VLAN	0	0

Figure 4-12-16: Network Policy Table Page Screenshot

The page includes the following fields:

Object	Description
• Application Type	Display current application type information.
• VLAN ID	Display current VLAN ID information.
• VLAN Type	Display current VLAN Type information.
• User Priority	Display current user priority information.
• DSCP	Display current DSCP information.

4.12.5 LLDP Remote Device

This Page provides a status overview for all LLDP remote devices. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP Remote Device screen in [Figure 4-12-17](#) appears.

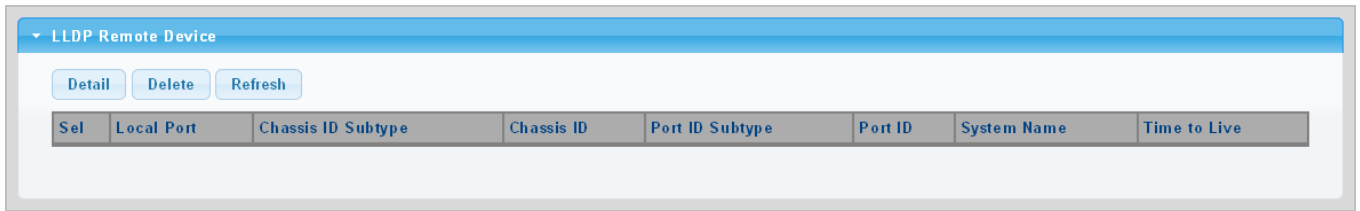


Figure 4-12-17: LLDP Remote Device Page Screenshot

The page includes the following fields:

Object	Description
• Sel	Display current sel information.
• Local Port	Display the current local port.
• Chassis ID Subtype	Display the current chassis ID subtype.
• Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
• Port ID Subtype	Display the current port ID subtype.
• Port ID	The Remote Port ID is the identification of the neighbor port.
• System Name	System Name is the name advertised by the neighbor unit.
• Time to Live	Display the current time to live.

Buttons

Delete

: Click to delete LLDP remote device entry.

Refresh

: Click to refresh LLDP remote device.

4.12.6 MED Network Policy

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

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

The network policy attributes advertised are:

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

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

The application types specifically addressed are:

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

A large network may support multiple VoIP policies across the entire organization, and different policies per application type.

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

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

The Voice Auto Mode Configuration, Network Policy Configuration and LLDP MED Network Policy Table screen in [Figure 4-12-18](#) and [Figure 4-12-19](#) appear.

LLDP MED Network Policy Setting

Voice Auto Mode Configuration

LLDP MED Policy for Voice Application

Auto Manual

Apply

Network Policy Configuration

Network Policy Number	1 ▾
Application	Voice ▾
VLAN ID	1 (1-4095)
VLAN Tag	<input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
L2 Priority	0 (0-7)
DSCP Value	0 (0-63)

Apply


Figure 4-12-18: Voice Auto Mode Configuration and Network Policy Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> LLDP MED Policy for Voice Application 	<p>Set the LLDP MED policy for voice application mode. The options are shown as below:</p> <p>Auto (Default)</p> <p>Manual</p>
<ul style="list-style-type: none"> Network Policy Number 	<p>Select network policy number for this drop down list.</p>
<ul style="list-style-type: none"> Application Type 	<p>Intended use of the application types:</p> <p>Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.</p> <p>Voice Signaling - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.</p> <p>Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.</p>

	<p>Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.</p> <p>Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.</p> <p>Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.</p> <p>App Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.</p> <p>Video Signaling - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.</p>
<ul style="list-style-type: none"> • VLAN ID 	<p>VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. The range is 1-4095.</p>
<ul style="list-style-type: none"> • VLAN Tag 	<p>Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.</p> <p>Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.</p>
<ul style="list-style-type: none"> • L2 Priority 	<p>L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.</p>
<ul style="list-style-type: none"> • DSCP Value 	<p>DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.</p>

Button

: Click to apply changes.

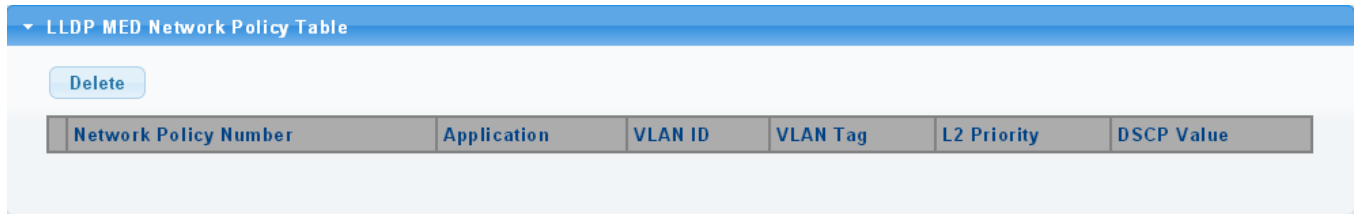


Figure 4-12-19: LLDP MED Network Policy Table Page Screenshot

The page includes the following fields:

Object	Description
• Network Policy Number	Display the current network policy number.
• Application	Display the current application.
• VLAN ID	Display the current VLAN ID.
• VLAN Tag	Display the current VLAN tag status.
• L2 Priority	Display the current L2 priority.
• DSCP Value	Dusplay the current DSCP value.

Button

: Click to delete LLDP MED network policy table entry.

4.12.7 MED Port Setting

The Port LLDP MED Configuration/Port Setting Table screens in [Figure 4-12-20](#) and [Figure 4-12-21](#) appear.

LLDP Port MED Setting

Port LLDP MED Configuration

Port Select	MED Enable	MED Optional TLVs	MED Network Policy
Select Ports ▼	Enable ▼	Select Optional TLVs ▼	Select Optional TLVs ▼

Apply

Figure 4-12-20: Port LLDP MED Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Port Select	Select port for this drop down list.
• MED Enable	Enable or disable MED configuration.
• MED Optional TVLs	Configures the information included in the MED TLV field of advertised messages. -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. -Location – This option advertises location identification details. -Inventory – This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.
• MED Network Policy	Select MED network policy for this drop down list.

Button

: Click to apply changes.

▼ LLDP MED Port Setting Table

Interface	LLDP MED Status	User Defined Network Policy		Location	Inventory
		Active	Application		
GE1	Enabled	Yes		No	No
GE2	Enabled	Yes		No	No
GE3	Enabled	Yes		No	No
GE4	Enabled	Yes		No	No
GE5	Enabled	Yes		No	No
GE6	Enabled	Yes		No	No
GE7	Enabled	Yes		No	No
GE8	Enabled	Yes		No	No
GE9	Enabled	Yes		No	No
GE10	Enabled	Yes		No	No
GE11	Enabled	Yes		No	No
GE12	Enabled	Yes		No	No
GE13	Enabled	Yes		No	No
GE14	Enabled	Yes		No	No
GE15	Enabled	Yes		No	No
GE16	Enabled	Yes		No	No
GE17	Enabled	Yes		No	No
GE18	Enabled	Yes		No	No
GE19	Enabled	Yes		No	No
GE20	Enabled	Yes		No	No
GE21	Enabled	Yes		No	No
GE22	Enabled	Yes		No	No
GE23	Enabled	Yes		No	No
GE24	Enabled	Yes		No	No
GE25	Enabled	Yes		No	No
GE26	Enabled	Yes		No	No

Figure 4-12-21: LLDP MED Port Setting Table Page Screenshot

The page includes the following fields:

Object	Description
• Interface	The switch port number of the logical port.
• LLDP MED Status	Display the current LLDP MED status..
• Active	Display the current active status.
• Application	Display the current application.
• Location	Display the current location.
• Inventory	Display the current inventory.

The MED Location Configuration and LLDP MED Port Location Table screens in [Figure 4-12-22](#) and [Figure 4-12-23](#) appear.

Figure 4-12-22: MED Location Configuration Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Ports 	Select port for this drop down list.
<ul style="list-style-type: none"> • Location Coordinate 	A string identifying the Location Coordinate that this entry should belong to.
<ul style="list-style-type: none"> • Location Civic Address 	A string identifying the Location Civic Address that this entry should belong to.
<ul style="list-style-type: none"> • Location ESC ELIN 	A string identifying the Location ESC ELIN that this entry should belong to.

Button



: Click to apply changes.

LLDP MED Port Location Table

Port	Coordinate	Civic Address	ECS ELIN
GE1			
GE2			
GE3			
GE4			
GE5			
GE6			
GE7			
GE8			
GE9			
GE10			
GE11			
GE12			
GE13			
GE14			
GE15			
GE16			
GE17			
GE18			
GE19			
GE20			
GE21			
GE22			
GE23			
GE24			
GE25			
GE26			

Figure 4-12-23: LLDP MED Port Location Table Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Coordinate	Display the current coordinate.
• Civic Address	Display the current civic address.
• ESC ELIN	Display the current ESC ELIN.

4.12.8 LLDP Overloading

The LLDP Port Overloading screen in [Figure 4-12-24](#) appears.

LLDP Port Overloading												
- LLDP Port Overloading Table												
Interface	Total(Bytes)	Left to Send(Bytes)	Status	Status								
				Mandatory TLVs	MED Capabilities	MED Location	MED Network Policy	MED Extended Power via MDI	802.3 TLVs	Optional TLVs	MED Inventory	802.1 TLVs
GE1	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE2	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE3	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE4	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE5	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE6	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE7	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE8	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE9	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE10	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE11	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE12	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE13	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE14	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE15	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE16	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE17	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE18	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE19	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE20	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE21	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE22	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE23	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE24	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE25	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE26	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)

Figure 4-12-24: LLDP Port Overloading Table Page Screenshot

The page includes the following fields:

Object	Description
• Interface	The switch port number of the logical port.
• Total (Bytes)	Total number of bytes of LLDP information that is normally sent in a packet.
• Left to Send (Bytes)	Total number of available bytes that can also send LLDP information in a packet.
• Status	Gives the status of the TLVs.
• Mandatory TLVs	Displays if the mandatory group of TLVs were transmitted or overloaded.
• MED Capabilities	Displays if the capabilities packets were transmitted or overloaded.
• MED Location	Displays if the location packets were transmitted or overloaded.
• MED Network Policy	Displays if the network policies packets were transmitted or overloaded.
• MED Extended Power via MDI	Displays if the extended power via MDI packets were transmitted or overloaded.
• 802.3 TLVs	Displays if the 802.3 TLVs were transmitted or overloaded.
• Optional TLVs	If the LLDP MED extended power via MDI packets were sent, or if they were overloaded.
• MED Inventory	Displays if the mandatory group of TLVs was transmitted or overloaded.
• 802.1 TLVs	Displays if the 802.1 TLVs were transmitted or overloaded.

4.12.9 LLDP Statistics

Use the LLDP Device Statistics screen to general statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces. The LLDP Global and Port Statistics screens in [Figure 4-12-25](#) and [Figure 4-12-26](#) appear.

LLDP Statistics	
▼ LLDP Global Statistics	
<input type="button" value="Clear"/> <input type="button" value="Refresh"/>	
Insertions	0
Deletions	0
Drops	0
Age Outs	0

Figure 4-12-25: LLDP Global Statistics Page Screenshot

The page includes the following fields:

Object	Description
• Insertions	Shows the number of new entries added since switch reboot.
• Deletions	Shows the number of new entries deleted since switch reboot.
• Drops	Shows the number of LLDP frames dropped due to that the entry table was full.
• Age Outs	Shows the number of entries deleted due to Time-To-Live expiring.

Buttons



: Click to clear the statistics.



: Click to refresh the statistics.

LLDP Port Statistics

Port	TX Frames	RX Frames			RX TLVs		RX Ageouts
	Total	Total	Discarded	Errors	Discarded	Unrecognized	Total
GE1	0	0	0	0	0	0	0
GE2	0	0	0	0	0	0	0
GE3	0	0	0	0	0	0	0
GE4	0	0	0	0	0	0	0
GE5	0	0	0	0	0	0	0
GE6	0	0	0	0	0	0	0
GE7	0	0	0	0	0	0	0
GE8	0	0	0	0	0	0	0
GE9	0	0	0	0	0	0	0
GE10	0	0	0	0	0	0	0
GE11	0	0	0	0	0	0	0
GE12	0	0	0	0	0	0	0
GE13	0	0	0	0	0	0	0
GE14	0	0	0	0	0	0	0
GE15	0	0	0	0	0	0	0
GE16	0	0	0	0	0	0	0
GE17	0	0	0	0	0	0	0
GE18	0	0	0	0	0	0	0
GE19	0	0	0	0	0	0	0
GE20	0	0	0	0	0	0	0
GE21	0	0	0	0	0	0	0
GE22	0	0	0	0	0	0	0
GE23	0	0	0	0	0	0	0
GE24	0	0	0	0	0	0	0
GE25	0	0	0	0	0	0	0
GE26	0	0	0	0	0	0	0

Figure 4-12-26: LLDP Port Statistics Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	The port on which LLDP frames are received or transmitted.
<ul style="list-style-type: none"> • TX Frame – Total 	The number of LLDP frames transmitted on the port.
<ul style="list-style-type: none"> • RX Frame – Total 	The number of LLDP frames received on the port.
<ul style="list-style-type: none"> • RX Frame – Discarded 	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
<ul style="list-style-type: none"> • RX Frame – Errors 	The number of received LLDP frames containing some kind of error.
<ul style="list-style-type: none"> • RX TLVs – Discarded 	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
<ul style="list-style-type: none"> • RX TLVs – Unrecognized 	The number of well-formed TLVs, but with an unknown type value.
<ul style="list-style-type: none"> • RX Ageout - Total 	The number of organizationally TLVs received.

4.13 Diagnostics

This section provides the system CPU / memory usage status and IP layer network diagnostics tool for troubleshooting. The diagnostic tool is designed for network manager to help them quickly diagnose problems between point to point and better service customers.

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

This section has the following items:

- **Cable Diagnostics**
- **System Status**
- **Ping Test**
- **IPv6 Ping Test**
- **Trace Router**

4.13.1 Cable Diagnostics

The Cable Diagnostics performs tests on copper cables. These functions have the ability to identify the cable length and operating conditions, and to isolate a variety of common faults that can occur on the Cat5 twisted-pair cabling. There might be two statuses as follow:

- If the link is established on the twisted-pair interface in 1000BASE-T mode, the Cable Diagnostics can run without disruption of the link or of any data transfer.
- If the link is established in 100BASE-TX or 10BASE-T, the Cable Diagnostics cause the link to drop while the diagnostics are running.

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

- Coupling between cable pairs.
- Cable pair termination
- Cable Length



Cable Diagnostics is only accurate for cables of length from 15 to 100 meters.

The Copper test and test result screens in [Figure 4-13-1](#) and [Figure 4-13-2](#) appear.

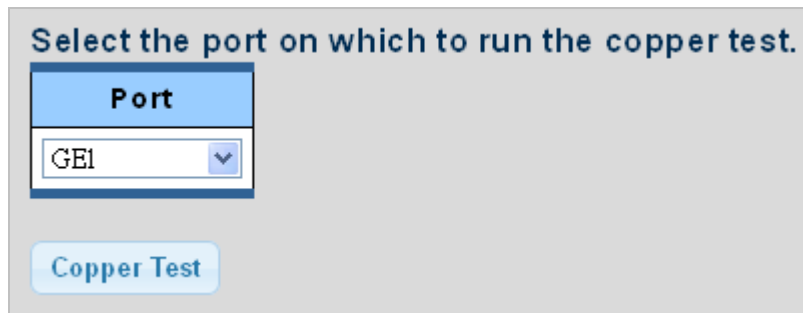


Figure 4-13-1: Copper Test Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	Select port for this drop down list

Button

Copper Test : Click to run the diagnostics

▼ Test Results									
Port	Channel A	Cable Length A	Channel B	Cable Length B	Channel C	Cable Length C	Channel D	Cable Length D	Result
GE24	NORMAL		NORMAL		NORMAL		NORMAL		PASS

Figure 4-13-2: Test Results Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	The port where you are requesting Cable Diagnostics.
<ul style="list-style-type: none"> • Channel A~D 	Display the current channel status.
<ul style="list-style-type: none"> • Cable Length A~D 	Display the current cable length.
<ul style="list-style-type: none"> • Result 	Display the test result.

4.13.2 System Status

The system status provides and display current system CPU and memory usage status. The system status screen in [Figure 4-13-3](#) appears.

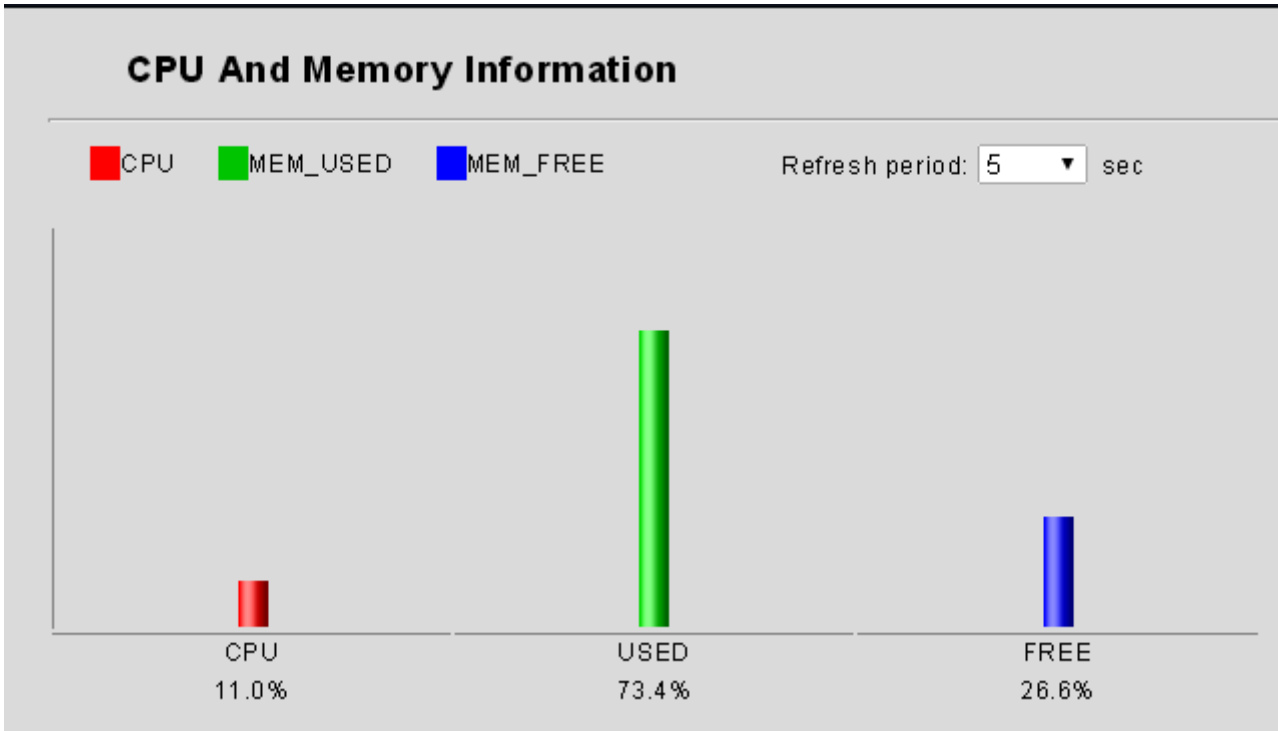


Figure 4-13-3: CPU and Memory Information Page Screenshot

The page includes the following fields:

Object	Description
• CPU	Display the current CPU usage status.
• MEM_USED	Display the current memory usage status.
• MEM_FREE	Display the current free memory status.
• Refresh Period	Provide 5 and 10 seconds for refresh period.

4.13.3 Ping Test

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues. After you press “**Apply**”, ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping screen in [Figure 4-13-4](#) appears.

Ping Test

Ping Test Setting

IP Address	<input type="text" value="192.168.1.100"/> (x.x.x.x or hostname)
Count	<input type="text" value="4"/> (1 - 5 Default : 4)
Interval (in sec)	<input type="text" value="1"/> (1 - 5 Default : 1)
Size (in bytes)	<input type="text" value="56"/> (8 - 5120 Default : 56)
Ping Results	<div style="border: 1px solid black; height: 150px; width: 100%;"></div>

Apply

Figure 4-13-4: IPv4 Ping Test Setting Page Screenshot

The page includes the following fields:

Object	Description
• IP Address	The destination IP Address.
• Count	Number of echo requests to send. The range is 1-5 and default is 4.
• Interval (in sec)	Send interval for each ICMP packet. The range is 1-5 and default is 1.
• Size (in bytes)	The payload size of the ICMP packet. Values range from 8bytes to 5120bytes.
• Ping Results	Display the current ping result.

Button

Apply: Click to transmit ICMPv4 packets.



Be sure the target IP Address is within the same network subnet of the Managed Switch, or you have to set up the correct gateway IP address.

4.13.4 IPv6 Ping Test

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you press “Apply”, 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMPv6 Ping screen in [Figure 4-13-5](#) appears.

Ping Test

Ping Test Setting

IPv6 Address	<input style="width: 90%;" type="text" value=""/> <small>(XX:XX:XXXX)</small>
Count	<input style="width: 20%;" type="text" value="4"/> (1 - 5 Default : 4)
Interval (in sec)	<input style="width: 20%;" type="text" value="1"/> (1 - 5 Default : 1)
Size (in bytes)	<input style="width: 20%;" type="text" value="56"/> (8 - 512 Default : 56)

Ping Results	
---------------------	--

Figure 4-13-5: IPv6 Ping Page Screenshot

The page includes the following fields:

Object	Description
• IPv6 Address	The destination IPv6 Address.
• Count	Number of echo requests to send. The range is 1-5 and default is 4.
• Interval (in sec)	Send interval for each ICMP packet. The range is 1-5 and default is 1.
• Size (in bytes)	The payload size of the ICMP packet. Values range from 8bytes to 5120bytes.
• Ping Results	Display the current ping result.

Button



: Click to transmit ICMPv6 packets

4.13.5 Trace Router

Traceroute function is for testing the gateways through which the data packets travel from the source device to the destination device, so to check the network accessibility and locate the network failure.

Execution procedure of the Traceroute function consists of: first a data packet with TTL at 1 is sent to the destination address, if the first hop returns an ICMP error message to inform this packet can not be sent (due to TTL timeout), a data packet with TTL at 2 will be sent. Also the send hop may be a TTL timeout return, but the procedure will carries on till the data packet is sent to its destination. These procedures is for recording every source address which returned ICMP TTL timeout message, so to describe a path the IP data packets traveled to reach the destination. The Trace Route Setting screen in [Figure 4-13-6](#) appears.

Trace Route

Trace Route Setting

IP Address	<input type="text" value="192.168.1.100"/> (x.x.x.x or hostname)
Max Hop	<input type="text" value="30"/> (2 - 255 Default : 30)
Trace Route Results	<div style="border: 1px solid gray; height: 150px;"></div>

Figure 4-13-6: Trace Route Setting Page Screenshot

The page includes the following fields:

Object	Description
• IP Address	The destination IP Address
• Max Hop	The maximum gateway number allowed by traceroute function
• Trace Route Results	Display the current trace route result

Button



: Click to strat trace route process.

4.14 Power over Ethernet (GS-4210-24P2S only)

Providing up to 24 PoE, in-line power interfaces, the GS-4210-24P2S PoE Managed Switch can easily build a power central-controlled IP phone system, IP Camera system, AP group for the enterprise. For instance, 24 camera / AP can be easily installed around the corner in the company for surveillance demands or build a wireless roaming environment in the office.

Without the power-socket limitation, the GS-4210-24P2S PoE Managed Switch makes the installation of cameras or WLAN AP more easily and efficiently.

Use the PoE sub-menu items to configure the PoE function of the GS-4210-24P2S PoE Managed Switch. Under PoE sub-menu, the following topics are provided to configure and view the PoE Setting:

This section has the following items:

- PoE Global Setting
- PoE Port Setting
- PoE Delay Setting

4.14.1 PoE Global Setting

This page allows adjusting the PoE budget and viewing PoE operation status and PoE chipset temperature. The PoE Global Setting screen in [Figure 4-14-1](#) appears.

PoE Global Setting

PoE Global Setting

Maximum PoE Budget (watts)	<input type="text" value="300"/>	(0-300watts)
System Operation Status	Off	
Power Allocation	0 (watts)	
PoE Temperature		
Port 1-8	55(C)	
Port 9-16	55(C)	
Port 17-24	57(C)	

Figure 4-14-1: PoE Global Setting Page Screenshot

Button

: Click to apply changes.

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Maximum PoE Budget (watts) 	Allow assign PoE Budget to the PoE Managed Switch. The range is 0-300 watts and default is 300 watts.
<ul style="list-style-type: none"> • System Operation Status 	Display current system operation status.
<ul style="list-style-type: none"> • Power Allocation 	Display current power allocation value in watts.
<ul style="list-style-type: none"> • PoE Temperature Port 1 -8 	Display the current PoE chipset temperature of port 1-8.
<ul style="list-style-type: none"> • PoE Temperature Port 9 -16 	Display the current PoE chipset temperature of port 9-16.
<ul style="list-style-type: none"> • PoE Temperature Port 17 -24 	Display the current PoE chipset temperature of port 17-24.

4.14.2 PoE Port Setting

This page allows adjusting per port PoE budget and viewing per PoE port status. The PoE Port Setting screen in [Figure 4-14-2](#) appears.

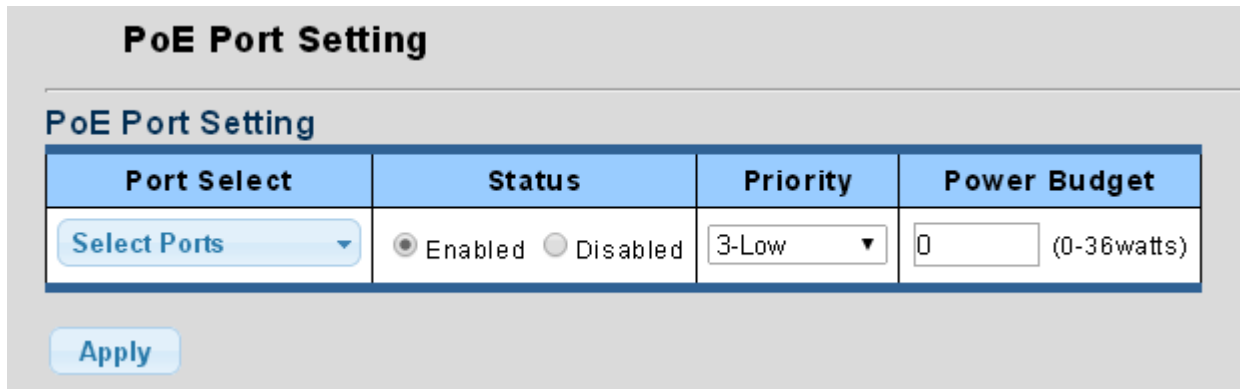


Figure 4-14-2: PoE Port Setting Page Screenshot

Button

Apply: Click to apply changes.

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port Select 	Select port from this drop down list.
<ul style="list-style-type: none"> • Status 	Disable or enable per port PoE function.
<ul style="list-style-type: none"> • Priority 	Select priority options from this drop down list. The available options are: 3-Low (Default) 2-High 1-Critical
<ul style="list-style-type: none"> • Power Budget 	Allow assign PoE Budget to per port of the PoE Managed Switch. The range is 0-36 watts.

▼ PoE Port Status

Port	Status	Class	Priority	Power Consumption(watts)	Power Budget(watts)
GE1	Disable	---	3	0.00	0
GE2	Disable	---	3	0.00	0
GE3	Disable	---	3	0.00	0
GE4	Disable	---	3	0.00	0
GE5	Disable	---	3	0.00	0
GE6	Disable	---	3	0.00	0
GE7	Disable	---	3	0.00	0
GE8	Disable	---	3	0.00	0
GE9	Disable	---	3	0.00	0
GE10	Disable	---	3	0.00	0
GE11	Disable	---	3	0.00	0
GE12	Disable	---	3	0.00	0
GE13	Disable	---	3	0.00	0
GE14	Disable	---	3	0.00	0
GE15	Disable	---	3	0.00	0
GE16	Disable	---	3	0.00	0
GE17	Disable	---	3	0.00	0
GE18	Disable	---	3	0.00	0
GE19	Disable	---	3	0.00	0
GE20	Disable	---	3	0.00	0
GE21	Disable	---	3	0.00	0
GE22	Disable	---	3	0.00	0
GE23	Disable	---	3	0.00	0
GE24	Disable	---	3	0.00	0

Figure 4-14-3: PoE Port Status Page Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port.
• Status	Display per PoE port operation status.
• Class	Display per PoE port PD device class information.
• Priority	Display per PoE port priority information.
• Power Consumption (watts)	Display per PoE port power consumption information.
• Power Budget (watts)	Display per PoE port power budget information.

4.14.3 PoE Delay Setting

PoE delay is to delay power feeding when the switch is completely booted up

This page allows adjusting per port PoE delay time and viewing per PoE port status. The PoE Delay Setting screen in [Figure 4-14-4](#) appears.

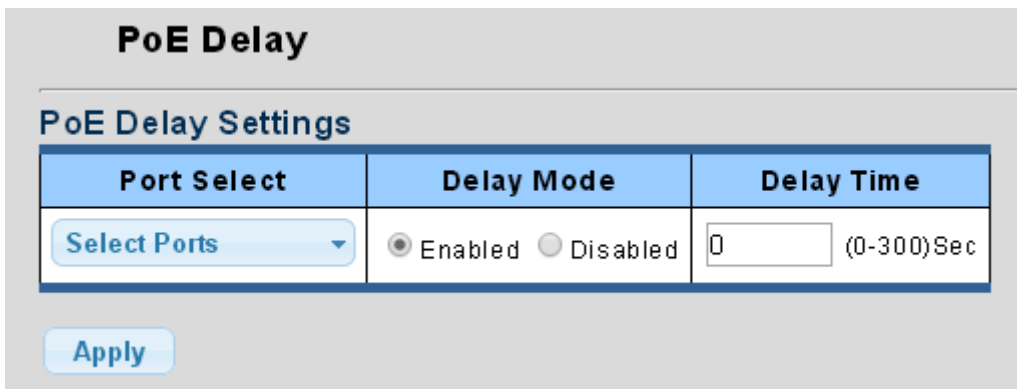


Figure 4-14-4: PoE Delay Setting Page Screenshot

Button

: Click to apply changes.

The page includes the following fields:

Object	Description
• Port Select	Select port from this drop down list.
• Delay Mode	Disable or enable delay mode.
• Delay Time	Allow assign delay time to the PoE Managed Switch. The range is 0-300 seconds.

▼ POE Delay Status

Port	Delay Mode	Delay Time(Second)
GE1	Disable	0
GE2	Disable	0
GE3	Disable	0
GE4	Disable	0
GE5	Disable	0
GE6	Disable	0
GE7	Disable	0
GE8	Disable	0
GE9	Disable	0
GE10	Disable	0
GE11	Disable	0
GE12	Disable	0
GE13	Disable	0
GE14	Disable	0
GE15	Disable	0
GE16	Disable	0
GE17	Disable	0
GE18	Disable	0
GE19	Disable	0
GE20	Disable	0
GE21	Disable	0
GE22	Disable	0
GE23	Disable	0
GE24	Disable	0

Figure 4-14-5: PoE Delay Status Page Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	The switch port number of the logical port.
<ul style="list-style-type: none"> • Delay Mode 	Display per port delay mode status.
<ul style="list-style-type: none"> • Delay Time (Second) 	Display per port delay time setting information.

4.14.4 Power over Ethernet Powered Device

 <p>3~5 Watts</p>	<p>Voice over IP phones</p> <p>Enterprise can install POE VoIP Phone, ATA and other Ethernet/non-Ethernet end-devices to the central where UPS is installed for un-interrupt power system and power control system.</p>
 <p>6~12 Watts</p>	<p>Wireless LAN Access Points</p> <p>Museum, Sightseeing, Airport, Hotel, Campus, Factory, Warehouse can install the Access Point any where with no hesitation.</p>
 <p>10~12 Watts</p>	<p>IP Surveillance</p> <p>Enterprise, Museum, Campus, Hospital, Bank, can install IP Camera without limits of install location – no need electrician to install AC sockets.</p>
 <p>3~12 Watts</p>	<p>PoE Splitter</p> <p>PoE Splitter split the PoE 52V DC over the Ethernet cable into 5/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.</p>
 <p>3~25 Watts</p>	<p>High Power PoE Splitter</p> <p>High PoE Splitter split the PoE 52V DC over the Ethernet cable into 24/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.</p>
 <p>30 Watts</p>	<p>High Power Speed Dome</p> <p>This state-of-the-art design is considerable to fit in various network environments like traffic centers, shopping malls, railway stations, warehouses, airports, and production facilities for the most demanding outdoor surveillance applications- no need electrician to install AC sockets.</p>



Since the GS-4210-24P2S PoE Managed Switch per PoE port supports 52V DC PoE power output, please check and assure the Powered Device's (PD) acceptable DC power range is from 52V DC; otherwise, it will damage the Powered Device (PD).

4.15 RMON

RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

MID of RMON consists of 10 groups. The switch supports the most frequently used group 1, 2, 3 and 9:

- **Statistics:** Maintain basic usage and error statistics for each subnet monitored by the Agent.
- **History:** Record periodical statistic samples available from Statistics.
- **Alarm:** Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON Agent records.
- **Event:** A list of all events generated by RMON Agent.

Alarm depends on the implementation of Event. Statistics and History display some current or history subnet statistics. Alarm and Event provide a method to monitor any integer data change in the network, and provide some alerts upon abnormal events (sending Trap or record in logs).

4.15.1 RMON Statistics

This Page provides a Detail of a specific RMON statistics entry; RMON Statistics screen in [Figure 4-15-1](#) appears.

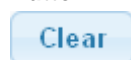
RMON Statistics	
Port GE1 RMON Statistics	
Port: GE1	<input type="button" value="Clear"/>
RMON MIB Name	Value
etherStatsDropEvents	0
etherStatsOctets	0
etherStatsPkts	0
etherStatsBroadcastPkts	0
etherStatsMulticastPkts	0
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	0
etherStatsPkts65to127Octets	0
etherStatsPkts128to255Octets	0
etherStatsPkts256to511Octets	0
etherStatsPkts512to1023Octets	0
etherStatsPkts1024to1518Octets	0

Figure 4-15-1: RMON Statistics Page Screenshot

The Page includes the following fields:

Object	Description
• Port	Select port for this drop down list.
• etherStatsDropEvents	The total number of events in which packets were dropped by the probe due to lack of resources.
• etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network.
• etherStatsPkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
• etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address.
• etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address.
• etherStatsCRCAAlignErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.
• etherStatsUnderSizePkts	The total number of packets received that were less than 64 octets.
• etherStatsOverSizePkts	The total number of packets received that were longer than 1518 octets.
• etherStatsFragments	The number of frames which size is less than 64 octets received with invalid CRC.
• etherStatsJabbers	The number of frames which size is larger than 64 octets received with invalid CRC.
• etherStatsCollisions	The best estimate of the total number of collisions on this Ethernet segment.
• etherStatsPkts64Octets	The total number of packets (including bad packets) received that were 64 octets in length.
• etherStatsPkts65to127Octets	The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
• etherStatsPkts128to255Octets	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
• etherStatsPkts256to511Octets	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
• etherStatsPkts512to1023Octets	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
• etherStatsPkts1024to1518Octets	The total number of packets (including bad packets) received that were between 1024 to 1518 octets in length.

Button



: Click to clear the RMON statistics.

4.15.2 RMON Event

Configure RMON Event table on this Page. The RMON Event screens in [Figure 4-15-2](#) and [Figure 4-15-3](#) appear.

RMON Event

RMON Event Settings

Select Index	<input type="text" value="Create New"/>
Index	<input type="text" value="0"/> (1-65535)
Type	<input type="text" value="None"/>
Community	<input type="text" value="public"/>
Owner	<input type="text"/> (0~31 Characters)
Description	<input style="width: 90%;" type="text"/> (0~127 Characters)

Figure 4-15-2: RMON Event Settings Page Screenshot

The Page includes the following fields:

Object	Description
• Select Index	Select index for this drop down list to create new index or modify index.
• Index	Indicates the index of the entry. The range is from 1 to 65535.
• Type	Indicates the notification of the event, the possible types are: <ul style="list-style-type: none"> ■ None: The total number of octets received on the interface, including framing characters. ■ Log: The number of uni-cast packets delivered to a higher-layer protocol. ■ SNMP-Trap: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. ■ Log and Trap: The number of inbound packets that are discarded even the packets are normal.
• Community	Specify the community when trap is sent, default is " public ".
• Owner	Indicates the owner of this event, the string length is from 0 to 31, default is a null string.
• Description	Indicates description of this event, the string length is from 0 to 127, default is a null string.

Button




: Click to apply changes.

Index	Event Type	Community	Description	Last Sent Time	Owner	Action
-------	------------	-----------	-------------	----------------	-------	--------

Figure 4-15-3: RMON Event Status Page Screenshot

The Page includes the following fields:

Object	Description
• Index	Display the current event index.
• Event Type	Display the current event type.
• Community	Display the current community for SNMP trap.
• Description	Display the current event description.
• Last Sent Time	Display the current last sent time.
• Owner	Display the current event owner.
• Action	Click  to delete RMON event entry.

4.15.3 RMON Event Log

This Page provides an overview of RMON Event Log. The RMON Event Log Table screen in Figure 4-15-4 appears.

RMON Event Log

▼ RMON Event Log Table

Event Index

Index	Alarm Index	Action	Log Time	Description
-------	-------------	--------	----------	-------------

Figure 4-15-4: RMON Event Log Table Page Screenshot

The Page includes the following fields:

Object	Description
• Event Index	Select index from this drop down list.
• Index	Indicates the index of the log entry.
• Alarm Index	Indicates the alarm index of the log entry.
• Action	Indicates the action of the log entry.
• Log Time	Indicates Event log time.
• Description	Indicates the Event description.

4.15.4 RMON Alarm

Configure RMON Alarm setting on this Page. The RMON Alarm screens in [Figure 4-15-5](#) and [Figure 4-15-6](#) appear.

RMON Alarm

RMON Alarm Settings

Select Index	<input type="text" value="Create New"/> ▼
Index	<input type="text" value="0"/> (1-65535)
Sample Port	<input type="text" value="GE1"/> ▼
Sample Variable	<input type="text" value="DropEvents"/> ▼
Sample Interval	<input type="text" value="0"/> (1-21 47 483647;
Sample Type	<input type="radio"/> Absolute <input type="radio"/> Delta
Rising Threshold	<input type="text" value="0"/> (0-21 47 483647;
Falling Threshold	<input type="text" value="0"/> (0-21 47 483647;
Rising Event	<input type="text" value="0: None (Unassigned)"/> ▼
Falling Event	<input type="text" value="0: None (Unassigned)"/> ▼
Owner	<input type="text"/> (0~31 Characters)

Figure 4-15-5: RMON Alarm Setting Page Screenshot

The Page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Select Index 	Select index for this drop down list to create the new index or modify the index.
<ul style="list-style-type: none"> • Index 	Indicates the index of the alarm entry. The range is 1-65535.
<ul style="list-style-type: none"> • Sample Port 	Select port from this drop down list.
<ul style="list-style-type: none"> • Sample Variable 	<p>Indicates the particular variable to be sampled, the possible variables are:</p> <ul style="list-style-type: none"> ■ DropEvents: The total number of events in which packets were dropped due to lack of resources. ■ Octets: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits. ■ Pkts: The total number of frames (bad, broadcast and multicast) received and transmitted. ■ BroadcastPkts: The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets. ■ MulticastPkts: The total number of good frames received that were directed to this multicast address. ■ CRCAlignErrors: The number of CRC/alignment errors (FCS or alignment errors). ■ UnderSizePkts: The total number of frames received that were less than 64 octets long(excluding framing bits, but including FCS octets) and were otherwise well formed. ■ OverSizePkts: The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets) and were otherwise well formed. ■ Fragments: The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error. ■ Jabbers: The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets), and had either an FCS or alignment error. ■ Collisions: The best estimate of the total number of collisions on this Ethernet segment. ■ Pkts64Octets: The total number of frames (including bad packets) received andtransmitted that were 64 octets in length (excluding framing bits but including FCS octets). ■ Pkts65to127Octets: The total number of frames (including bad packets) received andtransmitted where the number of octets fall within the specified

	<p>range (excluding framing bits but including FCS octets).</p> <ul style="list-style-type: none"> ■ Pkts128to255Octets: The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets). ■ Pkts256to511Octets: The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets). ■ Pkts512to1023Octets: The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets). ■ Pkts1024to1518Octets: The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).
• Sample Interval	Sample interval (1–2147483647)
• Sample Type	<p>The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:</p> <ul style="list-style-type: none"> ■ Absolute: Get the sample directly (default). ■ Delta: Calculate the difference between samples.
• Rising Threshold	Rising threshold value (0–2147483647).
• Falling Threshold	Falling threshold value (0–2147483647).
• Rising Event	Event to fire when the rising threshold is crossed.
• Falling Event	Event to fire when the falling threshold is crossed.
• Owner	Specify an owner for the alarm.


Button

: Click to apply changes.

RMON Alarm										
Index	Sample Port	Sample Variable	Sample Interval	Sample Type	Rising Threshold	Falling Threshold	Rising Event	Falling Event	Owner	Action

Figure 4-15-6: RMON Alarm Status Page Screenshot

The Page includes the following fields:

Object	Description
• Index	Indicates the index of Alarm control entry.
• Sample Port	Display the current sample port.
• Sample Variable	Display the current sample variable.
• Sample Interval	Display the current interval.
• Sample Type	Display the current sample type.
• Rising Threshold	Display the current rising threshold.
• Falling Threshold	Display the current falling threshold.
• Rising Event	Display the current rising event.
• Falling Event	Display the current falling event.
• Owner	Display the current owner.
• Action	Click  to delete RMON alarm entry.

4.15.5 RMON History

Configure RMON History table on this Page. The RMON History screens in [Figure 4-15-7](#) and [Figure 4-15-8](#) appear.

RMON History

RMON History Settings


Select Index	<input type="text" value="Create New"/> ▼
Index	<input type="text" value="0"/> (1-65535)
Sample Port	<input type="text" value="GE1"/> ▼
Bucket Requested	<input type="text" value="50"/> (1-65535, Default 50)
Interval	<input type="text" value="1800"/> (1-3600 Default 1800)
Owner	<input type="text"/> (0~31 Charactors)

Figure 4-15-7: RMON History Table Page Screenshot

The Page includes the following fields:

Object	Description
• Select Index	Select index for this drop down list to create the new index or modify the index
• Index	Indicates the index of the history entry. The range is 1-65535.
• Sample Port	Select port from this drop down list
• Bucket Requested	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 65535, default value is 50.
• Interval	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
• Owner	Specify an owner for the history. The range is 1-31 characters.

Button

: Click to apply changes.

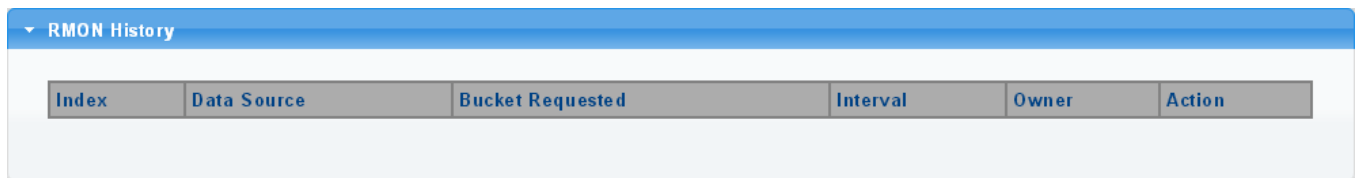



Figure 4-15-8: RMON History Status Page Screenshot

The Page includes the following fields:

Object	Description
• Index	Display the current index.
• Data Source	Display the current data source.
• Bucket Requested	Display the current bucket requested.
• Interval	Display the current interval.
• Owner	Display the current owner.
• Action	Click  to delete RMON history entry.

4.15.6 RMON History Log

This Page provides a detail of RMON history entries; screen in [Figure 4-15-9](#) appears.

Figure 4-15-9: RMON History Status Page Screenshot

The Page includes the following fields:

Object	Description
• History Index	Select history index from this drop down list

4.16 Maintenance

Use the Maintenance menu items to display and configure basic configurations of the Managed Switch. Under maintenance the following topics are provided to back up, upgrade, save and restore the configuration. This section has the following items:

- **Factory Default** You can reset the configuration of the switch on this page.
- **Reboot Switch** You can restart the switch on this page. After restart, the switch will boot normally.
- **Backup Manager** You can back up the switch configuration.
- **Upgrade Manager** You can upgrade the switch configuration.
- **Configuration Manager** You can save the switch configuration.
- **Enable Password** You can set the enable password.

4.16.1 Factory Default

You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary. The Factory Default screen in [Figure 4-16-1](#) appears and clicks to reset the configuration to Factory Defaults.

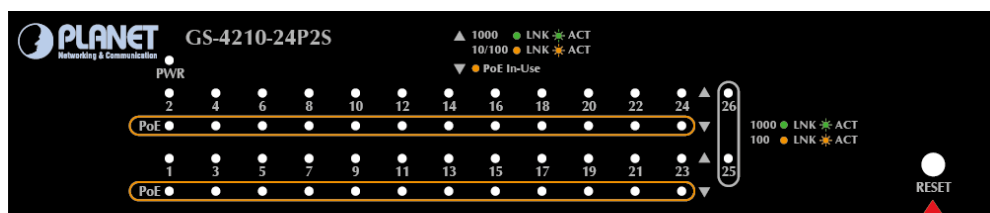


Figure 4-16-1: Factory Default Page Screenshot

After the “**Factory**” button is pressed and rebooted, the system will load the default IP settings as follows:

- Default IP address: **192.168.0.100**
- Subnet mask: **255.255.255.0**
- Default Gateway: **192.168.0.254**
- The other setting value is back to disable or none.

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



Hardware Reset button

4.16.2 Reboot Switch

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user has to re-login the WEB interface about 60 seconds later. The Reboot Switch screen in [Figure 4-16-2](#) appears and clicks to reboot the system.

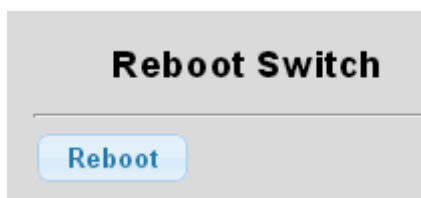


Figure 4-16-2: Reboot Switch Page Screenshot

4.16.3 Backup Manager

This function allows backup of the current image or configuration of the Managed Switch to the local management station. The Backup Manager screen in [Figure 4-16-3](#) appears.

Figure 4-16-3: Backup Manager Page Screenshot

The page includes the following fields:

Object	Description
• Backup Method	Select backup method from this drop down list. The options are TFTP and HTTP.
• Server IP	Fill in your TFTP server IP address.
• Backup Type	Select backup type.

Button

Backup: Click to backup image, configuration or log.

4.16.4 Upgrade Manager

This function allows reload the current image or configuration of the Managed Switch to the local management station. The Upgrade Manager screen in [Figure 4-16-4](#) appears.

Upgrade Manager	
Upgrade Method	TFTP ▼
Server IP	<input type="text"/> (IPv4 or IPv6 Address)
File Name	<input type="text"/>
Upgrade Type	<input checked="" type="radio"/> Image <input type="radio"/> Startup Configuration <input type="radio"/> Backup Configuration

Upgrade

Figure 4-16-4: Upgrade Manager Page Screenshot

The page includes the following fields:

Object	Description
• Upgrade Method	Select upgrade method from this drop down list. The options are TFTP and HTTP.
• Server IP	Fill in your TFTP server IP address.
• File Name	The name of firmware image or configuration.
• Upgrade Type	Select upgrade type.

Button

Upgrade: Click to upgrade image or configuration.

4.16.5 Configuration Manager

In the Managed Switch, the running configuration file stores in the RAM. In the current version, the running configuration sequence of running-config can be saved from the RAM to FLASH by click "SAVE" then "Save Configurations to FLASH" function, so that the running configuration sequence becomes the startup configuration file, which is called configuration save. This page also provides to save all applied changes and set the current configuration as a startup configuration or backup configuration. The startup-configuration file will be loaded automatically across a system reboot, the configuration manager screen in [Figure 4-16-5](#) appears.

Configuration Manager

Save Configuration

Source File	<input checked="" type="radio"/> Running configuration
Destination File	<input checked="" type="radio"/> Startup configuration <input type="radio"/> Backup configuration

Apply

Figure 4-16-5: Configuration Manager Page Screenshot

The Page includes the following fields:

Object	Description
• Source File	Provide Running configuration option.
• Destination File	Provide "Startup configuration" and "Backup configuration" options.

Button



: Click to apply changes.

4.16.6 Enable Password

The page allows configuring system password, the enable password screen in [Figure 4-16-6](#) appears.

Figure 4-16-6: Enable Password Page Screenshot

The Page includes the following fields:

Object	Description
• Privilege Value	Provide 0-15 option.
• Password Type	Provide “Clear Text” and “Encrypted” options.
• Password	Allow input the new password and available range is 30 characters.
• Retype Password	Allow input the new password again for confirm.

Button



: Click to apply changes.

Figure 4-16-7: Local Enable Password Page Screenshot

The Page includes the following fields:

Object	Description
• Privilege Value	Display current privilege value information.
• Password Type	Display current password type information.
• Modify	Click  to delete password entry.

5. COMMAND LINE INTERFACE

5.1 Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

This chapter describes how to use the Command Line Interface (CLI).



The following screen based on GS-4210-24P2S will be the same as that of GS-4210-16T2S and GS-4210-24T2S.

Logon to the Console

Once the terminal is connected to the device, power on the Managed Switch and the terminal will **run self testing procedures**.

Then, the following message asks to login user name and password. The factory default user name and password are shown as follows and the login screen in [Figure 5-1](#) appears.

```
Username: admin
Password: admin
```

1. On "Username" & "Password" prompt, enter "admin".
2. The user can now enter commands to manage the Managed Switch. For a detailed description of the commands, please refer to the following chapters.

```
Switch Command Line Interface

Press any key to continue

Username: admin
Password: *****
GS-4210-24P2S # _
```

Figure 5-1: Managed Switch Console Login Screen



1. For security reason, please change and memorize the new password after this first setup.
2. Only accept command in lowercase letter under console interface.

Configure IP address

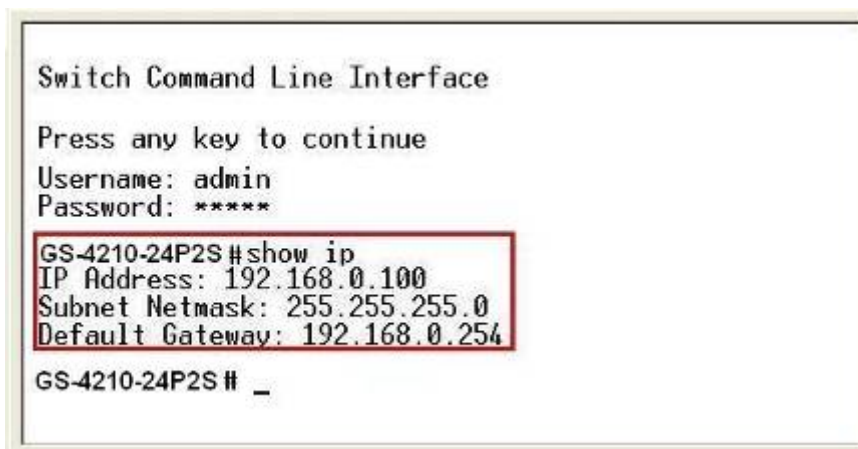
The Managed Switch is shipped with default IP address as follows:

```
IP Address: 192.168.0.100
Subnet Mask: 255.255.255.0
```

To check the current IP address or modify a new IP address for the Managed Switch, please use the procedures as follows:

■ Display of the current IP address

1. On "GS-4210-24P2S#" prompt, enter "show ip".
2. The screen displays the current IP address, Subnet Mask and Gateway shown in [Figure 5-2](#).



```
Switch Command Line Interface
Press any key to continue
Username: admin
Password: *****
GS-4210-24P2S#show ip
IP Address: 192.168.0.100
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.0.254
GS-4210-24P2S # _
```

Figure 5-2: IP Information Screen

■ Configuration of the IP address

3. On "GS-4210-24P2S#" prompt, enter "configure".
4. On "GS-4210-24P2S (config)#" prompt, enter the following command and press <Enter> as shown in [Figure 5-3](#).

```
GS-4210-24P2S (config)# ip address 192.168.1.100 mask 255.255.255.0
GS-4210-24P2S (config)# ip default-gateway 192.168.1.254
```

The previous command would apply the following settings for the Managed Switch.

```
IP Address: 192.168.1.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.254
```

```
GS-4210-24P2S# show ip
IP Address: 192.168.0.100
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.0.254
GS-4210-24P2S# configure
GS-4210-24P2S(config)# ip address 192.168.1.100 mask 255.255.255.0
GS-4210-24P2S(config)# ip default-gateway 192.168.1.254
GS-4210-24P2S(config)#
```

Figure 5-3: Setting IP Address Screen

5. Repeat Step 1 to check if the IP address is changed.

If the IP is successfully configured, the Managed Switch will apply the new IP address setting immediately. You can access the Web interface of Managed Switch through the new IP address.



If you do not familiar with console command or the related parameter, enter “?” anytime in console to get the help description.

5.2 Telnet Login

The Managed Switch also supports telnet for remote management. The Managed Switch asks for user name and password for remote login when using telnet, please use “**admin**” for username & password.

```
c:\ Telnet 192.168.0.100

Switch Command Line Interface (Version v1.0b140611)

Username: admin
Password: *****
GS-4210-24P2S#
```

Figure 5-4: Telnet Login Screen

6. Command Line Mode

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes supports specific software commands.



The following screen based on GS-4210-24P2S will be the same as that of GS-4210-16T2S and GS-4210-24T2S.

Mode-based Command Hierarchy

The **Command Line Interface (CLI)** groups all the commands in appropriate modes by the nature of the commands. Examples of the CLI command modes are described below. Each of the command modes supports specific switch's commands.

The CLI Command Modes table captures the command modes, the prompts visible in that mode and the exit method from that mode.

Command Mode	Access Method	Prompt	Exit or Access Previous Mode
User Mode	This is the first level of access. Perform basic tasks and list system information.	GS-4210-24P2S>	Enter exit command
Privileged Mode	From the User Mode, enter the enable command.	GS-4210-24P2S #	To exit to the User Mode, enter exit .
Global Config Mode	From the Privileged Mode, enter the configuration command.	GS-4210-24P2S (Config)#	To exit to the Privileged Mode, enter the exit command.

Table 6-1: CLI Command Modes

The CLI is divided into various modes. The commands in one mode are not available until the operator switches to that particular mode. The commands available to the operator at any point in time depend upon the mode. Entering a question mark (?) at the CLI prompt, and displays a list of the available commands and descriptions of the commands.

The CLI provides the following modes:

User Mode

When the operator logs into the CLI, the User Mode is the initial mode. The User Mode contains a limited set of commands. The command prompt shown at this level is:

Command Prompt: GS-4210-24P2S >

Privileged Mode

To have access to the full suite of commands, the operator must enter the Privileged Mode. The Privileged Mode requires password authentication. From Privileged Mode, the operator can issue any Exec command to enter the Global Configuration mode. The command prompt shown at this level is:

Command Prompt: GS-4210-24P2S #

Global Config Mode

This mode permits the operator to make modifications to the running configuration. General setup commands are grouped in this mode. From the Global Configuration mode, the operator can enter the Interface Configuration mode. The command prompt at this level is:

Command Prompt: GS-4210-24P2S (Config)#

From the Global Config mode, the operator may enter the following configuration modes:

6.1 User Mode Commands

6.1.1 enable command

Description:

Turn on privileged mode command

Syntax:

enable

Example:

```
GS-4210-24P2S> enable
Password:
GS-4210-24P2S#
```

6.1.2 exit command

Description:

Exit current mode and down to previous mode

Syntax:

exit

Example:

```
GS-4210-24P2S# exit
GS-4210-24P2S>
```

6.1.3 ping command

Description:

Send ICMP ECHO_REQUEST to network hosts

Syntax:

ping HOSTNAME (Host name)

Example:

```
GS-4210-24P2S> ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100): 56 data bytes
64 bytes from 192.168.0.100: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.0 ms
--- 192.168.0.100 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
GS-4210-24P2S>
```

6.1.4 Show Command

show arp

Description:

Show the IP ARP translation table

Syntax:

show arp

Example:

```
GS-4210-24P2S> show arp
Address                HWtype  HWaddress          Flags Mask          Iface
192.168.0.100          ether   C8:9C:DC:EC:D6:DD  C                   eth0
GS-4210-24P2S>
```

show history

Description:

List the last several history commands

Syntax:

show history

Example:

```
GS-4210-24P2S> show history
```

show info

Description:

Show basic information

Syntax:

show info

Example:

```
GS-4210-24P2S> show info
```

show ip

Description:

Show the IP Address, Subnet Mask, Default Gateway

Syntax:

show ip

Example:

```
GS-4210-24P2S> show ip
IP Address: 192.168.0.100
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.0.254
GS-4210-24P2S>
```

show privilege

Description:

Show the local user privilege level

Syntax:

show privilege

Example:

```
GS-4210-24P2S> show privilege
Current CLI Username: admin
Current CLI Privilege: 15
GS-4210-24P2S>
```

show version

Description:

Show the system hardware and software status

Syntax:

show version

Example:

```
GS-4210-24P2S> show version
Loader Version   : 2011.12.41872
Loader Date      : May 22 2014 - 19:28:43
Firmware Version : v1.0b140611
Firmware Date    : Wed Jun 11 10:13:28 CST 2014
Magic Number     : 83800000
GS-4210-24P2S>
```

6.1.5 traceroute command

Description:

Trace route to network hosts

Syntax:

traceroute HOSTNAME (The IP address or hostname address to trace)

Example:

```
GS-4210-24P2S> traceroute 192.168.0.100
```

6.2 Privileged Mode Commands

6.2.1 clear command

clear arp

Description:

Clear entries in the ARP cache

Syntax:

clear arp A.B.C.D (IP address to clear)

clear arp (the entire ARP cache is cleared)

Example:

```
GS-4210-24P2S# clear arp 192.168.0.100
GS-4210-24P2S#
GS-4210-24P2S# clear arp
GS-4210-24P2S#
```

clear gvrp

Description:

Clear the GVRP configuration

Syntax:

clear GVRP error-statistics (GVRP Error Statistics information)

clear GVRP statistics (GVRP Statistics information)

Example:

```
GS-4210-24P2S# clear gvrp error-statistics
GS-4210-24P2S# clear gvrp statistics
GS-4210-24P2S#
```

clear interfaces

Description:

Clear the Interface status and configuration

Syntax:

clear interface LAG <1-8> counters

clear interfaces GigabitEthernet <1-26> counters

Example:

```
GS-4210-24P2S# clear interfaces lag 1 counters
GS-4210-24P2S# clear interfaces GigabitEthernet 1 counters
GS-4210-24P2S#
```

clear ip arp

Description:

Clear the IP configuration

Syntax:

clear ip arp inspection interfaces LAG <1-8> statistics

clear ip arp inspection interfaces GigabitEthernet <1-26> statistics

Example:

```
GS-4210-24P2S# clear ip arp inspection interfaces lag 1 statistics
GS-4210-24P2S# clear ip arp inspection interfaces GigabitEthernet 1 statistics
GS-4210-24P2S#
```

clear ip dhcp

Description:

Clear the DHCP configuration

Syntax:

clear ip dhcp snooping database statistics

clear ip dhcp snooping interfaces LAG <1-8> statistics

clear ip dhcp snooping interfaces GigabitEthernet <1-26> statistics

Example:

```
GS-4210-24P2S# clear ip dhcp snooping database statistics
GS-4210-24P2S# clear ip dhcp snooping interfaces lag 1 statistics
GS-4210-24P2S# clear ip dhcp snooping interface GigabitEthernet 1 statistics
GS-4210-24P2S#
```

clear ip igmp

Description:

Clear the IGMP configuration

Syntax:

clear ip igmp snooping groups dynamic / static

clear ip igmp snooping statistics

clear ip dhcp snooping vlan x static-mac xx:xx:xx:xx:xx:xx

Example:

```
GS-4210-24P2S# clear ip igmp snooping groups dynamic
GS-4210-24P2S# clear ip igmp snooping groups static
GS-4210-24P2S# clear ip igmp snooping statistics
GS-4210-24P2S# clear ip igmp snooping vlan 1 static-mac 00:30:4F:00:00:01
GS-4210-24P2S#
```

clear ipv6

Description:

Clear the ipv6 information

Syntax:

clear ipv6 mld snooping groups dynamic / static

clear ipv6 mld snooping statistics

clear ipv6 mld snooping vlan x static-mac xx:xx:xx:xx:xx:xx

Example:

```
GS-4210-24P2S# clear ipv6 mld snooping groups dynamic
GS-4210-24P2S# clear ipv6 mld snooping groups static
GS-4210-24P2S# clear ipv6 mld snooping statistics
GS-4210-24P2S# clear ipv6 mld snooping vlan 1 static-mac 00:30:4F:00:00:01
GS-4210-24P2S#
```

clear line

Description:

Clear identify a specific line for configuration

Syntax:

clear line ssh / telnet

Example:

```
GS-4210-24P2S# clear line ssh
GS-4210-24P2S# clear line telnet
GS-4210-24P2S#
```

clear lldp

Description:

Clear lldp configuration

Syntax:

clear line lldp statistics

Example:

```
GS-4210-24P2S# clear lldp statistics
GS-4210-24P2S#
```

clear logging

Description:

Clear log configuration

Syntax:

clear logging buffered / flash

Example:

```
GS-4210-24P2S# clear logging buffered
GS-4210-24P2S# clear logging flash
GS-4210-24P2S#
```

clear mac**Description:**

Clear MAC configuration

Syntax:

clear mac address-table dynamic interface lag x

clear mac address-table dynamic interface GigabitEthernet x

clear mac address-table dynamic vlan x

Example:

```
GS-4210-24P2S# clear mac address-table dynamic interfaces lag 1
GS-4210-24P2S# clear mac address-table dynamic interfaces GigabitEthernet 1
GS-4210-24P2S# clear mac address-table dynamic vlan 1
GS-4210-24P2S#
```

clear rmon**Description:**

Clear RMON information

Syntax:

clear rmon interfaces lag x statistics

clear rmon interfaces GigabitEthernet x statistics

Example:

```
GS-4210-24P2S# clear rmon interfaces lag 1 statistics
GS-4210-24P2S# clear rmon interfaces GigabitEthernet 1 statistics
GS-4210-24P2S#
```

6.2.2 clock command**Description:**

Manage the system clock

Syntax:

clock set HH:MM:SS:Month: Date: Year

Example:

```
GS-4210-24P2S# clock set 13:36:00 jul 3 2014
13:36:00 DFL(UTC+8) Jul 03 2014
GS-4210-24P2S#
```

6.2.3 configure command

Description:

Enter Global Config mode

Syntax:

configure

Example:

```
GS-4210-24P2S# configure
GS-4210-24P2S(config)#
```

6.2.4 copy command

Description:

Copy from one file to another

Syntax:

copy backup-config / flash:// / running-config / startup-config / tftp:// running-config / startup-config / tftp://

Example:

```
GS-4210-24P2S# copy running-config startup-config
Success
GS-4210-24P2S#
```

6.2.5 debug command

Description:

Debug Options

Syntax:

debug acl all / common / reserve / user-defined

Example:

```
GS-4210-24P2S# debug acl all
GS-4210-24P2S# debug acl common
GS-4210-24P2S# debug acl reserve
GS-4210-24P2S# debug acl user-defined
GS-4210-24P2S#
```

6.2.6 delete command

Description:

Delete a file from the flash file system

Syntax:

delete backup-config / flash:// / startup-config / system image x

Example:

```
GS-4210-24P2S# delete backup-config
GS-4210-24P2S# delete flash://
GS-4210-24P2S# delete startup-config
GS-4210-24P2S# delete system image 0
GS-4210-24P2S#
```

6.2.7 disable command

Description:

Turn off privileged mode command

Syntax:

disable

Example:

```
GS-4210-24P2S# disable
GS-4210-24P2S>
```

6.2.8 end command

Description:

End current mode and change to enable mode

Syntax:

end

Example:

```
GS-4210-24P2S(config)# end
GS-4210-24P2S#
```

6.2.9 exit command

Description:

Exit current mode and down to previous mode

Syntax:

exit

Example:

```
GS-4210-24P2S# exit
GS-4210-24P2S>
```

6.2.10 no command

Description:

Negate command

Syntax:

no debug acl all / common / reserve / user-defined

Example:

```
GS-4210-24P2S# no debug acl all
GS-4210-24P2S# no debug acl common
GS-4210-24P2S# no debug acl reserve
GS-4210-24P2S# no debug acl user-defined
GS-4210-24P2S#
```

6.2.11 ping command

Description:

Send ICMP ECHO_REQUEST to network hosts

Syntax:

ping HOSTNAME (Host name)

Example:

```
GS-4210-24P2S> ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100): 56 data bytes
64 bytes from 192.168.0.100: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.0 ms
--- 192.168.0.100 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
GS-4210-24P2S>
```

6.2.12 reboot command

Description:

Halt and perform a cold restart

Syntax:

reboot

Example:

```
GS-4210-24P2S# reboot
*Jul 03 14:22:09: %System-4: System reboot
```

6.2.13 renew command

Description:

Renew IP configuration

Syntax:

renew ip dhcp snooping database

Example:

```
GS-4210-24P2S# renew ip dhcp snooping database
GS-4210-24P2S#
```

6.2.14 restore-defaults command

Description:

Restore to default

Syntax:

restore-defaults

Example:

```
GS-4210-24P2S# restore-defaults
Restore Default Success. Do you want to reboot now? (y/n)y
Rebooting now...
*Jan 01 08:16:00: %System-4: System reboot
```

6.2.15 save command

Description:

Save running configuration to flash

Syntax:

save

Example:

```
GS-4210-24P2S# save
Success
GS-4210-24P2S#
```

6.2.16 show command

Description:

Show running system information

Syntax:

show specific item

Example:

```
GS-4210-24P2S# show version
Loader Version   : 2011.12.41872
Loader Date      : May 22 2014 - 19:28:43
Firmware Version : v1.0b140611
Firmware Date    : Wed Jun 11 10:13:28 CST 2014
Magic Number     : 83800000
GS-4210-24P2S#
```

6.2.17 ssl command

Description:

Setup SSL host keys

Syntax:

ssl

Example:

```
GS-4210-24P2S# ssl
Generating a 1024 bit RSA private key
.....++++++
writing new private key to '/mnt/ssh/ssl_key.pem'
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:2
string is too short, it needs to be at least 2 bytes long
Country Name (2 letter code) [AU]:TW
State or Province Name (full name) [Some-State]:TW
Locality Name (eg, city) []:Taipei
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PLANET
Organizational Unit Name (eg, section) []:GS-4210-24P2S
Common Name (e.g. server FQDN or YOUR name) []:Marc
Email Address []:marcl@planet.com.tw
GS-4210-24P2S#
```

6.2.18 traceroute command

Description:

Trace route to network hosts

Syntax:

traceroute HOSTNAME (The IP address or hostname address to trace)

Example:

```
GS-4210-24P2S> traceroute 192.168.0.100
```

6.2.19 uddl command

Description:

Configure global UDLD setting

Syntax:

uddl reset

Example:

```
GS-4210-24P2S# uddl reset
```

```
GS-4210-24P2S# *Jan 01 08:16:26: %UDLD-5: No ports are disabled by UDLD
```

6.3 Global Config Mode Commands

6.3.1 aaa Command

Description:

AAA (Authentication, Authorization, Accounting)

Syntax:

aaa accounting commands / exec / system / update

aaa authentication enable / login

6.3.2 boot Command

Description:

Booting Operations

Syntax:

boot host auto-config

boot system image0/1

6.3.3 bridge Command

Description:

Global bridge table configuration

Syntax:

bridge multicast reserved-address xx:xx:xx:xx:xx:xx bridge / discard / peer

6.3.4 class-map Command

Description:

Create class map and enter class map configuration mode. Use no form in order to delete the class

Syntax:

class-map WORD<0-32> (specified the name of the class map).

6.3.5 clock Command

Description:

Manage the system clock

Syntax:

clock source local / sntp

clock summer-time

clock timezone

6.3.6 dos Command

Description:

DoS information

Syntax:

dos

daeqsa-deny	Destination MAC equals to source MAC
icmp-frag-pkts-deny	Fragmented ICMP packets
icmp-ping-max-length	DoS information
icmpv4-ping-max-check	Check ICMPv4 ping maximum packets size
icmpv6-ping-max-check	Check ICMPv6 ping maximum packets size
ipv6-min-frag-size-check	Check minimum size of IPv6 fragments
ipv6-min-frag-size-length	DoS information
land-deny	Source IP equals to destination IP
nullscan-deny	NULL Scan Attacks
pod-deny	Ping of Death Attacks
smurf-deny	Smurf Attacks
smurf-netmask	DoS information
syn-sportl1024-deny	SYN packets with sport less than 1024
synfin-deny	SYN and FIN bits set in the packet
synrst-deny	SYN and RST bits set in the packet
tcp-frag-off-min-check	TCP fragment packet with offset equals to one
tcpblat-deny	Source TCP port equals to destination TCP port
tcphdr-min-check	Check minimum TCP header
tcphdr-min-length	DoS information
udpblat-deny	Source UDP port equals to destination UDP port
xma-deny	Xmascan: sequence number is zero and the FIN, URG and PSH bits are set

6.3.7 dot1x Command

Description:

802.1x configuration

Syntax:

dot1x guest-vlan<1-4094> VLAN ID (e.g. 100)

6.3.8 do Command

Description:

To run exec commands in current mode

Syntax:

do SEQUENCE (Exec Command)

6.3.9 enable Command

Description:

Local Enable Password

Syntax:

enable password / privilege / secret

6.3.10 end Command

Description:

End current mode and change to enable mode

Syntax:

end

6.3.11 errdisable Command

Description:

Error Disable

Syntax:

errdisable recovery cause / interval

6.3.12 exit Command

Description:

Exit current mode and down to previous mode

Syntax:

Exit

6.3.13 gvrp Command

Description:

GVRP configuration

Syntax:

gvrp time join / leave / leaveall

6.3.14 hostname Command

Description:

Set system's network name

Syntax:

hostname WORD (this system's network name)

6.3.15 interface Command

Description:

Select an interface to configure

Syntax:

Interface GigabitEthernet / LAG / range

6.3.16 ip Command

Description:

IP configuration

Syntax:

ip
 acl This command creates an ACL, which perform classification on layer 3 fields and enters ip-access configuration mode.
 address IPv4 Address
 arp ARP configuration
 default-gateway Set default gateway IP address
 dhcp DHCP configuration
 dns Domain Name Server
 http HTTP server configuration
 https HTTPS server configuration
 igmp IGMP Configuration
 source IP Source Guard Configuration
 ssh SSH (Secure Shell) configuration
 telnet Telnet daemon configuration

6.3.17 ipv6 Command

Description:

IPV6 configuration

Syntax:

ipv6
 acl This command creates an ACL, which perform classification on layer 3 fields and enters to ipv6-access configuration mode.
 address Set IPv6 address and prefix
 autoconfig Enable Ipv6 auto-configuration
 default-gateway Set IPv6 gateway
 dhcp Set IPv6 DHCP Client
 mld MLD Configuration

6.3.18 jumbo-frame Command

Description:

Jumbo Frame configuration

Syntax:

jumbo-frame <64-9216> (Maximum frame size)

6.3.19 I2 Command

Description:

L2 information

Syntax:

I2 igmp snooping unknown-multicast action drop / flood

6.3.20 lacp Command

Description:

LACP Configuration

Syntax:

lacp system-priority <1-65535> (LACP system priority)

6.3.21 lag Command

Description:

Link Aggregation Group Configuration

Syntax:

lag load-balance src-dst-mac / src-dst-mac-ip

6.3.22 line Command

Description:

To identify a specific line for configuration

Syntax:

line console / ssh / telnet

6.3.23 lldp Command

Description:

LLDP Configuration

Syntax:

```
lldp
holdtime-multiplier    Configure LLDP holdtime multiplier
lldpdu                 Configure LLDP PDU handling when LLDP is disabled
med                    LLDP MED configuration
reinit-delay           Configure LLDP reinitialization delay
tx-delay               Configure LLDP TX delay
tx-interval            Configure LLDP transmission interval
```

6.3.24 logging Command

Description:

Log Configuration

Syntax:

```
logging
buffered  RAM
flash    Flash
host      Remote syslog host
```

6.3.25 mac Command

Description:

MAC Configuration

Syntax:

```
mac
acl          This command enters the extended MAC ACL configuration in order to create layer 2 extended ACL.
address-table  MAC address table configuration
```

6.3.26 management-vlan Command

Description:

Management VLAN configuration

Syntax:

```
management-vlan vlan <1-4094>  VLAN ID (e.g. 100)
```

6.3.27 mirror Command

Description:

Mirror configuration

Syntax:

mirror session <1-4> Session ID (e.g. 1-4)configuraton destination / source interface / GigabitEthernet <1-26> GigabitEthernet device number

6.3.28 no Command

Description:

Negate command

Syntax:

no

6.3.29 policy-map Command

Description:

This command create policy map and enter policy map configuration mode. Use no form to delete the policy map

Syntax:

policy-map WORD<0-32> (Enter the policy-map name)

6.3.30 port-security Command

Description:

Port security Configuration

Syntax:

port-security

6.3.31 qos Command

Description:

Enable / Disable QoS on the device and enter the QoS mode (advance / basic)

Syntax:

qos

advanced Enable/Disable QoS on the device and enter the QoS mode (advance/basic).

advanced-mode Set the trust mode when the default action is ports-trusted in advanced mode.

aggregate-policer Configure a policer that can be applied to multiple classes within the same policy map. Use the no form of the command to remove policer.

basic Set system QoS advance mode.

map Configure the QoS maps.

queue Queue configuration

trust Configure the global trust mode . Use the no form to return untrusted state.

6.3.32 radius Command

Description:

RADIUS server information

Syntax:

radius default-config / host

6.3.33 rate-limit Command

Description:

Rate limit configuration of the specified incoming traffic

Syntax:

rate-limit egress / ingress

6.3.34 rmon Command

Description:

RMON information

Syntax:

rmon alarm / event / history

6.3.35 Snmp Command

Description:

SNMP information

Syntax:

```
snmp
community      Set community or security name string
engineid       SNMP engine id setting
group          Set access group string
host           Trap or inform host
trap          Snmp class trap setting
user          Set user Settings
view          Set view string
```

6.3.36 sntp Command

Description:

Simple Network Time Protocol

Syntax:

```
sntp host
```

6.3.37 spanning-tree Command

Description:

Spanning-tree configuration

Syntax:

```
Spanning-tree
bpd          action for bpdu packet
forward-delay Sets the forward-delay parameter
hello-time   Sets the hello-time parameter
max-hops     Sets the max-hops parameter
maximum-age  Changes the interval between messages the spanning tree receive s from the root switch
mode        Spanning tree protocol type
mst         Multiple spanning tree configuration
pathcost    Spanning tree path-cost method
priority     Sets the priority for specified instance
tx-hold-count Set spanning-tree tx hold count, in seconds
```

6.3.38 storm-control Command

Description:

Storm control configuration

Syntax:

Storm-control

ifg Interframe configuration

unit Unit configuration

6.3.39 system Command

Description:

System information

Syntax:

contact Set host contact

location Set host location

name Set host name

6.3.40 tacacs Command

Description:

TACACS+ server information

Syntax:

tacacs

default-config TACACS+ server default parameters

host TACACS+ server host

6.3.41 uddl Command

Description:

Configure global UDLD setting

Syntax:

uddl

aggressive Enable UDLD protocol in aggressive mode on fiber ports except where locally configured

enable Enable UDLD protocol on fiber ports except where locally configured

message Set UDLD message parameters

6.3.42 username Command

Description:

Local User Configuration

Syntax:

username USERNAME Local user name
nopassword No password for this user
password Use clear text password
privilege Local user privilege level
secret Use encrypted password

6.3.43 vlan Command

Description:

VLAN Configuration

Syntax:

vlan
VLAN-LIST VLAN List (e.g. 3,6-8): The range of VLAN ID is 1 to 4094
protocol-vlan 802.1v protocol VLAN configuration

6.3.44 voice-vlan Command

Description:

Voice VLAN Configuration

Syntax:

voice vlan <1-4094> (Specifies the Voice VLAN Identifier)

7. SWITCH OPERATION

7.1 Address Table

The Switch is implemented with an address table. This address table composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port no, etc. This information comes from the learning process of Ethernet Switch.

7.2 Learning

When one packet comes in from any port, the Switch will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

7.3 Forwarding & Filtering

When one packet comes from some port of the Ethernet Switching, it will also check the destination address besides the source address learning. The Ethernet Switching will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, the Ethernet Switching 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

7.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward Ethernet Switching stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets occurrence, it is the best choice when a network needs efficiency and stability.

The Ethernet Switch scans the destination address from the packet-header, searches the routing table provided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment existence hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using conventional cabling and adapters.

Due to the learning function of the Ethernet switching, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The Switch performs "Store and forward" therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

7.5 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 detect the modes and speeds at the second of both device is connected and capable of, both 10BASE-T and 100BASE-TX devices can connect with the port in either Half- or Full-Duplex mode.

If attached device is:	100BASE-TX port will set to:
10Mbps, no auto-negotiation	10Mbps.
10Mbps, with auto-negotiation	10/20Mbps (10BASE-T/Full-Duplex)
100Mbps, no auto-negotiation	100Mbps
100Mbps, with auto-negotiation	100/200Mbps (100BASE-TX/Full-Duplex)

8. POWER OVER ETHERNET OVERVIEW

What is PoE?

The PoE is an abbreviation of Power over Ethernet; the PoE technology means a system to pass electrical power safely, along with data on Ethernet UTP cable. The IEEE standard for PoE technology requires Category 5 cable or higher for high power PoE levels, but can operate with category 3 cable for low power levels. Power is supplied in common mode over two or more of the differential pairs of wires found in the Ethernet cables and comes from a power supply within a PoE-enabled networking device such as an Ethernet switch or can be injected into a cable run with a mid-span power supply.

The original IEEE 802.3af-2003 PoE standard provides up to 15.4 W of DC power (minimum 44 V DC and 350mA) to each device. Only 12.95 W is assured to be available at the powered device as some power is dissipated in the cable.

The updated IEEE 802.3at-2009 PoE standard also known as PoE+ or PoE plus, provides up to 25.5 W of power. The 2009 standard prohibits a powered device from using all four pairs for power

The 802.3af / 802.3at define two types of source equipment: Mid-Span and End-Span.

Mid-Span

Mid-Span device is placed between legacy switch and the powered device. Mid-Span is tap the unused wire pairs 4/5 and 7/8 to carry power, the other four is for data transmit.

End-Span

End-Span device is direct connecting with power device. End-Span could also tap the wire 1/2 and 3/6.

PoE System Architecture

The specification of PoE typically requires two devices: the **Powered Source Equipment (PSE)** and the **Powered Device (PD)**. The PSE is either an End-Span or a Mid-Span, while the PD is a PoE-enabled terminal, such as IP Phones, Wireless LAN, etc. Power can be delivered over data pairs or spare pairs of standard CAT-5 cabling.

Powered Source Equipment (PSE)

Power sourcing equipment (PSE) is a device such as a switch that provides (sources) power on the Ethernet cable. The maximum allowed continuous output power per cable in IEEE 802.3af is 15.40 W. A later specification, IEEE 802.3at, offers 25.50 W. When the device is a switch, it is commonly called an End-span (although IEEE 802.3af refers to it as endpoint). Otherwise, if it's an intermediary device between a non PoE capable switch and a PoE device, it's called a Mid-span. An external PoE injector is a Mid-span device

Powered device

A powered device (PD) is a device powered by a PSE and thus consumes energy. Examples include wireless access points, IP Phones, and IP cameras. Many powered devices have an auxiliary power connector for an optional, external, power supply. Depending on the PD design, some, none, or all power can be supplied from the auxiliary port, with the auxiliary port sometimes acting as backup power in case of PoE supplied power failure.

How Power is Transferred Through the Cable

A standard CAT5 Ethernet cable has four twisted pairs, but only two of these are used for 10BASE-T and 100BASE-TX. The specification allows two options for using these cables for power, shown in Figure 1 and Figure 2:

The spare pairs are used. Figure 1 shows the pair on pins 4 and 5 connected together and forming the positive supply, and the

pair on pins 7 and 8 connected and forming the negative supply. (In fact, a late change to the spec allows either polarity to be used).

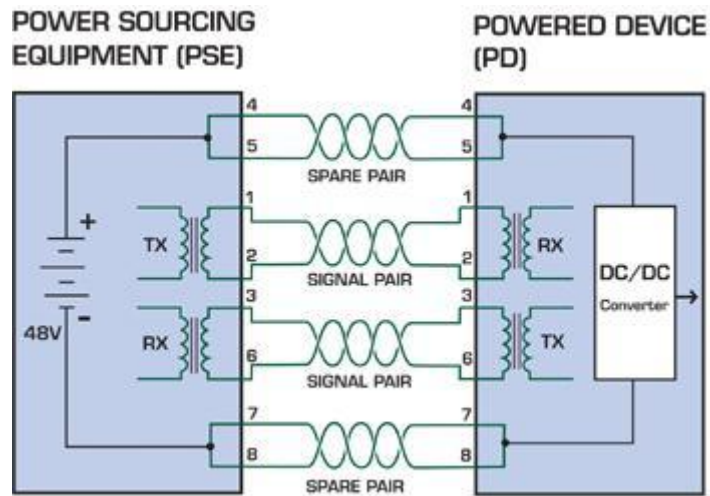


Figure 8-1: Power Supplied over the Spare Pins

The data pairs are used. Since Ethernet pairs are transformer coupled at each end, it is possible to apply DC power to the center tap of the isolation transformer without upsetting the data transfer. In this mode of operation the pair on pins 3 and 6 and the pair on pins 1 and 2 can be of either polarity.

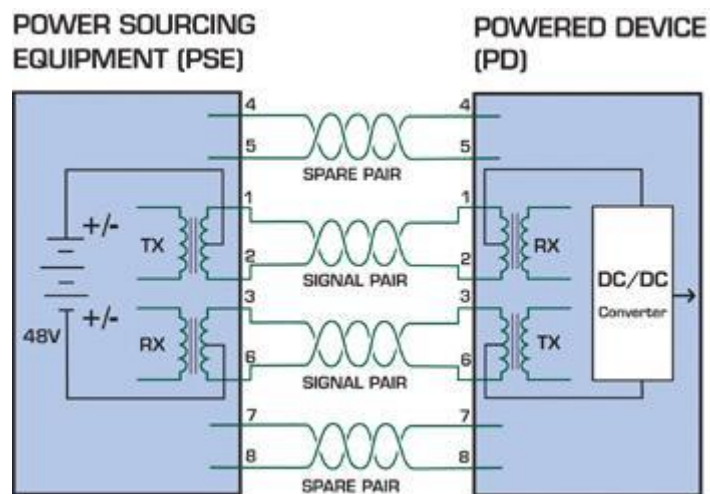


Figure 8-2: Power Supplied over the Data Pins

9. TROUBLESHOOTING

This chapter contains information to help you solve your issue. If the Managed Switch is not functioning properly, make sure the Managed Switch is set up according to instructions in this manual.

■ The Link LED is not lit

Solution:

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

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

Solution:

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

■ Performance is bad

Solution:

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

■ Why the Switch doesn't connect to the network

Solution:

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

■ 100BASE-TX port link LED is lit, but the traffic is irregular

Solution:

Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

■ Switch does not power up

Solution:

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

APPENDIX A

A.1 Switch's RJ45 Pin Assignments 1000Mbps, 1000BASE-T

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

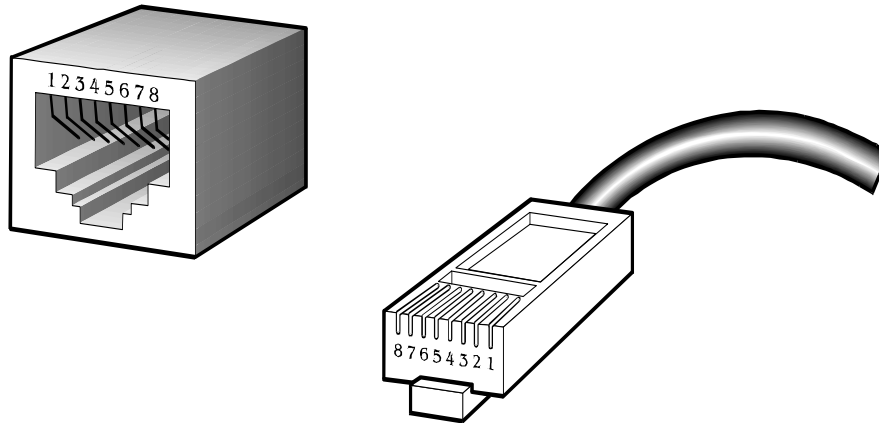
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

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

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ45 receptacle/connector and their pin assignments:

RJ45 Connector pin assignment		
Contact	MDI Media Dependent Interface	MDI-X Media Dependent Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

The standard cable, 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 cable and crossover cable connection:

Straight-through Cable		SIDE 1	SIDE 2						
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 SIDE 2	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		
1	2	3	4	5	6	7	8		
1	2	3	4	5	6	7	8		
1	2	3	4	5	6	7	8		
1	2	3	4	5	6	7	8		
1	2	3	4	5	6	7	8		
Crossover Cable		SIDE 1	SIDE 2						
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 SIDE 2	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		
1	2	3	4	5	6	7	8		
1	2	3	4	5	6	7	8		
1	2	3	4	5	6	7	8		
1	2	3	4	5	6	7	8		
1	2	3	4	5	6	7	8		

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 table before deploying the cables into your network.



EC Declaration of Conformity

For the following equipment:

*Type of Product : 24-Port 10/100/1000T 802.3at PoE + 2-Port 100/1000X SFP
Managed Switch
*Model Number : GS-4210-24P2S
* Produced by:
Manufacturer's Name : **Planet Technology Corp.**
Manufacturer's Address : 10F., No.96, Minquan Rd., Xindian Dist.,
New Taipei City 231, Taiwan (R.O.C.).

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (2004/108/EC) and Low Voltage Directive 2006/95/EC.

For the evaluation regarding the EMC, the following standards were applied:

EN 55022	(2010)
EN 61000-3-2	(2006+A1:2009+A2:2009)
EN 61000-3-3	(2013)
EN 55024	(2010)
EN 61000-4-2	(2009)
EN 61000-4-3	(2006+A1:2008+A2:2010)
EN 61000-4-4	(2012)
EN 61000-4-5	(2006)
EN 61000-4-6	(2014)
EN 61000-4-8	(2010)
EN 61000-4-11	(2004)
EN60950-1	(2006+A11:2009+A1:2010+A12:2011+AC:2011+A2:2013)

Responsible for marking this declaration if the:

Manufacturer Authorized representative established within the EU

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.)**

Person responsible for making this declaration

Name, Surname **Kent Kang**

Position / Title : **Product Manager**

Taiwan
Place

15th, Aug., 2014
Date


Legal Signature

PLANET TECHNOLOGY CORPORATION

e-mail: sales@planet.com.tw http://www.planet.com.tw

10F., No.96, Minquan Rd., Xindian Dist., New Taipei City, Taiwan, R.O.C. Tel:886-2-2219-9518 Fax:886-2-2219-9528

EC Declaration of Conformity

For the following equipment:

*Type of Product : 16-Port Layer 2 Managed Gigabit Ethernet Switch W/2 SFP Interfaces

*Model Number : GS-4210-16T2S

* Produced by:

Manufacturer's Name : **Planet Technology Corp.**

Manufacturer's Address : 10F., No.96, Minquan Rd., Xindian Dist.,
New Taipei City 231, Taiwan (R.O.C.).

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (2004/108/EC) and Low Voltage Directive 2006/95/EC.

For the evaluation regarding the EMC, the following standards were applied:

EN 55022	(2010+AC: 2011)
EN 61000-3-2	(2014)
EN 61000-3-3	(2013)
EN 55024	(2010)
IEC 61000-4-2	(2008)
IEC 61000-4-3	(2010)
IEC 61000-4-4	(2012)
IEC 61000-4-5	(2005)
IEC 61000-4-6	(2013)
IEC 61000-4-8	(2009)
IEC 61000-4-11	(2004)
EN60950-1	(2006+A11:2009+A1:2010+A12:2011+A2:2013)

Responsible for marking this declaration if the:

Manufacturer Authorized representative established within the EU

Authorized representative established within the EU (if applicable):

Company Name: Planet Technology Corp.

Company Address: 10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.)

Person responsible for making this declaration

Name, Surname Kent Kang

Position / Title : Product Manager

Taiwan

Place

25th June, 2015

Date



Legal Signature

PLANET TECHNOLOGY CORPORATION

e-mail: sales@planet.com.tw http://www.planet.com.tw

10F., No.96, Minquan Rd., Xindian Dist., New Taipei City, Taiwan, R.O.C. Tel:886-2-2219-9518 Fax:886-2-2219-9528

EC Declaration of Conformity

For the following equipment:

*Type of Product : 24-Port Layer 2 Managed Gigabit Ethernet Switch W/2 SFP Interfaces

*Model Number : GS-4210-24T2S

* Produced by:

Manufacturer's Name : **Planet Technology Corp.**

Manufacturer's Address : 10F., No.96, Minquan Rd., Xindian Dist.,
New Taipei City 231, Taiwan (R.O.C.).

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (2004/108/EC) and Low Voltage Directive 2006/95/EC.

For the evaluation regarding the EMC, the following standards were applied:

EN 55022	(2010+AC: 2011)
EN 61000-3-2	(2014)
EN 61000-3-3	(2013)
EN 55024	(2010)
IEC 61000-4-2	(2008)
IEC 61000-4-3	(2010)
IEC 61000-4-4	(2012)
IEC 61000-4-5	(2005)
IEC 61000-4-6	(2013)
IEC 61000-4-8	(2009)
IEC 61000-4-11	(2004)
EN60950-1	(2006+A11:2009+A1:2010+A12:2011+A2:2013)

Responsible for marking this declaration if the:

Manufacturer Authorized representative established within the EU

Authorized representative established within the EU (if applicable):

Company Name: Planet Technology Corp.

Company Address: 10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.)

Person responsible for making this declaration

Name, Surname Kent Kang

Position / Title : Product Manager

Taiwan

Place

26th June, 2015

Date



Legal Signature

PLANET TECHNOLOGY CORPORATION

e-mail: sales@planet.com.tw http://www.planet.com.tw

10F., No.96, Minquan Rd., Xindian Dist., New Taipei City, Taiwan, R.O.C. Tel:886-2-2219-9518 Fax:886-2-2219-9528