

User's Manual



Gigabit Ethernet L2/L4 Managed Switch

► GS-4210 Series



Trademarks

Copyright © PLANET Technology Corp. 2016.

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 GS-4210 Series User's Manual

FOR MODEL: GS-4210-8P2S / GS-4210-8P2T2S /GS-4210-16P4C/ GS-4210-24P4C / GS-4210-24PL4C / GS-4210-48T4S / GS-4210-48P4S

REVISION: 1.3 (Aug, 2016)

Part No: EM-GS-4210-series_v1.3

TABLE OF CONTENTS

1. INTRODUCTION.....	10
1.1 Packet Contents	10
1.2 Product Description	11
1.3 How to Use This Manual	14
1.4 Product Features	15
1.5 Product Specifications	18
2. INSTALLATION	31
2.1 Hardware Description	31
2.1.1 Switch Front Panel	31
2.1.2 LED Indications	33
2.1.3 Switch Rear Panel	39
2.2 Installing the Switch.....	41
2.2.1 Desktop Installation	41
2.2.2 Rack Mounting.....	42
2.2.3 Installing the SFP transceiver	44
3. SWITCH MANAGEMENT	47
3.1 Requirements.....	47
3.2 Management Access Overview.....	48
3.3 Administration Console	49
3.4 Web Management	50
3.5 SNMP-based Network Management	51
3.6 PLANET Smart Discovery Utility	51
4. WEB CONFIGURATION	54
4.1 Main Web Page	57
4.1.1 Save Button.....	58
4.1.2 Configuration Manager	59
4.1.2.1 Saving Configuration	60
4.2 System.....	61

4.2.1 System Information.....	61
4.2.2 IP Configurations	62
4.2.3 IPv6 Configuration	64
4.2.4 User Configuration.....	66
4.2.5 Time Settings.....	67
4.2.5.1 System Time.....	67
4.2.5.2 SNTP Server Settings	70
4.2.6 Log Management.....	71
4.2.6.1 Local Log.....	71
4.2.6.2 Local Log.....	72
4.2.6.3 Remote Syslog	73
4.2.6.4 Log Message	75
4.2.7 SNMP Management	77
4.2.7.1 SNMP Overview	77
4.2.7.2 SNMP System Information	78
4.2.7.3 SNMP View	79
4.2.7.4 SNMP Access Group.....	80
4.2.7.5 SNMP Community	82
4.2.7.6 SNMP User.....	83
4.2.7.7 SNMPv1, 2 Notification Recipients	85
4.2.7.8 SNMPv3 Notification Recipients	86
4.2.7.9 SNMP Engine ID	87
4.2.7.10 SNMP Remote Engine ID.....	88
4.3 Port Management	90
4.3.1 Port Configuration.....	90
4.3.2 Port Counters	92
4.3.3 Bandwidth Utilization	97
4.3.4 Port Mirroring.....	98
4.3.5 Jumbo Frame	100
4.3.6 Port Error Disabled Configuration.....	101
4.3.7 Port Error Disabled	103
4.3.8 Protected Ports.....	103
4.3.9 EEE	106
4.3.10 SFP Module Information	107
4.3.10.1 SFP Module Status.....	107
4.3.10.1 SFP Module Detail Status.....	109
4.4 Link Aggregation	110
4.4.1 LAG Setting	112
4.4.2 LAG Management	113

4.4.3 LAG Port Setting.....	114
4.4.4 LACP Setting.....	116
4.4.5 LACP Port Setting.....	117
4.4.6 LAG Status	118
4.5 VLAN.....	121
4.5.1 VLAN Overview	121
4.5.2 IEEE 802.1Q VLAN	122
4.5.3 Management VLAN	126
4.5.4 Create VLAN	127
4.5.5 Interface Settings.....	128
4.5.6 Port to VLAN.....	132
4.5.7 Port VLAN Membership.....	133
4.5.8 Protocol VLAN Group Setting	134
4.5.9 Protocol VLAN Port Setting	136
4.5.10 GVRP Setting	137
4.5.11 GVRP Port Setting	139
4.5.12 GVRP VLAN	140
4.5.13 GVRP Statistics	141
4.5.14 VLAN setting example:	143
4.5.14.1 Two separate 802.1Q VLANs	143
4.5.14.2 VLAN Trunking between two 802.1Q aware switches	146
4.6 Spanning Tree Protocol	149
4.6.1 Theory	149
4.6.2 STP Global Settings	156
4.6.3 STP Port Setting.....	158
4.6.4 CIST Instance Setting.....	161
4.6.5 CIST Port Setting.....	163
4.6.6 MST Instance Configuration	165
4.6.7 MST Port Setting	167
4.6.8 STP Statistics.....	169
4.7 Multicast.....	170
4.7.1 Properties	170
4.7.2 IGMP Snooping	171
4.7.2.1 IGMP Setting	175
4.7.2.2 IGMP Querier Setting	177
4.7.2.3 IGMP Static Group.....	178
4.7.2.4 IGMP Group Table.....	179
4.7.2.5 IGMP Router Setting	180
4.7.2.6 IGMP Router Table	181

4.7.2.7 IGMP Forward All	182
4.7.3 IGMP Snooping Statics	183
4.7.4 MLD Snooping.....	186
4.7.4.1 MLD Setting.....	186
4.7.4.2 MLD Static Group	188
4.7.4.3 MLD Group Table	189
4.7.4.4 MLD Router Setting.....	189
4.7.4.5 MLD Router Table.....	191
4.7.4.6 MLD Forward All	192
4.7.5 MLD Snooping Statics	193
4.7.6 Multicast Throttling Setting	195
4.7.7 Multicast Filter	196
4.7.7.1 Multicast Profile Setting.....	197
4.7.7.2 IGMP Filter Setting	198
4.7.7.3 MLD Filter Setting.....	199
4.8 Quality of Service	201
4.8.1 Understanding QoS	201
4.8.2 General.....	202
4.8.2.1 QoS Properties.....	202
4.8.2.2 QoS Port Settings.....	203
4.8.2.3 Queue Settings.....	204
4.8.2.4 CoS Mapping.....	205
4.8.2.5 DSCP Mapping.....	207
4.8.2.6 IP Precedence Mapping	208
4.8.3 QoS Basic Mode.....	210
4.8.3.1 Global Settings	210
4.8.3.2 Port Settings.....	211
4.8.4 Rate Limit	212
4.8.4.1 Ingress Bandwidth Control	212
4.8.4.2 Egress Bandwidth Control	213
4.8.4.3 Egress Queue	214
4.8.5 Voice VLAN	215
4.8.5.1 Introduction to Voice VLAN.....	215
4.8.5.2 Properties	216
4.8.5.3 Telephony OUI MAC Setting.....	217
4.8.5.4 Telephony OUI Port Setting	219
4.9 Security	221
4.9.1 802.1X	221
4.9.1.1 Understanding IEEE 802.1X Port-based Authentication.....	222

4.9.1.2 802.1X Setting	225
4.9.1.3 802.1X Port Setting	226
4.9.1.4 Guest VLAN Setting	228
4.9.1.5 Authenticated Host	230
4.9.2 RADIUS Server	231
4.9.3 TACACS+ Server	234
4.9.4 AAA	236
4.9.4.1 Login List	237
4.9.4.2 Enable List	238
4.9.5 Access	239
4.9.5.1 Telnet	239
4.9.5.2 SSH	240
4.9.5.3 HTTP	242
4.9.5.4 HTTPs	243
4.9.6 Management Access Method	244
4.9.6.1 Profile Rules	244
4.9.6.2 Access Rules	246
4.9.7 DHCP Snooping	247
4.9.7.1 DHCP Snooping Overview	247
4.9.7.2 Global Setting	248
4.9.7.3 DHCP Snooping VLAN Setting	249
4.9.7.4 Port Setting	251
4.9.7.5 Statistics	253
4.9.7.6 Database Agent	254
4.9.7.7 Rate Limit	256
4.9.7.8 Option82 Global Setting	257
4.9.7.9 Option82 Port Setting	258
4.9.7.10 Option82 Circuit-ID Setting	260
4.9.8 Dynamic ARP Inspection	261
4.9.8.1 Global Setting	261
4.9.8.2 VLAN Setting	262
4.9.8.3 Port Setting	263
4.9.8.4 Statistics	265
4.9.8.5 Rate Limit	266
4.9.9 IP Source Guard	267
4.9.9.1 Port Settings	268
4.9.9.2 Binding Table	270
4.9.10 Port Security	271
4.9.11 DoS	273
4.9.11.1 Global DoS Setting	273

4.9.11.2 DoS Port Setting	276
4.9.12 Storm Control.....	277
4.9.12.1 Global Setting.....	277
4.9.12.2 Port Setting.....	278
4.10 ACL	280
4.10.1 MAC-based ACL	281
4.10.2 MAC-based ACE	282
4.10.3 IPv4-based ACL.....	285
4.10.4 IPv4-based ACE	286
4.10.5 IPv6-based ACL.....	291
4.10.6 IPv6-based ACE	292
4.10.7 ACL Binding.....	297
4.11 MAC Address Table	298
4.11.1 Static MAC Setting	299
4.11.2 MAC Filtering	300
4.11.3 Dynamic Address Setting.....	301
4.11.4 Dynamic Learned.....	302
4.12 LLDP	304
4.12.1 Link Layer Discovery Protocol	304
4.12.2 LLDP Global Setting	305
4.12.3 LLDP Port Setting	307
4.12.4 LLDP Local Device	310
4.12.5 LLDP Remove Device	312
4.12.6 MED Network Policy.....	313
4.12.7 MED Port Setting.....	317
4.12.8 LLDP Overloading	320
4.12.9 LLDP Statistics.....	321
4.13 Diagnostics	323
4.13.1 Cable Diagnostics.....	323
4.13.2 Ping	325
4.13.3 Ping Test.....	325
4.13.4 IPv6 Ping Test.....	326
4.13.5 Trace Router	327
4.14 RMON.....	328
4.14.1 RMON Statistics	328
4.14.2 RMON Event	330
4.14.3 RMON Event Log	331
4.14.4 RMON Alarm	332

4.14.5 RMON History	335
4.14.6 RMON History Log	336
4.15 Power over Ethernet	337
4.15.1 Power over Ethernet Powered Device	338
4.15.2 System Configuration	339
4.15.3 Power over Ethernet Configuration.....	340
4.15.4 PoE Schedule	343
4.15.5 PoE Alive Check Configuration	346
4.16 Maintenance.....	348
4.16.1 Factory Default	348
4.16.2 Reboot Switch	348
4.16.3 Backup Manager	349
4.16.4 Upgrade Manager.....	349
4.16.5 Dual Image	351
5. SWITCH OPERATION	352
5.1 Address Table	352
5.2 Learning	352
5.3 Forwarding and Filtering	352
5.4 Store-and-Forward	352
5.5 Auto-Negotiation	353
6. TROUBLESHOOTING.....	354
APPENDIX A Switch's RJ45 Pin Assignments	356
A.1 1000Mbps, 1000BASE-T	356
A.2 10/100Mbps, 10/100BASE-TX.....	356

1. INTRODUCTION

Thank you for purchasing PLANET GS-4210 Managed Switch series, which comes with multiple Gigabit Ethernet copper and SFP fiber optic connectivity and robust layer 2 and layer 4 features. The description of this model is shown below:

GS-4210-8P2S	8-Port 10/100/1000T 802.3at PoE + 2-Port 100/1000X SFP Managed Switch
GS-4210-8P2T2S	8-Port 10/100/1000BASE-T 802.3at PoE Plus + 2-Port 10/100/1000BASE-T + 2-Port 100/1000BASE-X SFP Managed Switch (240W)
GS-4210-16P4C	16-Port 10/100/1000BASE-T PoE Plus Plus + 4-Port Gigabit TP/SFP Combo Managed Switch (220W)
GS-4210-24P4C	24-Port 10/100/1000BASE-T PoE Plus Plus + 4-Port Gigabit TP/SFP Combo Managed Switch (220W)
GS-4210-24PL4C	24-Port 10/100/1000BASE-T PoE Plus Plus + 4-Port Gigabit TP/SFP Combo Managed Switch (440W)
GS-4210-48T4S	48-Port 10/100/1000BASE-T + 4-Port 100/1000BASE-X SFP Managed Gigabit Switch
GS-4210-48P4S	48-Port 10/100/1000T 802.3at PoE + 4-Port 100/1000BASE-X SFP Managed Switch (440W)

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

1.1 Packet Contents

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

Model Name	GS-4210-8P2S	GS-4210-8P2T2S	GS-4210-16P4C	GS-4210-24P4C GS-4210-24PL4C	GS-4210-48T4S GS-4210-48P4S
Item					
The Managed Switch	■	■	■	■	■
Quick Installation Guide	■	■	■	■	■
RS-232 to RJ45 Console Cable	x	■	■	■	x
Rubber Feet	■	■	■	■	■
Two Rack-mounting Brackets with Attachment Screws	■	■	■	■	■
Power Cord	■	■	■	■	■
SFP Dust Caps	2	2	4	4	4

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

1.2 Product Description

Perfect Managed PoE+ Switch with Full PoE+ Power Budget

PLANET GS-4210 PoE series is the new generation of PLANET Managed Gigabit PoE+ Switch featuring PLANET **intelligent PoE** functions to improve the availability of critical business applications. It provides a quick, safe and cost-effective Power over Ethernet network solution to IP security surveillance for small businesses and enterprises.

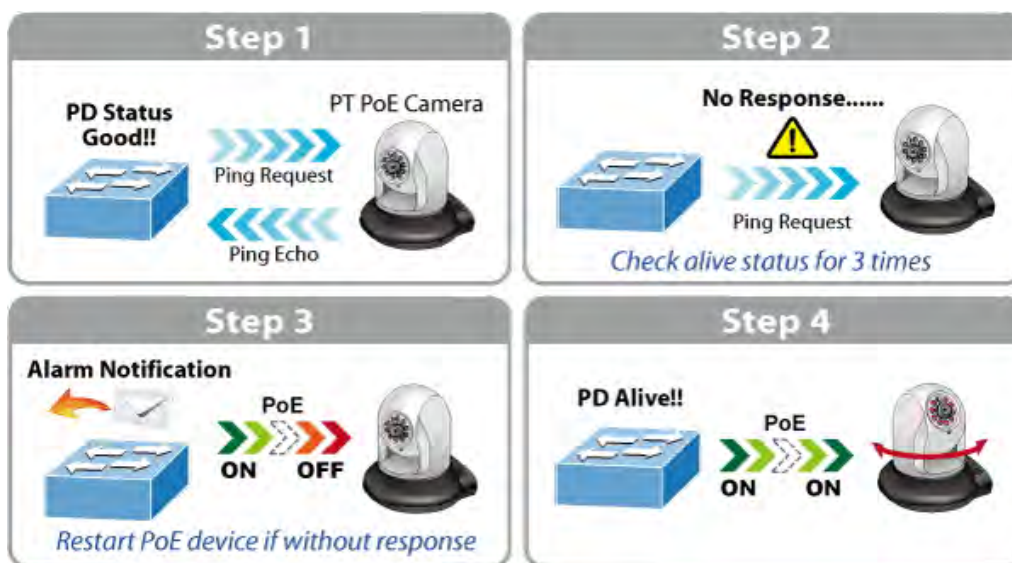
Built-in Unique PoE Functions for Powered Devices Management

As a managed PoE Switch for surveillance, wireless and VoIP networks, the GS-4210 PoE series features special PoE Management functions:

- PD Alive Check
- Scheduled Power Recycling
- PoE Schedule
- PoE Usage Monitoring

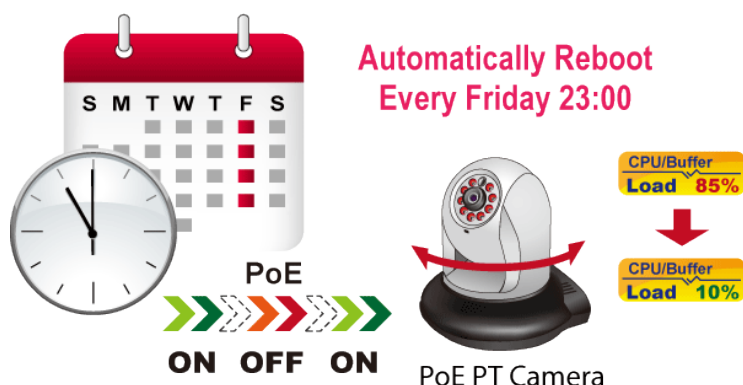
Intelligent Powered Device Alive Check

The GS-4210 PoE series can be configured to monitor connected PD (powered device) status in real time via ping action. Once the PD stops working and responding, the GS-4210 PoE series will resume the PoE port power and bring the PD back to work. It will greatly enhance the network reliability through the PoE port resetting the PD's power source and reducing administrator management burden.



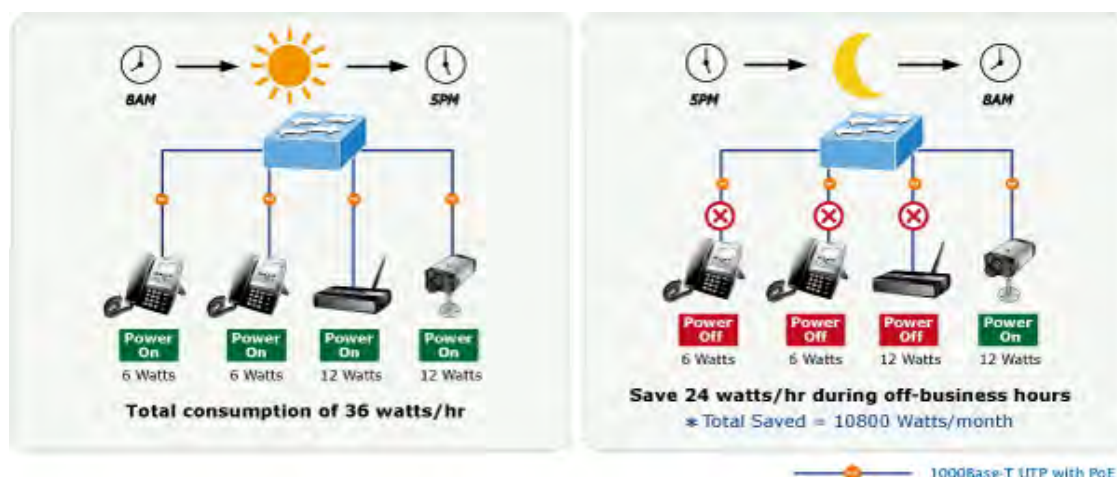
Scheduled Power Recycling

The GS-4210 PoE series allows each of the connected PoE IP cameras or PoE wireless access points to reboot at a specific time each week. Therefore, it will reduce the chance of IP camera or AP crash resulting from buffer overflow.



PoE Schedule for Energy Saving

Under the trend of energy saving worldwide and contributing to environmental protection, the GS-4210 PoE series can effectively control the power supply besides its capability of giving high watts power. The “**PoE schedule**” function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is a powerful function to help SMBs or enterprises save power and money. It also increases security by powering off PDs that should not be in use during non-business hours.



PoE Usage Monitoring

Via the power usage chart in the web management interface, the GS-4210 PoE series enables the administrator to monitor the status of the power usage of the connected PDs in real time. Thus, it greatly enhances the management efficiency of the facilities.

Environment-friendly, Smart Fan Design for Silent Operation

The GS-4210 series features a desktop-sized metal housing, a low noise design and an effective ventilation system. It supports the smart fan technology to automatically control the speed of the built-in fan to reduce noise and maintain the temperature of the PoE switch for optimal power output capability. The GS-4210 series is able to operate reliably, stably and quietly in any environment without affecting its performance.

IPv6/IPv4 Dual Stack

Supporting both IPv6 and IPv4 protocols, the GS-4210 series helps the SMBs to step in the IPv6 era with the lowest investment as its network facilities need not be replaced or overhauled if the IPv6 FTTx edge network is set up.

Robust Layer 2 Features

The GS-4210 series 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 GS-4210 series allows the operation of a high-speed trunk to combine with multiple ports such as a 16Gbps 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 GS-4210 series 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 **storm control**, per port **bandwidth control**, IP DSCP QoS priority and remarking. It guarantees the best performance for VoIP and video stream transmission, and empowers the enterprises to take full advantage of the limited network resources.

Powerful Security

PLANET GS-4210 series offers 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** user and device 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 to limit the number of network devices on a given port.

Advanced Network Security

The GS-4210 series also provides **DHCP Snooping**, **IP Source Guard** and **Dynamic ARP Inspection** functions to prevent IP snooping from attack and discard ARP packets with invalid MAC address. The network administrators can now construct highly secured corporate networks with considerably less time and effort than before.

Friendly and Secure Management

For efficient management, the GS-4210 series is equipped with console, **Web**, **Telnet** and **SNMP** management interfaces. With the built-in Web-based management interface, the GS-4210 series offers an easy-to-use, platform-independent management and configuration facility. By supporting the 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 GS-4210 series offers secure remote management by supporting **SSH**, **SSL** and **SNMPv3** connections which encrypt the packet content at each session.

Flexibility and Extension Solution

The GS-4210 series provides Gigabit TP/SFP interfaces supporting 10/100/1000BASE-T RJ45 copper to connect with surveillance network devices such as NVR, Video Streaming Server or NAS to facilitate surveillance management. Or through these dual-speed fiber SFP slots, it can also connect with the **100BASE-FX/1000BASE-SX/LX** SFP (small form-factor pluggable) fiber transceiver and then to backbone switch and monitoring center over a long distance. The distance can be extended from 550 meters to 2 kilometers (multi-mode fiber) and up to 10/20/30/40/50/70/120 kilometers (single-mode fiber or WDM fiber). They are well suited for applications within the enterprise data centers and distributions.

Intelligent SFP Diagnosis Mechanism

The GS-4210 series supports SFP-DDM (**Digital Diagnostic Monitor**) function that greatly helps network administrator to easily monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current and transceiver supply voltage.

1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2, INSTALLATION

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

Section 3, SWITCH MANAGEMENT

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

Section 4, WEB CONFIGURATION

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

Section 5, SWITCH OPERATION

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

Section 6, TROUBLESHOOTING

The chapter explains how to troubleshoot the Managed Switch.

Appendix A

The section contains cable information of the Managed Switch.

1.4 Product Features

► Physical Port

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

► Power over Ethernet (GS-4210 PoE Series)

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

► Layer 2 Features

- Prevents packet loss with back pressure (half-duplex) and IEEE 802.3x pause frame flow control (full-duplex)
- High performance Store and Forward architecture, broadcast storm control, runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
- Supports **VLAN**
 - IEEE 802.1Q tagged VLAN
 - Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
 - Protocol VLAN
 - Voice VLAN
 - Private VLAN
 - 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
- Storm Control support
 - Broadcast/Unknown unicast/Unknown multicast
- Traffic classification
 - IEEE 802.1p CoS
 - TOS/DSCP/IP precedence of IPv4/IPv6 packets
- Strict priority and Weighted Round Robin (WRR) CoS policies

► **Multicast**

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

► **Security**

- Authentication
 - IEEE 802.1X port-based network access authentication
 - Built-in RADIUS client to cooperate with the RADIUS servers
 - RADIUS/TACACS+ login user access authentication
- Access Control List
 - IPv4/IPv6 IP-based ACL
 - MAC-based ACL
- 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
- SSH/SSL

► **Management**

- IPv4 and IPv6 dual stack management
- Switch Management Interface
 - Web switch management
 - Telnet Command Line Interface
 - SNMP v1, v2c and v3
 - SSH/SSL secure access
- User Privilege Levels Control
- Built-in Trivial File Transfer Protocol (TFTP) client
- BOOTP and DHCP for IP address assignment
- System Maintenance
 - Firmware upload/download via HTTP / TFTP
 - Configuration upload/download through Web interface
 - Dual Images
 - Hardware reset button for system reboot or reset to factory default
- SNTP Network Time Protocol
- Cable diagnostics
- Link Layer Discovery Protocol (LLDP) 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
- Smart fan with speed control

1.5 Product Specifications

GS-4210-8P2S / GS-4210-8P2T2S

Product	GS-4210-8P2S	GS-4210-8P2T2S
Hardware Specifications		
Copper Ports	8 x 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports	10 x 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports
SFP/mini-GBIC Slots	2 x 100/1000BASE-X SFP interfaces with Port-9 to Port-10. Supports 100/1000Mbps dual mode and DDM	2 x 100/1000BASE-X SFP interfaces with Port-11 to Port-12. Supports 100/1000Mbps dual mode and DDM
PoE Injector Port	8 ports with 802.3at/af PoE injector function with Port-1 to Port-8	8 ports with 802.3at/af PoE injector function with Port-1 to Port-8
Console	---	1 x RS-232-to-RJ45 serial port (115200, 8, N, 1)
Switch Architecture	Store-and-Forward	
Switch Fabric	20Gbps/non-blocking	24Gbps/non-blocking
Switch Throughput@64Bytes	14.88Mpps	17.76Mpps
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	10K bytes	
Reset Button	< 5 sec: System reboot > 5 sec: Factory default	
LED	PWR, Fan Alert, LNK/ACT, PoE-in-Use, 1000	PWR, SYS, LNK/ACT, PoE-in-Use, 1000
Smart Fan	1	1
Dimensions (W x D x H)	330 x 155 x 43.5 mm, 1U high	330 x 200 x 44.5 mm, 1U height
Weight	1687g	2kg
Power Requirements	AC 100~240V, 50/60Hz, auto-sensing	
ESD Protection	2KV DC	6KV DC
Power Consumption/ Dissipation	165 watts (max.)/563 BTU	320 watts (max.)/1091.8 BTU
Enclosure	Metal	
Power over Ethernet		
PoE Standard	IEEE 802.3af / 802.3at PoE / PSE	
PoE Power Supply Type	End-span	
PoE Power Output	Per port 52V DC, 36 watts (max.)	Per port 54V DC, 36 watts (max.)
Power Pin Assignment	1/2(+), 3/6(-)	

PoE Power Budget	120 watts (max.) @ 25 degrees C 100 watts (max.) @ 50 degrees C	240 watts (max.) @ 25 degrees C 200 watts (max.) @ 50 degrees C
PoE Ability PD @ 9 watts	8 units	8 units
PoE Ability PD @ 15 watts	8 units	8 units
PoE Ability PD @ 30 watts	4 units	8 units
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 Voice VLAN Protocol VLAN Private VLAN (protected port) GVRP	
Link Aggregation	IEEE 802.3ad LACP and static trunk Supports 8 groups, 8 ports per trunk group	
Spanning Tree Protocol	STP, RSTP, MSTP	
IGMP Snooping	IGMP (v2/v3) snooping IGMP querier Up to 256 multicast groups	
MLD Snooping	MLD (v1/v2) snooping, up to 256 multicast groups	
Access Control List	IPv4/IPv6 IP-based ACL/MAC-based ACL	
QoS	8 mapping ID to 8 level priority queues <ul style="list-style-type: none">- Port number- 802.1p priority- 802.1Q VLAN tag- DSCP field in IP packet Traffic classification based, strict priority and WRR	
Security	IEEE 802.1X – port-based authentication Built-in RADIUS client to cooperate with RADIUS server RADIUS/TACACS+ user access authentication IP-MAC port binding MAC filter Static MAC address DHCP snooping and DHCP option82 STP BPDU guard, BPDU filtering and BPDU forwarding DoS attack prevention ARP inspection IP source guard	
Management Functions		
Basic Management Interfaces	Web browser; Telnet; SNMP v1, v2c Firmware upgrade by HTTP/TFTP protocol through Ethernet network Remote/Local Syslog	

	System log LLDP protocol SNTP
Secure Management Interfaces	SSH/SSL, SNMP v3
SNMP MIBs	RFC 1213 MIB-II RFC 1215 Generic Traps RFC 1493 Bridge MIB RFC 2674 Bridge MIB Extensions RFC 2737 Entity MIB (Version 2) RFC 2819 RMON (1, 2, 3, 9) RFC 2863 Interface Group MIB RFC 3635 Ethernet-like MIB
Standards Conformance	
Regulatory Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/100BASE-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging IEEE 802.1x Port Authentication Network Control IEEE 802.1ab LLDP IEEE 802.3af Power over Ethernet IEEE 802.3at High Power over Ethernet 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: -20 ~ 70 degrees C Relative Humidity: 5 ~ 95% (non-condensing)

GS-4210-16P4C

Product	GS-4210-16P4C
Hardware Specifications	
Copper Ports	20 x 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports
SFP/mini-GBIC Slots	4 x 100/1000BASE-X SFP interfaces shared with Port-17 to Port-20. Supports 100/1000Mbps dual mode and DDM
PoE Injector Port	16 ports with 802.3at/af PoE injector function with Port-1 to Port-16
Console	1 x RS-232-to-RJ45 serial port (115200, 8, N, 1)
Switch Architecture	Store-and-Forward
Switch Fabric	40Gbps / non-blocking
Switch Throughput@64Bytes	29.76Mpps
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	10K bytes
Reset Button	< 5 sec: System reboot > 5 sec: Factory default
LED	PWR, SYS, LNK/ACT, PoE-in-Use, 1000, FAN 1 Alert, FAN 2 Alert, PoE PWR Alert
Smart Fan	2
Dimensions (W x D x H)	440 x 300 x 44.5 mm, 19-inch, 1U height
Weight	4.132kg
Power Requirements	AC 100~240V, 50/60Hz, auto-sensing
ESD Protection	6KV DC
Power Consumption/ Dissipation	251 watts (max.)/861.2 BTU
Enclosure	Metal
Power over Ethernet	
PoE Standard	IEEE 802.3af/802.3at PoE/PSE
PoE Power Supply Type	End-span
PoE Power Output	Per Port 52V DC, 30.8 watts (max.)
Power Pin Assignment	1/2(+), 3/6(-)
PoE Power Budget	220 watts (max.) @ 25 degrees C 190 watts (max.) @ 50 degrees C
PoE Ability PD @ 9 watts	16 units
PoE Ability PD @ 15.4 watts	14 units
PoE Ability PD @ 30 watts	7 units
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 Voice VLAN Protocol VLAN Private VLAN (Protected port) GVRP
Link Aggregation	IEEE 802.3ad LACP and static trunk Supports 8 groups, 8 ports per trunk group
Spanning Tree Protocol	STP, RSTP, MSTP
IGMP Snooping	IGMP (v2/v3) snooping IGMP querier Up to 256 multicast groups
MLD Snooping	MLD (v1/v2) snooping, up to 256 multicast groups
Access Control List	IPv4/IPv6 IP-based ACL/MAC-based ACL
QoS	8 mapping ID to 8 level priority queues - Port number - 802.1p priority - 802.1Q VLAN tag - DSCP field in IP packet Traffic classification based, strict priority and WRR
Security	IEEE 802.1X – Port-based authentication Built-in RADIUS client to cooperate with RADIUS server RADIUS/TACACS+ user access authentication IP-MAC port binding MAC filter Static MAC address DHCP snooping and DHCP option82 STP BPDU guard, BPDU filtering and BPDU forwarding DoS attack prevention ARP inspection IP source guard
Management Functions	
Basic Management Interfaces	Web browser; Telnet; SNMP v1, v2c Firmware upgrade by HTTP/TFTP protocol through Ethernet network Remote/Local Syslog System log LLDP protocol SNTP
Secure Management Interfaces	SSH/SSL, SNMP v3
SNMP MIBs	RFC 1213 MIB-II RFC 1215 Generic Traps RFC 1493 Bridge MIB RFC 2674 Bridge MIB Extensions RFC 2737 Entity MIB (version 2)

	RFC 2819 RMON (1, 2, 3, 9) RFC 2863 Interface Group MIB RFC 3635 Ethernet-like MIB
Standards Conformance	
Regulatory Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/100BASE-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging IEEE 802.1x Port Authentication Network Control IEEE 802.1ab LLDP IEEE 802.3af Power over Ethernet IEEE 802.3at High Power over Ethernet 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: -20 ~ 70 degrees C Relative Humidity: 5 ~ 95% (non-condensing)

GS-4210-24P4C / GS-4210-24PL4C

Product	GS-4210-24P4C		GS-4210-24PL4C
Hardware Specifications			
Copper Ports	28 x 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports		
SFP/mini-GBIC Slots	4 x 100/1000BASE-X SFP interfaces shared with Port-25 to Port-28. Supports 100/1000Mbps dual mode and DDM		
PoE Injector Port	24 ports with 802.3at/af PoE injector function with Port-1 to Port-24		
Console	1 x RS-232-to-RJ45 serial port (115200, 8, N, 1)		
Switch Architecture	Store-and-Forward		
Switch Fabric	56Gbps / non-blocking		
Switch Throughput@64Bytes	41.67Mpps		
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	10K bytes		
Reset Button	< 5 sec: System reboot > 5 sec: Factory default		
LED	PWR, SYS, LNK/ACT, PoE-in-Use, 1000, FAN 1 Alert, FAN 2 Alert, PoE PWR Alert		
Smart Fan	2	3	
Dimensions (W x D x H)	440 x 300 x 44.5 mm, 19-inch, 1U height		
Weight	4.214kg	4.814kg	
Power Requirements	AC 100~240V, 50/60Hz, auto-sensing		
ESD Protection	2KV DC		
Power Consumption/ Dissipation	275 watts (max.)/ 938.3 BTU	544 watts (max.)/1856.2 BTU	
Enclosure	Metal		
Power over Ethernet			
PoE Standard	IEEE 802.3af/802.3at PoE/PSE		
PoE Power Supply Type	End-span		
PoE Power Output	Per Port 52V DC, 30.8 watts (max.)		
Power Pin Assignment	1/2(+), 3/6(-)		
PoE Power Budget	220 watts (max.) @ 25 degrees C 190 watts (max.) @ 50 degrees C	440 watts (max.) @ 25 degrees C 380 watts (max.) @ 50 degrees C	
PoE Ability PD @ 9 watts	24 units		
PoE Ability PD @ 15.4 watts	14 units	24 units	
PoE Ability PD @ 30 watts	7 units	14 units	
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 Voice VLAN Protocol VLAN Private VLAN (Protected port) GVRP
Link Aggregation	IEEE 802.3ad LACP and static trunk Supports 8 groups, 8 ports per trunk group
Spanning Tree Protocol	STP, RSTP, MSTP
IGMP Snooping	IGMP (v2/v3) snooping IGMP querier Up to 256 multicast groups
MLD Snooping	MLD (v1/v2) snooping, up to 256 multicast groups
Access Control List	IPv4/IPv6 IP-based ACL/MAC-based ACL
QoS	8 mapping ID to 8 level priority queues <ul style="list-style-type: none"> - Port number - 802.1p priority - 802.1Q VLAN tag - DSCP field in IP packet Traffic classification based, strict priority and WRR
Security	IEEE 802.1X – port-based authentication Built-in RADIUS client to cooperate with RADIUS server RADIUS/TACACS+ user access authentication IP-MAC port binding MAC filter Static MAC address DHCP snooping and DHCP option82 STP BPDU guard, BPDU filtering and BPDU forwarding DoS attack prevention ARP inspection IP source guard
Management Functions	
Basic Management Interfaces	Web browser; Telnet; SNMP v1, v2c Firmware upgrade by HTTP/TFTP protocol through Ethernet network Remote/Local Syslog System log LLDP protocol SNTP
Secure Management Interfaces	SSH, SSL, SNMP v3
SNMP MIBs	RFC 1213 MIB-II RFC 1215 Generic Traps RFC 1493 Bridge MIB RFC 2674 Bridge MIB Extensions RFC 2737 Entity MIB (version 2)

	RFC 2819 RMON (1, 2, 3, 9) RFC 2863 Interface Group MIB RFC 3635 Ethernet-like MIB
Standards Conformance	
Regulatory Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/100BASE-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging IEEE 802.1x Port Authentication Network Control IEEE 802.1ab LLDP IEEE 802.3af Power over Ethernet IEEE 802.3at High Power over Ethernet 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: -20 ~ 70 degrees C Relative Humidity: 5 ~ 95% (non-condensing)

GS-4210-48T4S

Product	GS-4210-48T4S	GS-4210-48P4S
Hardware Specifications		
Copper Ports	48 x 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports	
SFP/mini-GBIC Slots	4 100/1000BASE-X SFP interfaces, Supports 100/1000Mbps dual mode and DDM	
PoE Injector Port	---	48 ports with 802.3at/af PoE injector function with port-1 to port-48
Switch Architecture	Store-and-Forward	
Switch Fabric	104Gbps/non-blocking	
Switch Throughput@64Bytes	77.38Mpps @64Bytes	
Address Table	16K entries	
Shared Data Buffer	12Mbit SRAM packet buffer	
Flow Control	IEEE 802.3x pause frame for full-duplex Back pressure for half-duplex	
Jumbo Frame	10K bytes	
Reset Button	< 5 sec: System reboot > 5 sec: Factory default	
LED	System: PWR(Power) (Green) SYS(System) (Green) 10/100/1000T RJ45 Interfaces (Port 1 to Port 48): 1000Mbps (Orange), LNK/ACT (Green) 10/100Mbps (None), LNK/ACT (Green) 100/1000Mbps SFP Interfaces (Port 49 to Port 52): 1000Mbps, LNK/ACT (Green) 100Mbps, LNK/ACT (Orange)	System: PWR (Power) (Green) SYS (System) (Green) 10/100/1000T RJ45 Interfaces (Port 1 to Port 48): 10/100/1000Mbps, LNK/ACT (Green) PoE-in-Use (Orange) 100/1000Mbps SFP Interfaces (Port 49 to Port 52): 1000Mbps, LNK/ACT (Green) 100Mbps, LNK/ACT (Orange)
Thermal Fan	Fanless design (no fan)	3 x smart fan
Power Requirements	AC 100~240V, 50/60Hz, auto-sensing.	100~240V AC, 50/60Hz, auto-sensing
ESD Protection	6KV DC	6KV DC
Power Consumption/Dissipation	34 watts/116 BTU	481 watts (max.)/1641 BTU
Dimensions (W x D x H)	440 x 300 x 44.5 mm, 1U height	440 x 300 x 44.5 mm, 1U height
Weight	3.7 kg	5.476 kg
Enclosure	Metal	Metal
Power over Ethernet		
PoE Standard	---	IEEE 802.3af/802.3at PoE+ PSE
PoE Power Supply Type	---	End-span

PoE Power Output	---	Per port 52V DC, 36 watts (max.)
Power Pin Assignment	---	1/2(+), 3/6(-)
PoE Power Budget	---	440 watts (max.) @ 25 degrees C 380 watts (max.) @ 50 degrees C
PoE Ability PD @ 9 watts	---	48 units
PoE Ability PD @ 15 watts	---	29 units
PoE Ability PD @ 30 watts	---	14 units
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 Protocol VLAN Private VLAN (Protected port) GVRP Management VLAN	
Link Aggregation	IEEE 802.3ad LACP and static trunk Supports 8 groups, 8 ports per trunk group	
Spanning Tree Protocol	IEEE 802.1D Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) STP BPDU guard, BPDU filtering and BPDU forwarding	
IGMP Snooping	IGMP (v2/v3) snooping IGMP querier Up to 256 multicast groups	
MLD Snooping	IPv6 MLD (v1/v2) snooping, up to 256 multicast groups	
Access Control List	IPv4/IPv6 IP-based ACL/MAC-based ACL IPv4/IPv6 IP-based ACE/MAC-based ACE	
QoS	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	
Security	IEEE 802.1X port-based authentication Built-in RADIUS client to cooperate 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
Management Functions	
Basic Management Interfaces	Web browser; Telnet; SNMP v1, v2c, v3 Firmware upgrade by HTTP/ FTP protocol through Ethernet network Configuration upload/download through HTTP/TFTP Remote/Local Syslog System log LLDP protocol SNTP PLANET Smart Discovery Utility
Secure Management Interfaces	SSH, SSL, 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	
Regulatory Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/100BASE-FX IEEE 802.3z 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: -20 ~ 70 degrees C Relative Humidity: 5 ~ 95% (non-condensing)

2. INSTALLATION

This section describes the hardware features and installation of the Managed Switch on the desktop or rack mount. For easier management and control of the Managed Switch, familiarize yourself with its display indicators and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the Managed Switch, please read this chapter completely.

2.1 Hardware Description

2.1.1 Switch Front Panel

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

GS-4210-8P2S Front Panel

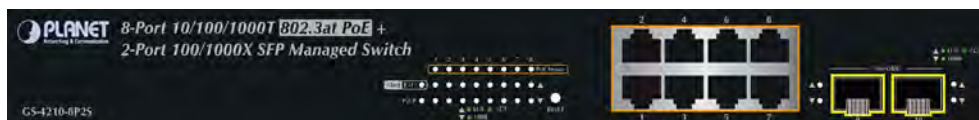


Figure 2-1-1a GS-4210-8P2S Front Panel

GS-4210-8P2T2S Front Panel



Figure 2-1-1b GS-4210-8P2T2S Front Panel

GS-4210-16P4C Front Panel



Figure 2-1-1c GS-4210-16P4C Front Panel

GS-4210-24P4C Front Panel

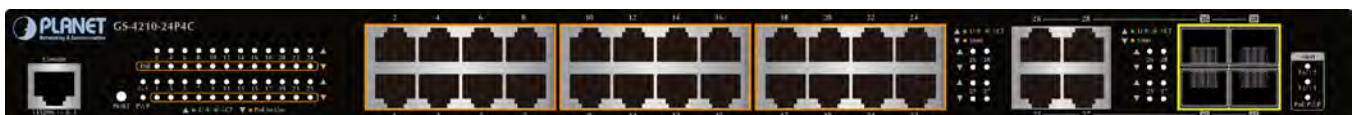


Figure 2-1-1d GS-4210-24P4C Front Panel

GS-4210-24PL4C Front Panel



Figure 2-1-1e GS-4210-24PL4C Front Panel

GS-4210-48T4S Front Panel



Figure 2-1-1f GS-4210-48T4S Front Panel

GS-4210-48P4S Front Panel

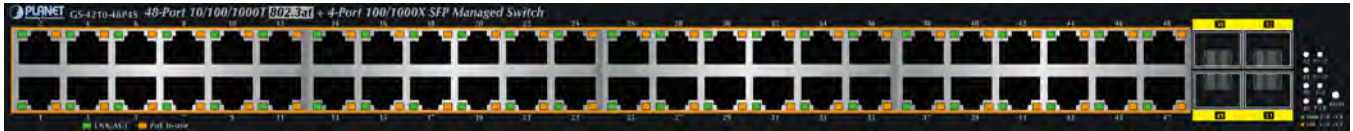


Figure 2-1-1g GS-4210-48P4S Front Panel

■ Gigabit TP Interface

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

■ 100/1000BASE-X SFP Slots

Each of the SFP (small form-factor pluggable) slots supports dual-speed, 1000BASE-SX/LX or 100BASE-FX

- For 1000BASE-SX/LX SFP transceiver module: From 550 meters (multi-mode fiber) to 10/30/50/70/120 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 an 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

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

Reset Button Pressed and Released	Function
< 5 sec: System Reboot	Reboot the Managed Switch.
> 5 sec: Factory Default	<p>Reset the Managed Switch to Factory Default configuration. The Managed Switch will then reboot and load the default settings shown below:</p> <ul style="list-style-type: none"> ◦ Default username: admin ◦ Default password: admin ◦ Default IP address: 192.168.0.100 ◦ Subnet mask: 255.255.255.0 ◦ Default gateway: 192.168.0.254

2.1.2 LED Indications

The front panel LEDs indicate instant status of port links, data activity and system power; it helps monitor and troubleshoot when needed. Figures 2-1-2a to 2-1-2f show the LED indications of these Managed Switches.

GS-4210-8P2S LED Indication

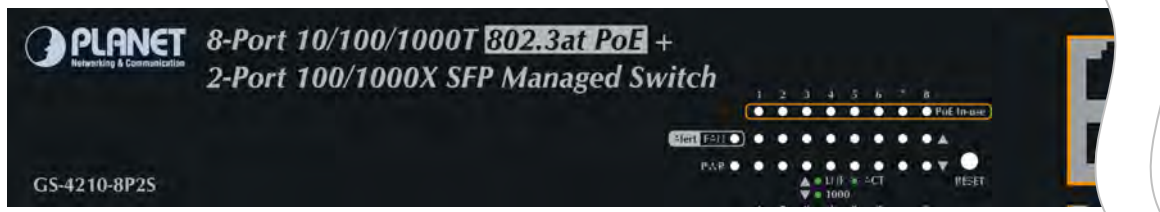


Figure 2-1-2a GS-4210-8P2S LED Panel

■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
FAN	Orange	Lights to indicate that the Fan is down.

■ 10/100/1000BASE-T interfaces

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

■ 100/1000BASE-X SFP interfaces

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

GS-4210-8P2T2S LED Indication



Figure 2-1-2b GS-4210-8P2T2S LED Panel

System

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

10/100/1000BASE-T interfaces

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

100/1000BASE-X SFP interfaces

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

GS-4210-16P4C LED Indication



Figure 2-1-2c GS-4210-16P4C LED Panel

System Alert

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
SYS	Green	Lights to indicate the system is working. Off to indicate the system is booting.
FAN 1	Red	Lights to indicate that FAN1 is down.
FAN 2	Red	Lights to indicate that FAN2 is down.
PoE PWR	Red	Lights to indicate that the PoE power is down.

10/100/1000BASE-T interfaces (Port-1 to Port-16)

LED	Color	Function
LNK/ACT	Green	Lights: To indicate the link through that port is successfully established. Blinks: To indicate that the switch is actively sending or receiving data over that port.
PoE	Orange	Lights: To indicate the port is providing 56V DC in-line power. Off: To indicate the connected device is not a PoE Powered Device (PD).

10/100/1000BASE-T interfaces (Port-17 to Port-20)

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

100/1000BASE-SX/LX SFP interfaces (Port-17 to Port-20)

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

GS-4210-24P (L) 4C LED Indication



Figure 2-1-2d GS-4210-24P (L) 4C LED Panel

System / Alert

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
SYS	Green	Lights to indicate the system is working. Off to indicate the system is booting.
FAN 1	Red	Lights to indicate that FAN1 is down.
FAN 2	Red	Lights to indicate that FAN2 is down.
PoE PWR	Red	Lights to indicate that the PoE power is down.

10/100/1000BASE-T interfaces (Port-1 to Port-24)

LED	Color	Function
LNK/ACT	Green	Lights: To indicate the link through that port is successfully established. Blinks: To indicate that the switch is actively sending or receiving data over that port.
PoE	Orange	Lights: To indicate the port is providing 56V DC in-line power. Off: To indicate the connected device is not a PoE powered device (PD).

10/100/1000BASE-T interfaces (Port-25 to Port-28)

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

100/1000BASE-SX/LX SFP interfaces (Port-25 to Port-28)

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

GS-4210-48T4S LED Indication



Figure 2-1-2e GS-4210-48T4S LED Panel

System

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

Per 10/100/1000Mbps RJ45 interfaces (Port-1 to Port-48)

LED	Color	Function
Speed	Orange	Indicates the link through that port is successfully established at 1000Mbps.
	None	Indicates the link through that port is successfully established at 10/100Mbps.
LNK/ACT	Green	Blinks: Indicates that the Switch is actively sending or receiving data over that port.

Per 100/1000Mbps SFP Interface (Port-49 to Port-52)

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

GS-4210-48P4S LED Indication

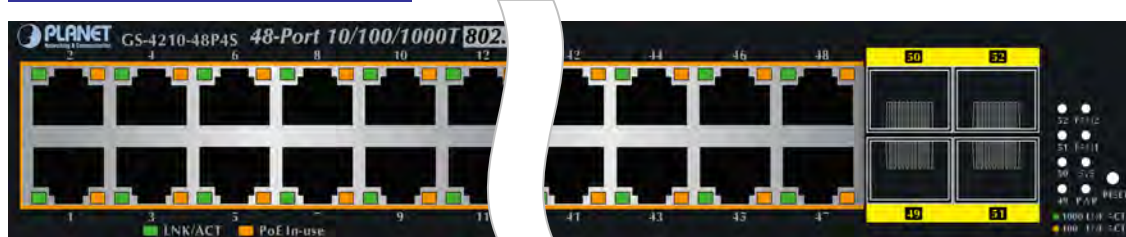


Figure 2-1-2f GS-4210-48P4S LED Panel

System

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

■ Per 10/100/1000Mbps RJ45 interfaces (Port-1 to Port-48)

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

■ Per 100/1000Mbps SFP Interface (Port-49 to Port-52)

LED	Color	Function	
LNK/ACT	Green	Lights:	Indicates the link through that port is successfully established at 1000Mbps.
		Blinks:	Indicates that the Switch is actively sending or receiving data over that port.
	Orange	Lights:	Indicates the link through that port is successfully established at 100Mbps.
		Blinks:	Indicates 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. [Figures 2-1-3a to 2-1-3g](#) show the rear panels of these Managed Switches

GS-4210-8P2S Rear Panel



Figure 2-1-3a Rear Panel of GS-4210-8P2S

GS-4210-8P2T2S Rear Panel



Figure 2-1-3b Rear Panel of GS-4210-8P2T2S

GS-4210-16P4C Rear Panel



Figure 2-1-3c Rear Panel of GS-4210-16P4C

GS-4210-24P4C Rear Panel



Figure 2-1-3d Rear Panel of GS-4210-24P4C

GS-4210-24PL4C Rear Panel



Figure 2-1-3e Rear Panel of GS-4210-24PL4C

GS-4210-48T4S Rear Panel

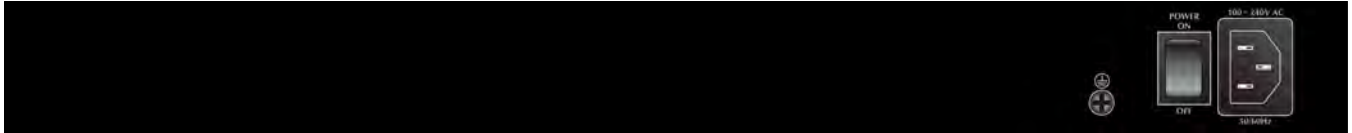


Figure 2-1-3f Rear Panel of GS-4210-48T4S

GS-4210-48P4S Rear Panel



Figure 2-1-3g Rear Panel of GS-4210-48P4S

■ AC Power Receptacle

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

Plug the female end of the power cord firmly into the 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.

The device is a power-required device, which means it will not work till it is powered. If your networks

Power Notice: 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.

2.2 Installing the Switch

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

2.2.1 Desktop Installation

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

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

Step 2: Place the Managed Switch on the desktop or the shelf near an AC power source, as shown in Figure 2-1-4.

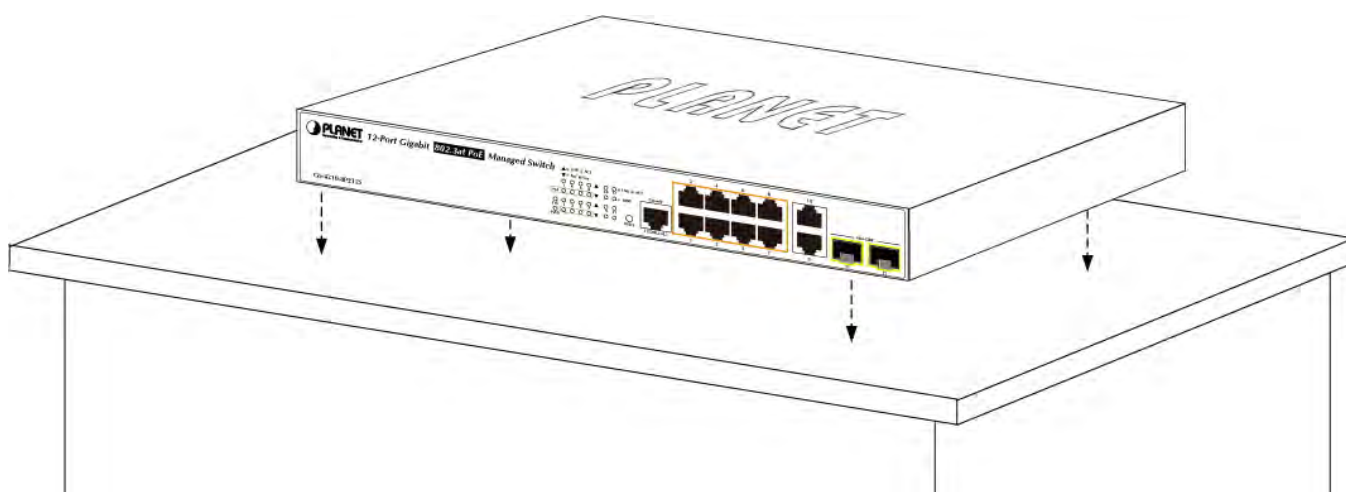
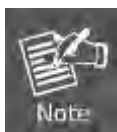


Figure 2-1-4 Place the Managed Switch on the desktop

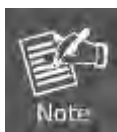
Step 3: Keep enough ventilation space between the Managed Switch and the surrounding objects.



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

Step 4: Connect the Managed Switch to network devices.

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



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

Step 5: Supply power to the Managed Switch.

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

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

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

2.2.2 Rack Mounting

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

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

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

Figure 2-1-5 shows how to attach brackets to one side of the Managed Switch.

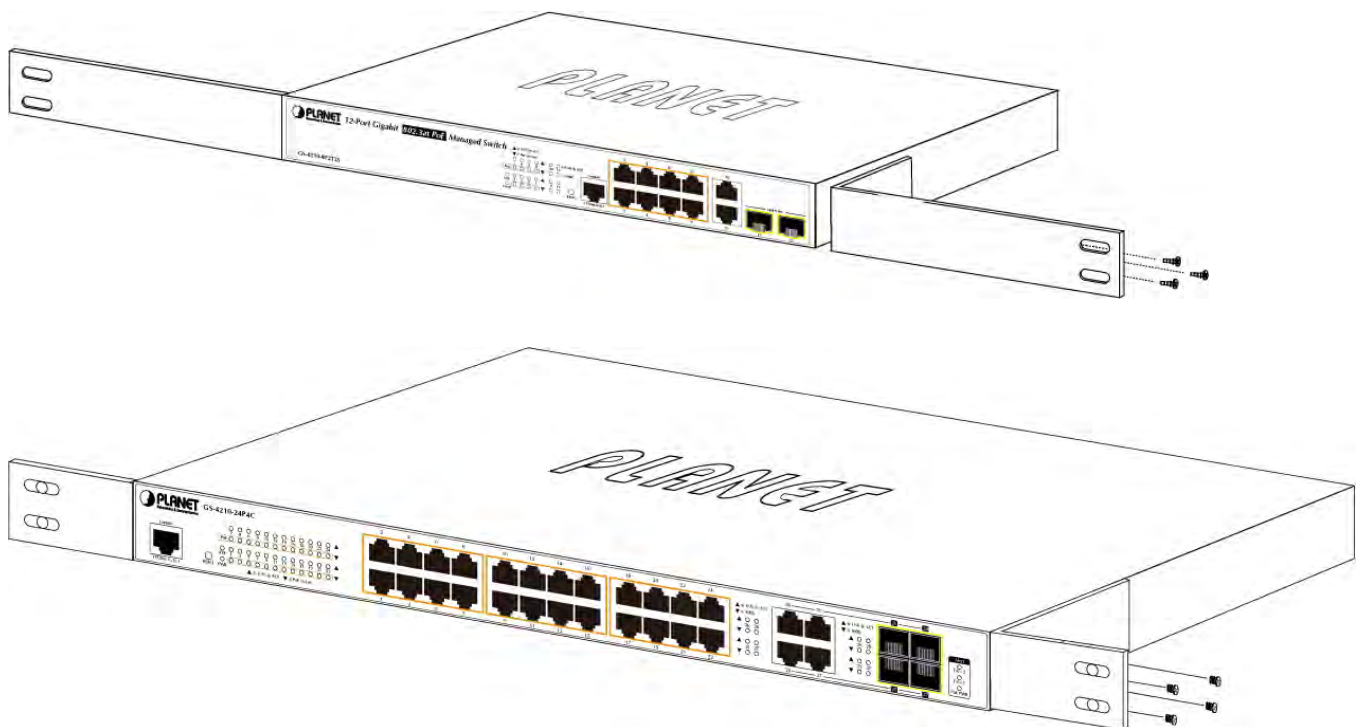


Figure 2-1-5 Attach Brackets to the Managed Switch.



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

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 2-1-6.

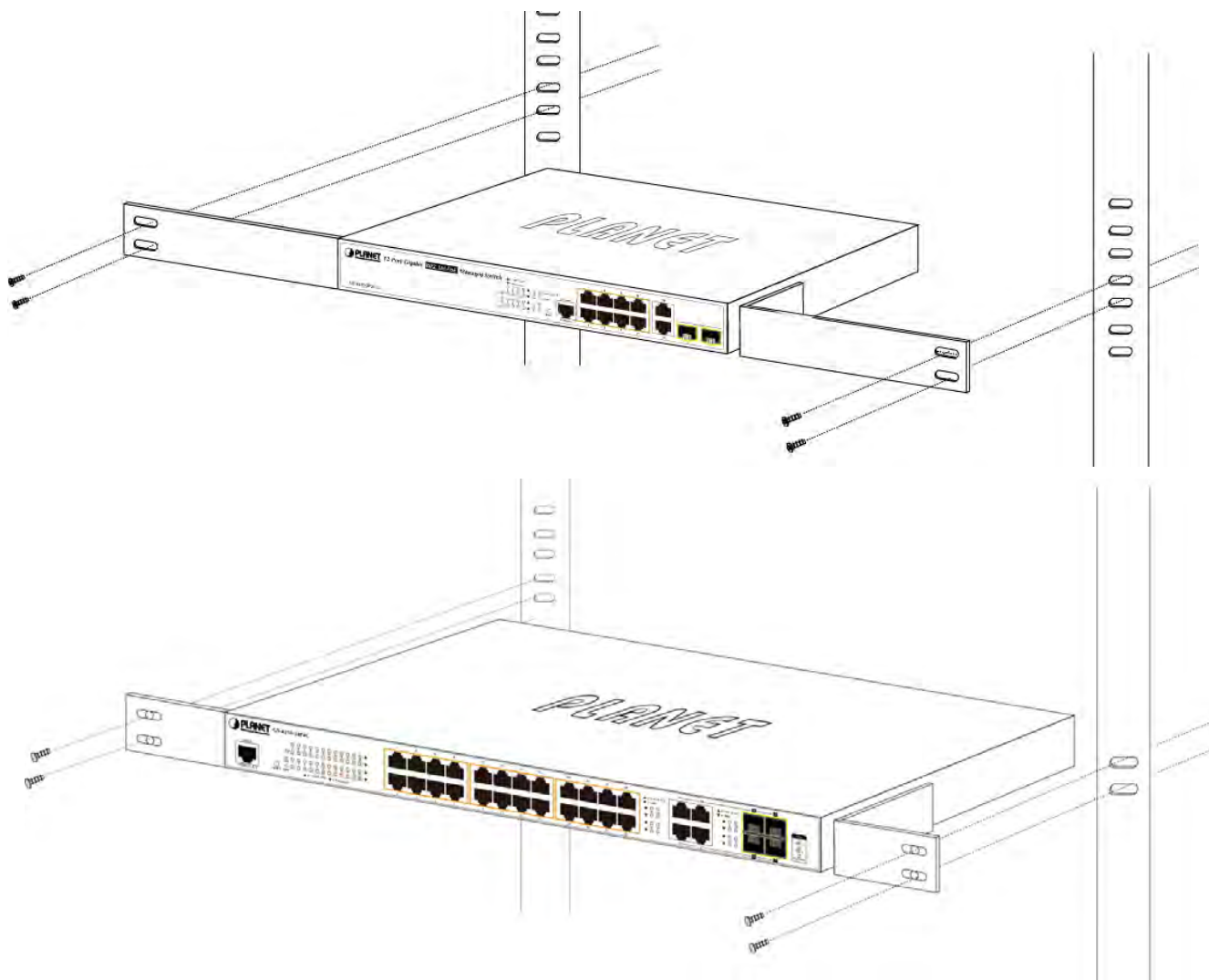


Figure 2-1-6 Mounting Managed Switch in a Rack

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 2-1-7](#) shows.



Figure 2-1-7 Plug in the SFP transceiver

■ Approved PLANET SFP Transceivers

PLANET Managed Switch supports both single mode and multi-mode SFP transceivers. 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
- **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-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-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



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.



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

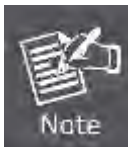
1. Before we connect Managed Switch to the other network device, we have to make sure both sides of the SFP transceivers are with the same media type; for example, 1000BASE-SX to 1000BASE-SX, 1000BASE-LX to 1000BASE-LX.
 2. Check whether the fiber-optic cable type matches with the SFP transceiver requirement.
 - To connect to 1000BASE-SX SFP transceiver, please use the multi-mode fiber cable with one side being the male duplex LC connector type.
 - To connect to 1000BASE-LX SFP transceiver, please use the single-mode fiber cable with one side being the male duplex LC connector type.
-
- **Connect 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**”.

- **Remove the Transceiver Module**

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



Figure 2-1-8 How to Pull Out the SFP Transceiver



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

3. SWITCH MANAGEMENT

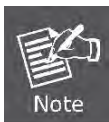
This chapter explains the methods that you can use to configure management access to the Managed Switch. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. 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 comes 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 Explorer 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 interfaces are embedded in the Managed Switch software and are available for immediate use. Each of these management methods has their own advantages. Table 3-1 compares the three management methods.

Method	Advantages	Disadvantages
Console	<ul style="list-style-type: none"> No IP address or subnet needed Text-based Telnet functionality and HyperTerminal built into Windows 95/98/NT/2000/ME/XP operating systems Secure 	<ul style="list-style-type: none"> Must be near the switch or use dial-up connection Not convenient for remote users Modem connection may prove to be unreliable or slow
Web Browser	<ul style="list-style-type: none"> Ideal for configuring the switch remotely Compatible with all popular browsers Can be accessed from any location Most visually appealing 	<ul style="list-style-type: none"> Security can be compromised (hackers need to 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 to 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. By 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.

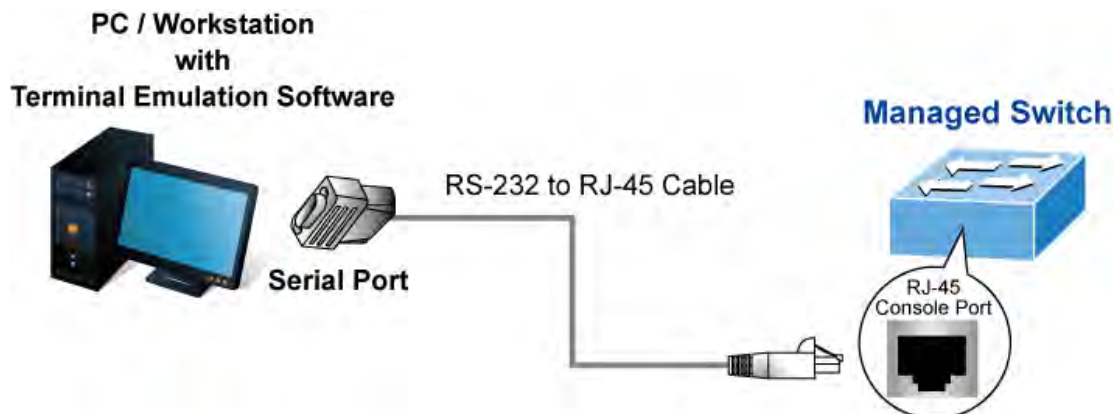


Figure 3-1-1: Console Management

Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as **HyperTerminal**) to the Managed Switch console (serial) port. When using this management method, a **straight 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:

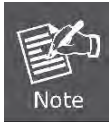
The default parameters are:

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



Figure 3-1-2: Terminal Parameter Settings

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



Console interface is not available for the GS-4210-8P2S, GS-4210-48T4S and GS-4210-48P4S.

3.4 Web Management

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

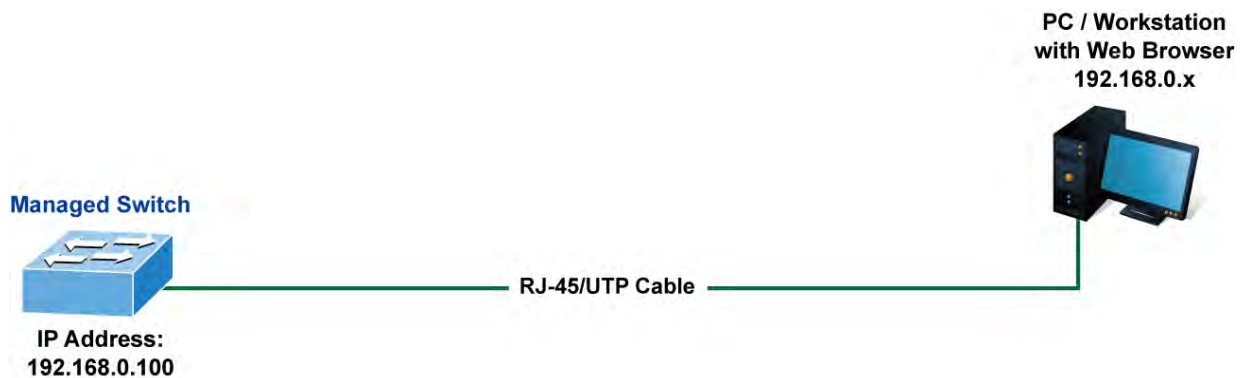


Figure 3-1-3 Web Management

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



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

3.5 SNMP-based Network Management

You can use an external SNMP-based application to configure and manage the Managed Switch, such as 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.

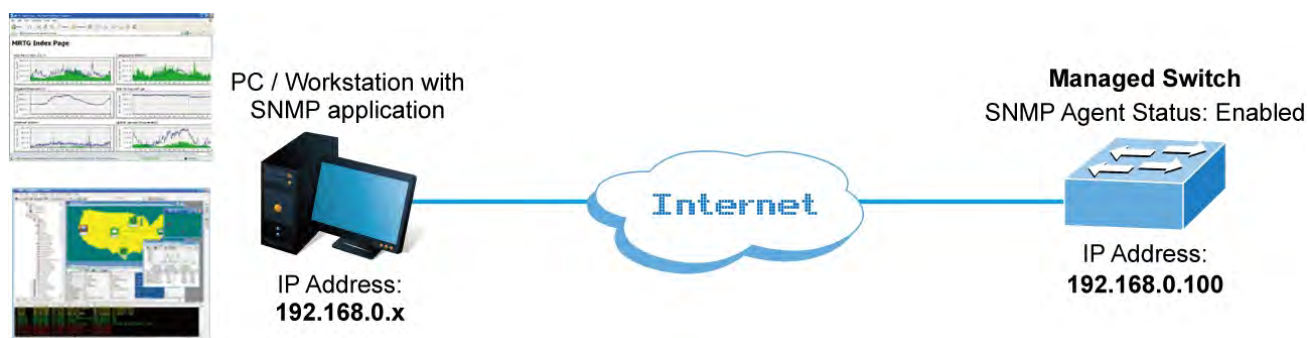


Figure 3-1-5 SNMP Management

3.6 PLANET Smart Discovery Utility

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

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

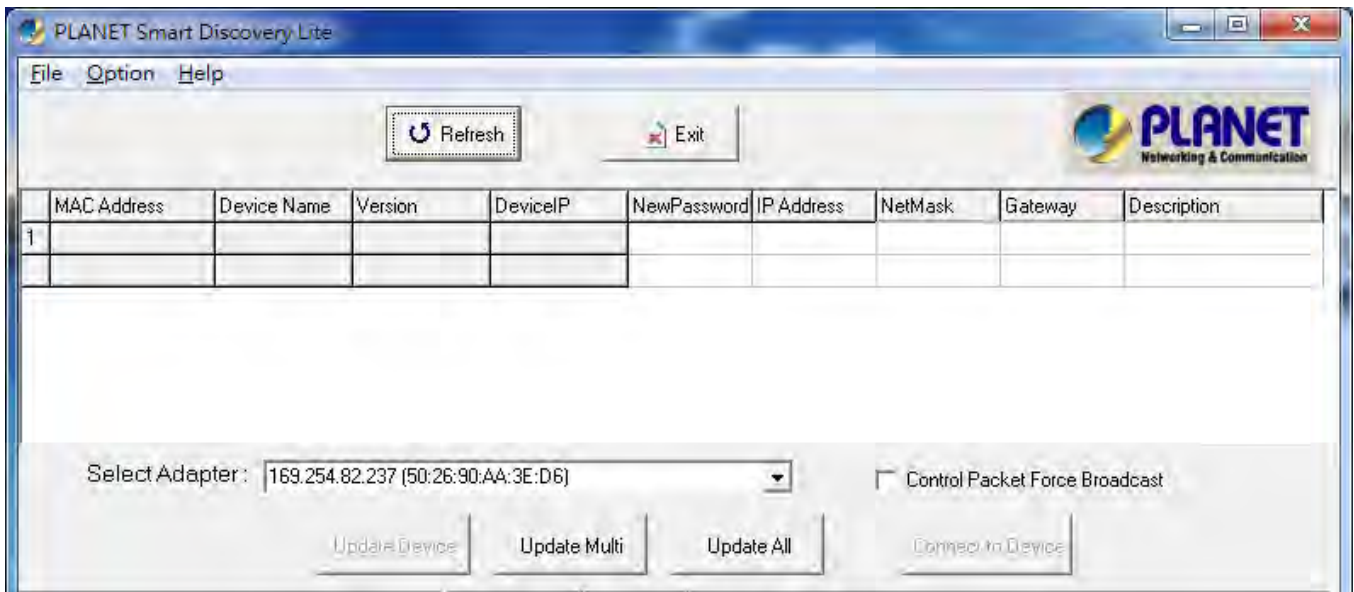
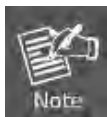


Figure 3-1-6: Planet Smart Discovery Utility Screen



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

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

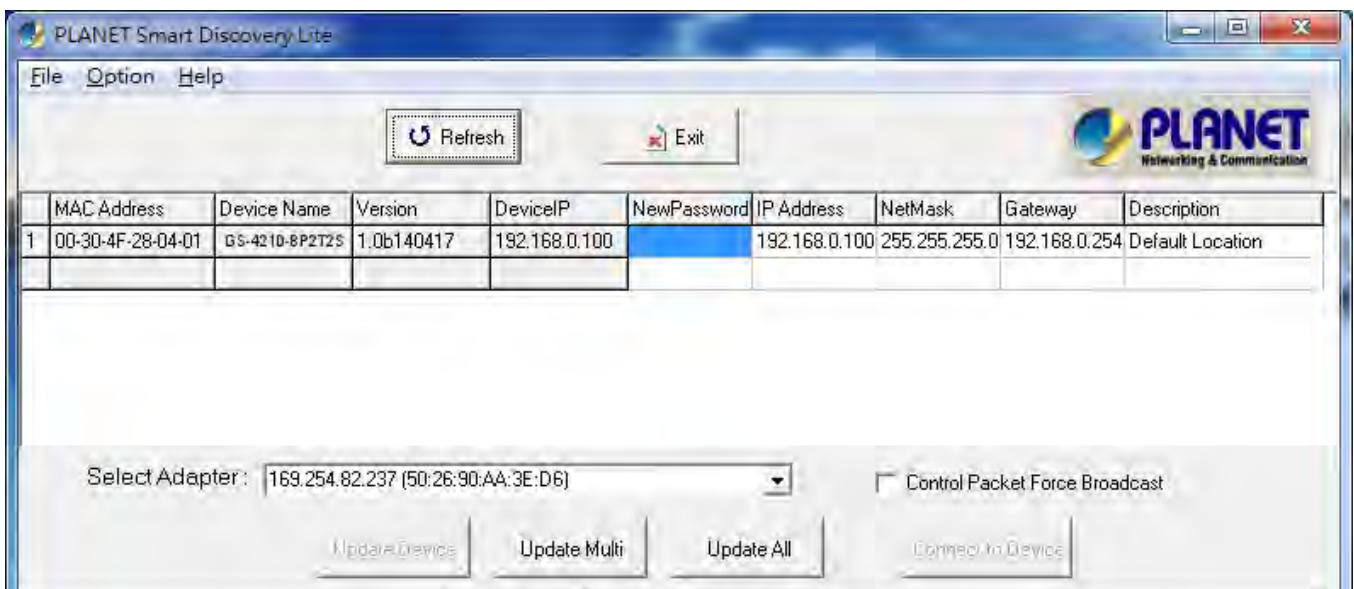


Figure 3-1-7: Planet Smart Discovery Utility Screen

1. This utility shows all necessary information from the devices, such as MAC address, device name, firmware version and device IP subnet address. It can also assign new password, IP subnet address and description to the devices.

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

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

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

3. To click the **“Control Packet Force Broadcast”** function, it allows you to assign a new setting value to the Web Smart Switch under a different IP subnet address.
4. Press the **“Connect to Device”** button and the Web login screen appears in [Figure 3-1-4](#).
5. Press the **“Exit”** button to shut down the Planet Smart Discovery Utility.

4. WEB CONFIGURATION

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

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 to 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 to **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 to 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on manager PC.

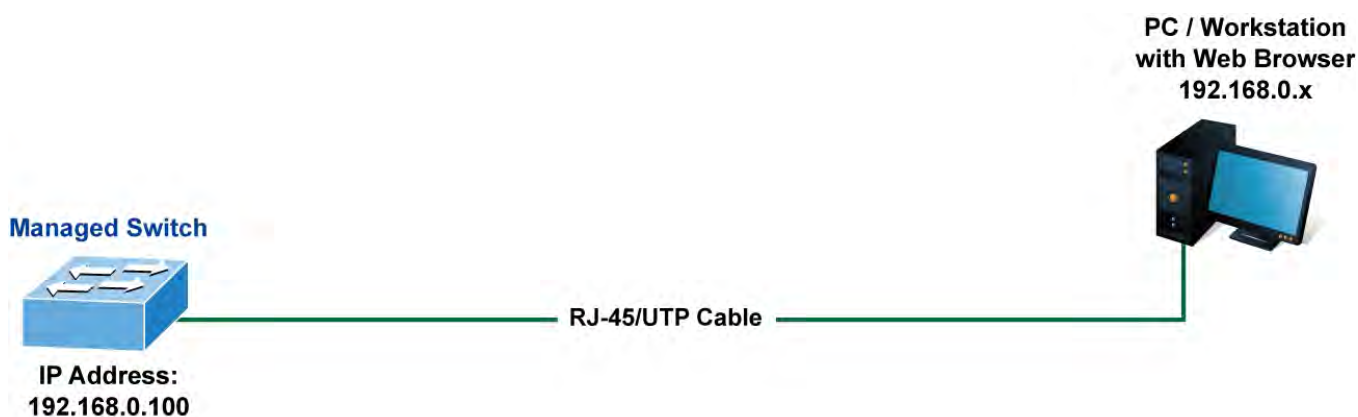


Figure 4-1-1 Web Management

■ Logging on the switch

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

http://192.168.0.100

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

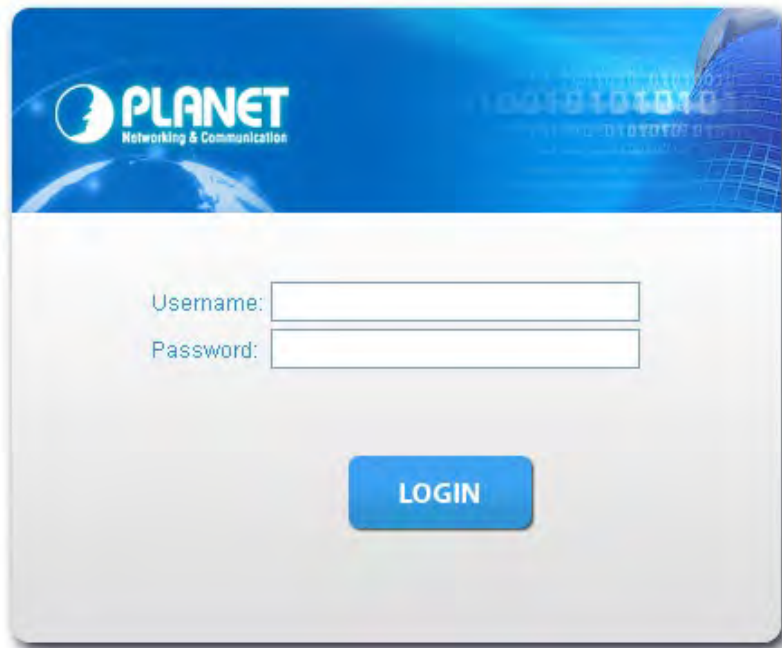


Figure 4-1-2 Login screen

Default User Name: **admin**

Default Password: **admin**

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



Figure 4-1-3 Default Main Page

Now, you can use the Web management interface to continue the switch management or manage the Managed Switch by Web interface. The Switch Menu on the left of the web page lets 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 **Save** 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.

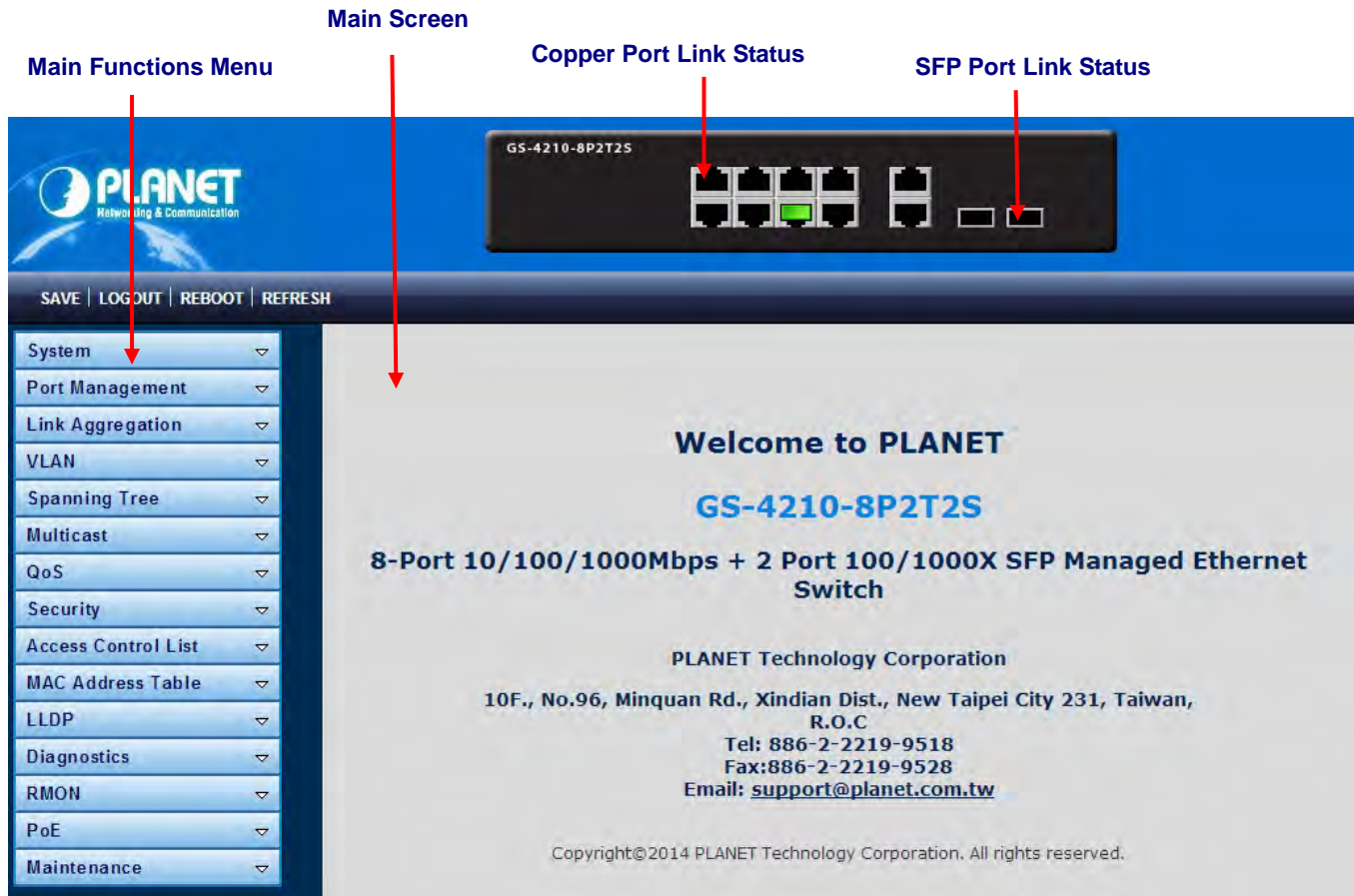








Figure 4-1-4 Main Page

Panel Display

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

The port states are illustrated as follows:

State	Disabled	Down	Link
RJ45 Ports			
SFP Ports			

Main Menu

By 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.

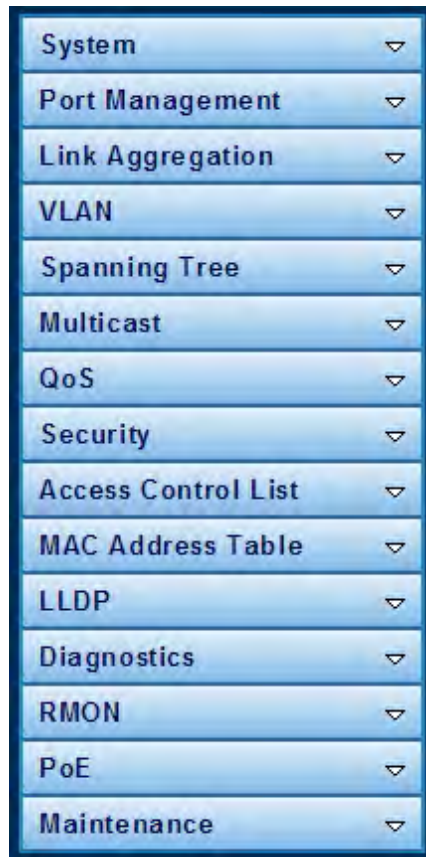


Figure 4-1-5 Managed Switch Main Functions Menu

Buttons



: Click to save changes or reset to default.



: Click to logout the Managed Switch.



: Click to reboot the Managed Switch.



: Click to refresh the page.

4.1.1 Save Button

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

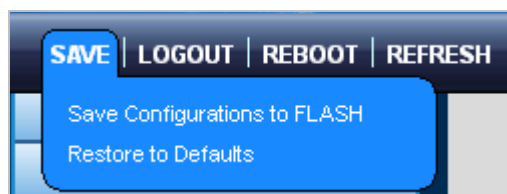


Figure 4-1-6 Save Button Screenshot

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 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 chapter 4.15.1

4.1.2 Configuration Manager

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

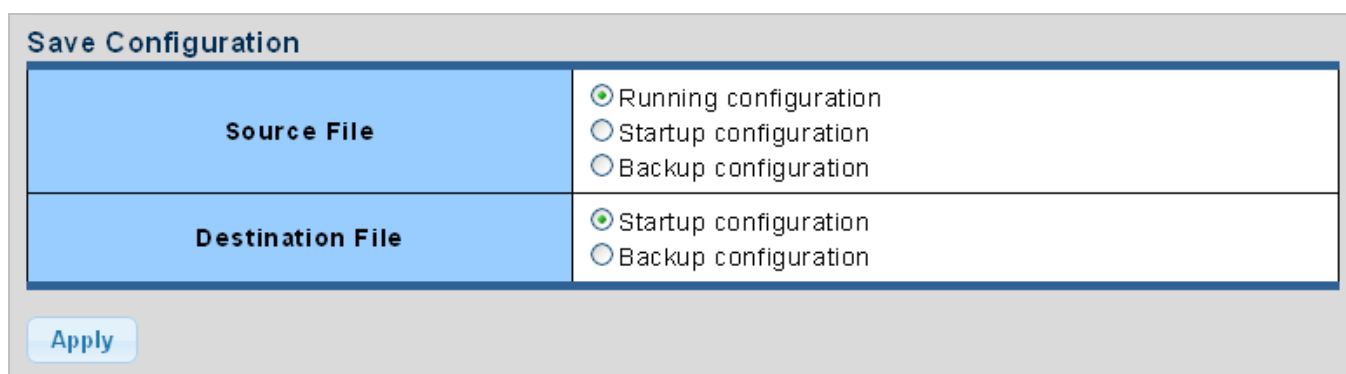



Figure 4-1-7 Save Button Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Running Configuration 	<p>Refers to the running configuration sequence use in the switch.</p> <p>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 startup configuration file, which is called configuration save.</p> <p>To prevent illicit file upload and easier configuration, switch mandates the name of running configuration file to be running-config.</p>
<ul style="list-style-type: none"> • Startup Configuration 	<p>Refers to the configuration sequence used in switch startup.</p> <p>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.</p> <p>If the device does not support multi-config file, mandates the name of startup</p>

	configuration file to be startup-config.
• Backup Configuration	The backup configuration is empty in FLASH; please save the backup configuration first by " Maintenance > Backup Manager ".

Buttons

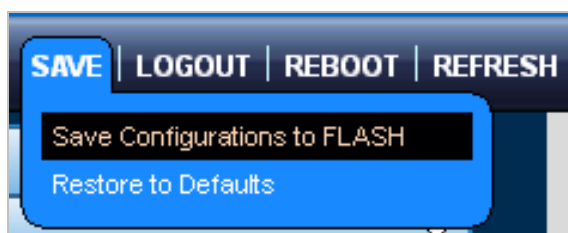
: Click to save configuration.

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".

Save Configuration

Source File	<input checked="" type="radio"/> Running configuration <input type="radio"/> Startup configuration <input type="radio"/> Backup 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 start up configuration.

4.2 System

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

- **System Information** The switch system information is provided here.
- **IP Configurations** 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 screens in [Figure 4-2-1](#) and [Figure 4-2-2](#) appear.

System Information	
Information Name	Information Value
System Name	Edit GS-4210-8P2T2S
System Location	Edit Default Location
System Contact	Edit Default Contact
MAC Address	00:30:4F:00:00:00
IP Address	192.168.0.100
Subnet Mask	255.255.255.0
Gateway	192.168.0.254
Loader Version	2011.12.46351
Loader Date	Apr 16 2014 - 14:51:06
Firmware Version	1.0b140417
Firmware Date	Wed May 7 15:41:06 UZT 2014
System Object ID	1.3.6.1.4.1.10456.1.1509
System Up Time	0 days, 2 hours, 6 mins, 32 secs
PCB/HW Version	V1


Figure 4-2-1 System Information Screenshot

The page includes the following fields:

Object	Description
• System Name	Display the current system name

• System Location	Display the current system location
• System Contact	Display the current system contact
• MAC Address	The MAC address of this Managed Switch.
• IP Address	The IP address of this Managed Switch.
• Subnet Mask	The subnet mask of this Managed Switch.
• Gateway	The gateway of this Managed Switch.
• Loader Version	The loader version of this Managed Switch.
• Loader Date	The loader date of this Managed Switch.
• Firmware Version	The firmware version of this Managed Switch.
• Firmware Date	The firmware date of this 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.
• PCN/HW Version	The hardware version of this Managed Switch.

Buttons

: Click to edit parameter.

4.2.2 IP Configurations

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

IP Address Setting

Mode	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.254"/>
DNS Server 1	<input type="text" value="168.95.1.1"/>
DNS Server 2	<input type="text" value="168.95.192.1"/>




Figure 4-2-2 IP Address Setting Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Mode 	<p>Indicates the IP address mode operation. Possible modes are:</p> <p>Static: Enable NTP mode operation.</p> <p>When enabling NTP mode operation, the agent forwards and transfers NTP messages between the clients and the server when they are not on the same subnet domain.</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>
<ul style="list-style-type: none"> IP Address 	Provide the IP address of this switch in dotted decimal notation.
<ul style="list-style-type: none"> Subnet Mask 	Provide the subnet mask of this switch in dotted decimal notation.
<ul style="list-style-type: none"> Gateway 	Provide the IP address of the router in dotted decimal notation.
<ul style="list-style-type: none"> DNS Server 1/2 	Provide the IP address of the DNS Server in dotted decimal notation.

Buttons

: Click to apply changes.

IP Information	
Information Name	Information Value
DHCP State	Disabled
Static IP Address	192.168.1.1
Static Subnet Mask	255.255.255.0
Static Gateway	192.168.1.254
Static DNS Server 1	168.95.1.1
Static DNS Server 2	168.95.192.1

Figure 4-2-3 IP Information Screenshot

The page includes the following fields:

Object	Description
• DHCP State	Display the current DHCP state.
• IP Address	Display the current IP address.
• Subnet Mask	Display the current subnet mask.
• Gateway	Display the current gateway.
• DNS Server 1/2	Display the current DNS server.

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.

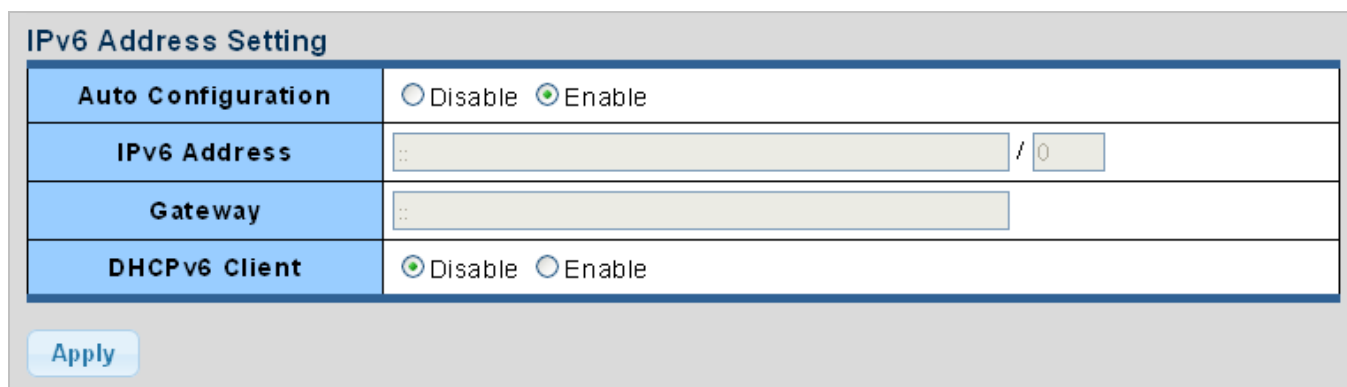


Figure 4-2-4 IPv6 Address Setting Screenshot

The page includes the following fields:

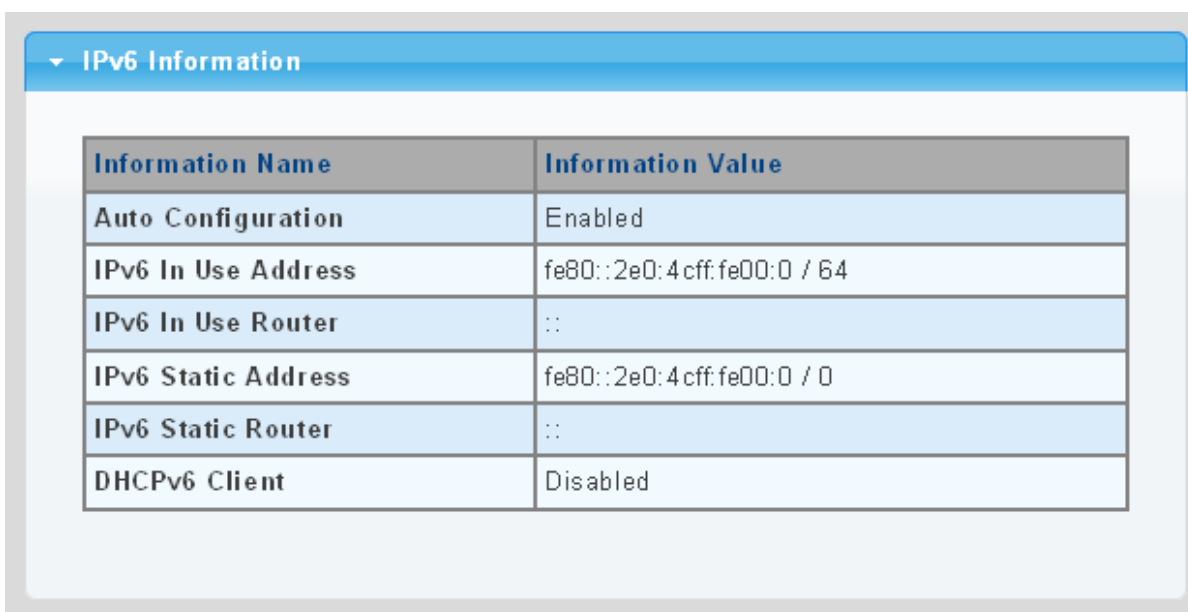
Object	Description
• Auto Configuration	<p>Enable IPv6 auto-configuration by checking this box.</p> <p>If it fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds; the total time needed to complete auto-configuration can be significantly longer.</p>
• 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</p>

	<p>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 from 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>

Buttons



: Click to apply changes.



IPv6 Information	
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

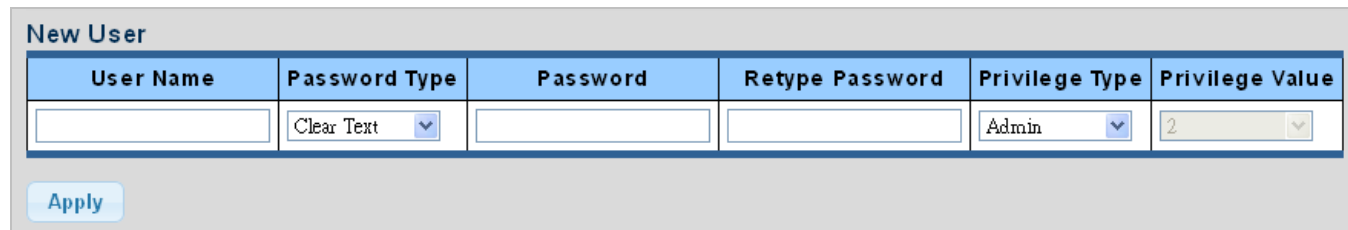
Figure 4-2-5 IPv6 Information Screenshot

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 the setup is completed, please press **"Apply"** button to take effect. Please login Web interface with a new user name and password; the screens in [Figure 4-2-6](#) and [Figure 4-2-7](#) appear.



User Name	Password Type	Password	Retype Password	Privilege Type	Privilege Value
<input type="text"/>	Clear Text ▼	<input type="text"/>	<input type="text"/>	Admin ▼	2 ▼

Apply

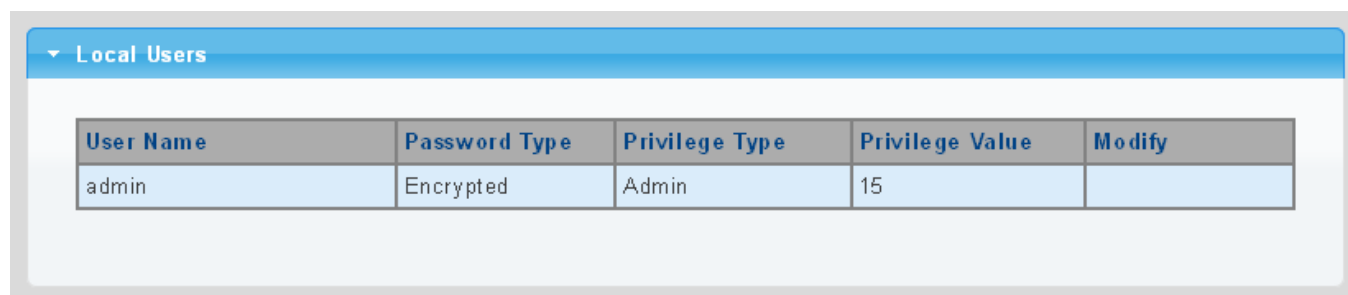
Figure 4-2-6 Local User Information Screenshot

The page includes the following fields:

Object	Description
• Username	The name identifying the user. Maximum length: 32 characters; Maximum number of users: 8
• Password Type	The password type for the user.
• Password	Enter the user's new password here. (Range: 0-32 characters plain text, case sensitive)
• Retype Password	Please enter the user's new password here again to confirm.
• Privilege Type	The privilege type for the user. Options: <ul style="list-style-type: none"> • Admin • User • Other

Buttons

: Click to apply changes.



Local Users				
User Name	Password Type	Privilege Type	Privilege Value	Modify
admin	Encrypted	Admin	15	

Figure 4-2-7 Local User Screenshot

The page includes the following fields:

Object	Description
• Username	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 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 Screenshot

The page includes the following fields:

Object	Description
• Enable SNTP	Enabled: Enable SNTP mode operation. When enabling SNTP mode operation, the agent forwards and transfers SNTP messages between the clients and the server when they are not

	<p>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>Allows to select the time zone according to the 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)</p>
<ul style="list-style-type: none"> • Recurring From 	<ul style="list-style-type: none"> • Week - Select the starting week number. • Day - Select the starting day. • Month - Select the starting month. • Hours - Select the starting hour. • Minutes - Select the starting minute.
<ul style="list-style-type: none"> • Recurring To 	<ul style="list-style-type: none"> • Week - Select the starting week number. • Day - Select the starting day. • Month - Select the starting month. • Hours - Select the starting hour. • Minutes - Select the starting minute.
<ul style="list-style-type: none"> • Non-recurring From 	<ul style="list-style-type: none"> • Week - Select the starting week number. • Day - Select the starting day. • Month - Select the starting month. • Hours - Select the starting hour. • Minutes - Select the starting minute.
<ul style="list-style-type: none"> • Non-recurring To 	<ul style="list-style-type: none"> • Week - Select the starting week number. • Day - Select the starting day. • Month - Select the starting month. • Hours - Select the starting hour. • Minutes - Select the starting minute.

Buttons

Apply: Click to apply changes.

System Time Informations	
Information Name	Information Value
Current Date/Time	09:13:10 DFL(UTC+8) Jan 01 2000
SNTP	Disabled
Time zone	UTC+8
Daylight Saving Time	Disabled
Daylight Saving Time Offset	
From	
To	

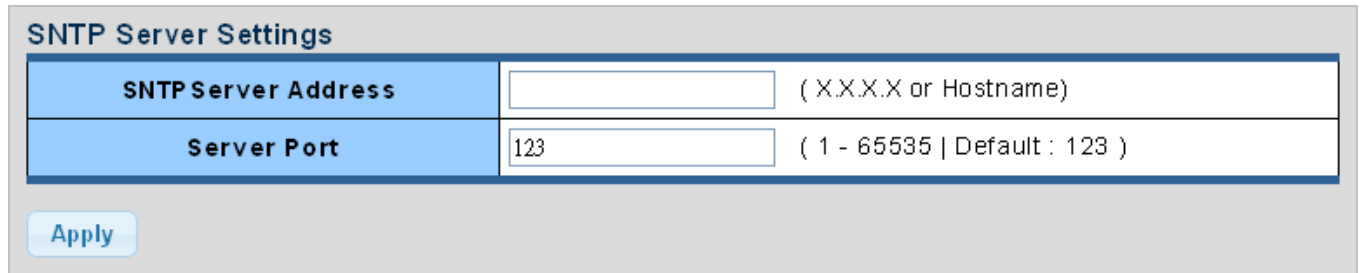
Figure 4-2-9 Time Information Screenshot

The page includes the following fields:

Object	Description
• Current Data/Time	Display the current data/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 Server Settings

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




The screenshot shows the 'SNTP Server Settings' configuration screen. It features two input fields: 'SNTP Server Address' with a placeholder '(X.X.X.X or Hostname)' and 'Server Port' with a value of '123' and a range '(1 - 65535 | Default : 123)'. An 'Apply' button is located at the bottom left.

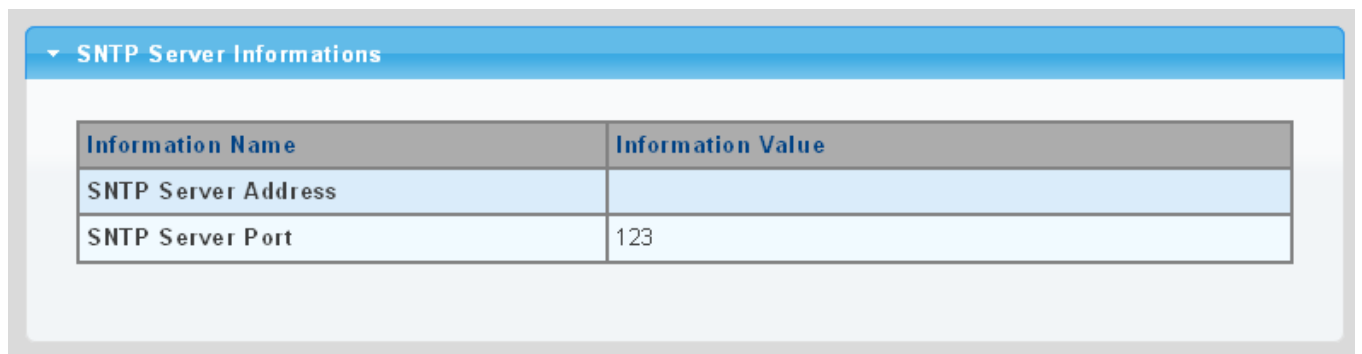
Figure 4-2-10 SNTP Setup Screenshot

The page includes the following fields:

Object	Description
• SNTP Server Address	Type the IP address or domain name of the SNTP server
• Server Port	Type the port number of the SNTP

Buttons

: Click to apply changes.



The screenshot shows the 'SNTP Server Information' screen. It displays a table with two columns: 'Information Name' and 'Information Value'. The table contains two rows: 'SNTP Server Address' and 'SNTP Server Port' with the value '123'.

Figure 4-2-11 SNTP Server Information Screenshot

The page includes the following fields:

Object	Description
• SNTP Server Address	Display the current SNTP server address
• 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 Local Log

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

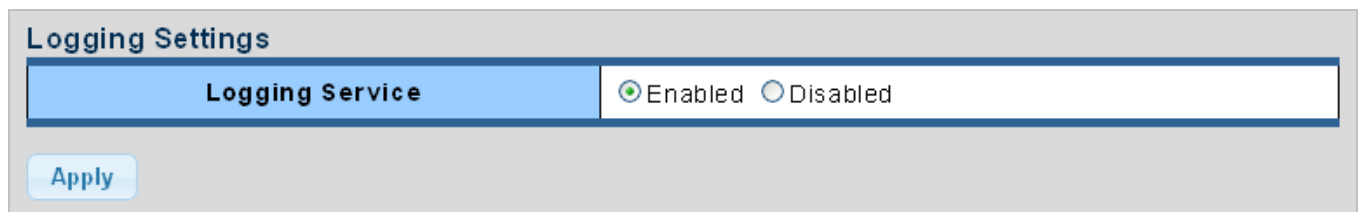


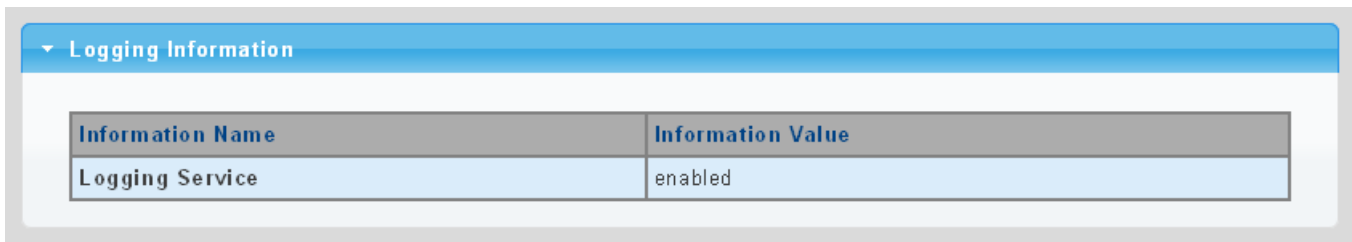
Figure 4-2-12 Logging Settings Screenshot

The page includes the following fields:

Object	Description
• Logging Service	Enabled: Enable logging service operation. Disabled: Disable logging service operation.

Buttons

: Click to apply changes.



The screenshot shows a web interface with a blue header bar containing a dropdown menu labeled 'Logging Information'. Below this is a table with two columns: 'Information Name' and 'Information Value'. The table contains one row with 'Logging Service' in the first column and 'enabled' in the second column.

Information Name	Information Value
Logging Service	enabled

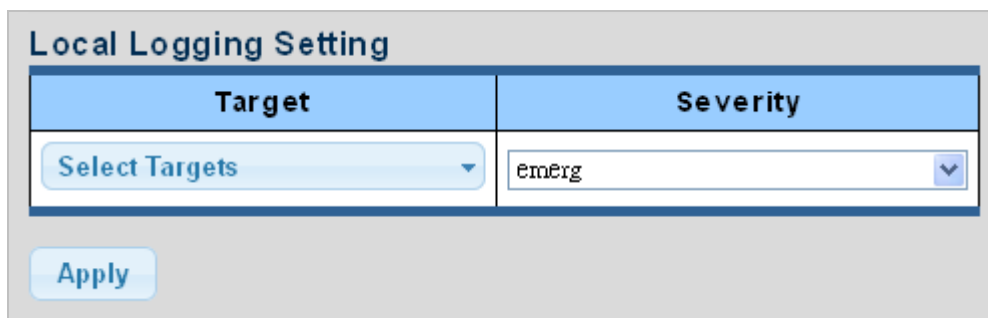
Figure 4-2-13 Logging Information Screenshot

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 Log

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



The screenshot shows a web interface titled 'Local Logging Setting'. It contains two dropdown menus: 'Target' with the text 'Select Targets' and 'Severity' with the text 'emERG'. Below these is an 'Apply' button.

Figure 4-2-14 Local Log Target Setting Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Target 	<p>The target of the local log entry. The following target types are supported:</p> <ul style="list-style-type: none"> Buffered: Target the buffer of the local log. File: Target the file of the local log.
<ul style="list-style-type: none"> Severity 	<p>The severity of the local log entry. The following severity types are supported:</p> <ul style="list-style-type: none"> emerg: Emergency level of the system unstable 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.

Buttons

Apply: Click to apply changes.

Local Logging Setting Status			
Status	Target	Severity	Action
enabled	buffered	emerg, alert, crit, error, warning, notice	Delete

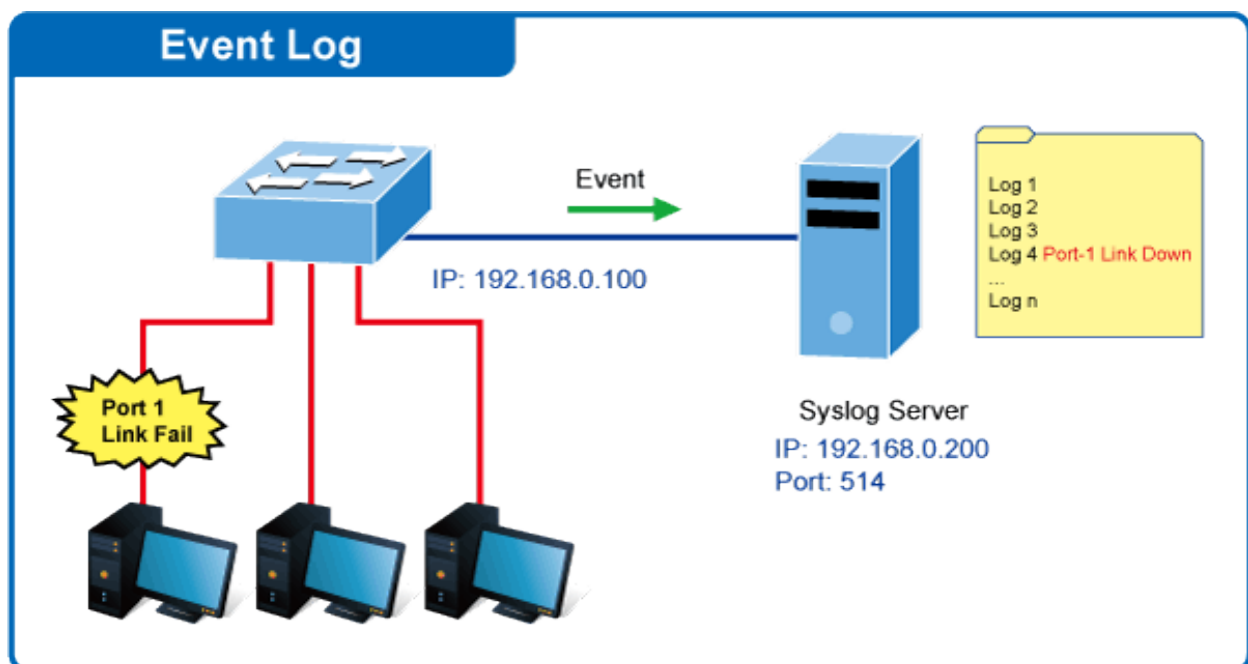
Figure 4-2-15 Local Log Setting Status Screenshot

The page includes the following fields:

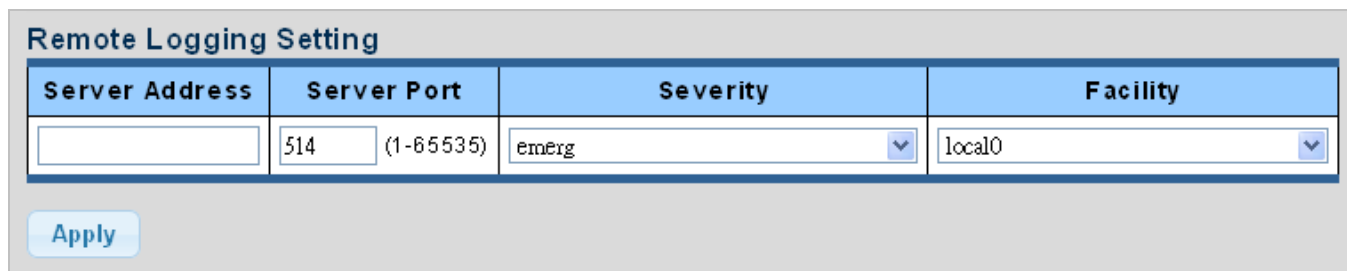
Object	Description
• Status	Display the current local log state
• Target	Display the current local log target
• Severity	Display the current local log severity
• Action	Delete : Delete the current status

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.



Remote Logging Setting

Server Address	Server Port	Severity	Facility
<input type="text"/>	<input type="text" value="514"/> (1-65535)	<input type="text" value="emerg"/>	<input type="text" value="local0"/>

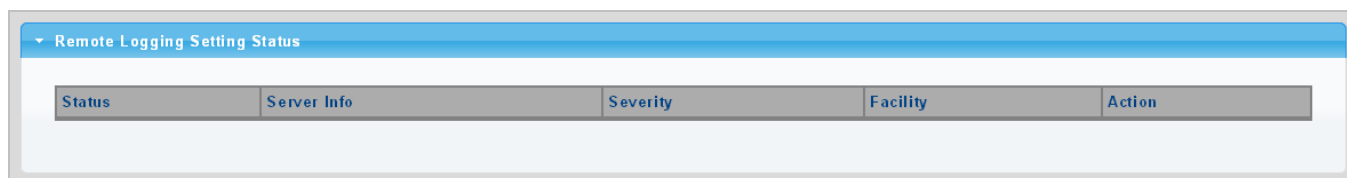
Figure 4-2-16 Remote Log Target Screenshot

The page includes the following fields:

Object	Description
• Server Address	Provide the remote syslog IP address of this switch.
• Server Port	Provide the port number of remote syslog server. Default Port no.: 514
• 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 unstable 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.
• Facility	Local0~7 : local user 0~7

Buttons

: Click to apply changes.



Remote Logging Setting Status

Status	Server Info	Severity	Facility	Action

Figure 4-2-17 Remote Log Setting Status 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 Log 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.

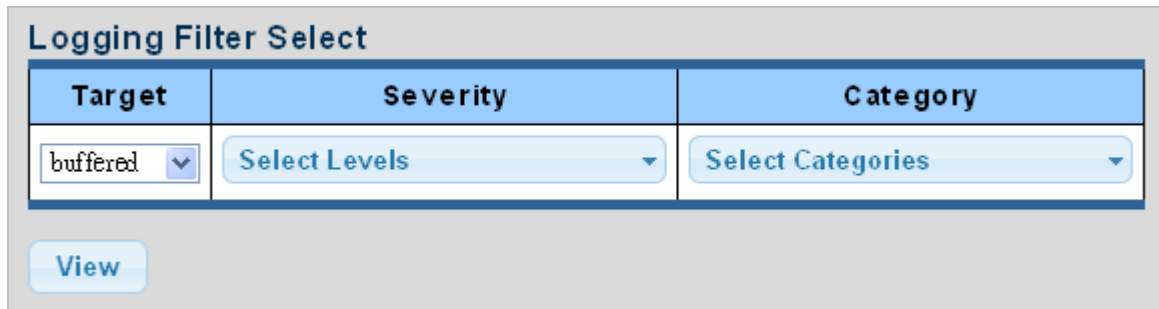


Figure 4-2-18 Log Information Select Screenshot

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. ■ File: Target the file 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 unstable 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 includes: AAA, ACL, CABLE_DIAG, DAI, DHCP_SNOOPING, Dot1X, GVRP, IGMP_SNOOPING, IPSG, L2, LLDP, Mirror, MLD_SNOOPING, Platform, PM, Port, PORT_SECURITY, QoS, Rate, SNMP and STP

Buttons

View: Click to view log.

Logging Information	
Information Name	Information Value
Target	buffered
Severity	emerg, alert, crit, error, warning, notice
Category	AAA, ACL, CABLE_DIAG, DAI, DHCP_SNOOPING, Dot1X, GVRP, IGMP_SNOOPING, IPSG, L2, LLDP, Mirror, MLD_SNOOPING, Platform, PM, Port, PORT_SECURITY, QoS, Rate, SNMP, STP, Security-suite, System, Trunk, VLAN
Total Entries	1

Figure 4-2-19 Logging Information 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

Logging Messages				
Clear buffered messages		Refresh		
FIRST	PREV	1	NEXT	LAST
No.	Timestamp	Category	Severity	Message
1	Jan 01 2000 08:00:19	Port	notice	Port gi1 link up

Figure 4-2-20 Logging Messages 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: Click to clear the log.: 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 (NMS's), SNMP agents, Management information base (MIB) and network-management protocol:

- **Network management stations (NMS's):** Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMS's 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 NMS's. SNMP is the Internet community's de facto standard management protocol.

SNMP Operations

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

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

SNMP community

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

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

4.2.7.2 SNMP System Information

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




The screenshot shows the 'SNMP Global Setting' interface. It features a 'State' section with two radio buttons: 'Disabled' (selected) and 'Enabled'. Below this is an 'Apply' button.

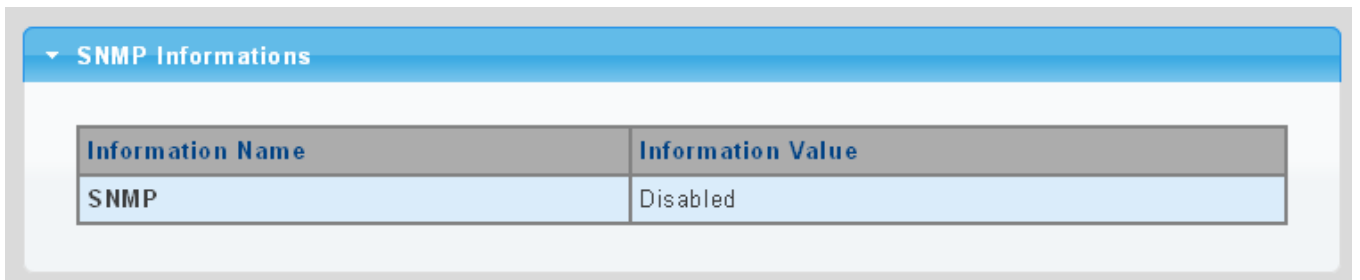
Figure 4-2-21 SNMP Global Setting Screenshot

The page includes the following fields:

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

Buttons

: Click to apply changes.



The screenshot shows the 'SNMP Informations' section. It contains a table with two columns: 'Information Name' and 'Information Value'. The table has one row with 'SNMP' as the name and 'Disabled' as the value.

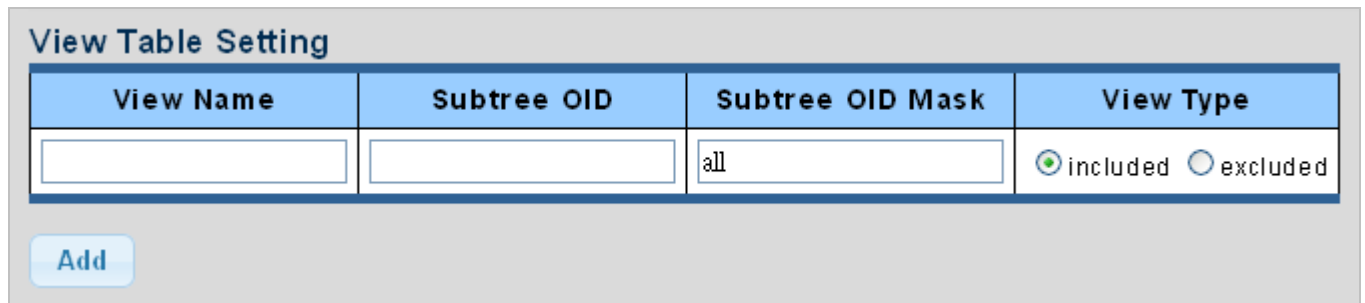
Figure 4-2-22 SNMP Information Screenshot

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 'View Table Setting' interface. It features a table with four columns: 'View Name', 'Subtree OID', 'Subtree OID Mask', and 'View Type'. The 'View Name' and 'Subtree OID' columns have empty text input fields. The 'Subtree OID Mask' column has a text input field containing 'all'. The 'View Type' column has two radio buttons: 'included' (which is selected) and 'excluded'. Below the table is a blue 'Add' button.

Figure 4-2-23 SNMPv3 View Table Setting Screenshot

The page includes the following fields:

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

Buttons

Add: Click to add a new view entry.



The screenshot shows the 'View Table Status' interface. It features a table with five columns: 'View Name', 'Subtree OID', 'OID Mask', 'View Type', and 'Action'. The 'View Name' column contains 'all', the 'Subtree OID' column contains '.1', the 'OID Mask' column contains 'all', and the 'View Type' column contains 'included'. The 'Action' column is empty.

Figure 4-2-24 SNMP View Table Status Screenshot

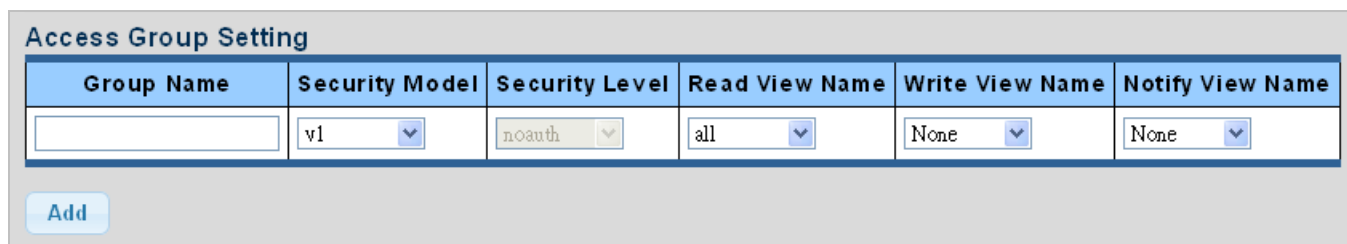
The page includes the following fields:

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	<div>Delete</div> : 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.



The screenshot shows the 'Access Group Setting' interface. It features a table with six columns: Group Name, Security Model, Security Level, Read View Name, Write View Name, and Notify View Name. Below the table is an 'Add' button.

Group Name	Security Model	Security Level	Read View Name	Write View Name	Notify View Name
<input type="text"/>	v1	noauth	all	None	None

Add

Figure 4-2-25 SNMPv3 Access Group Setting 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.

	<ul style="list-style-type: none"> ■ auth: Authentication and none privacy. ■ priv: Authentication and privacy. <p>Note: The Security Level applies to SNNPv3 only.</p>
• 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>
• 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>
• Notify View Name	<p>Notify view name is the name of the view in which you specify a notify, inform, or trap.</p>

Buttons

Add : Click to add a new access entry.

Delete : Check to delete the entry.



Access Group Status						
Group Name	Security Model	Security Level	Read View Name	Write View Name	Notify View Name	Action

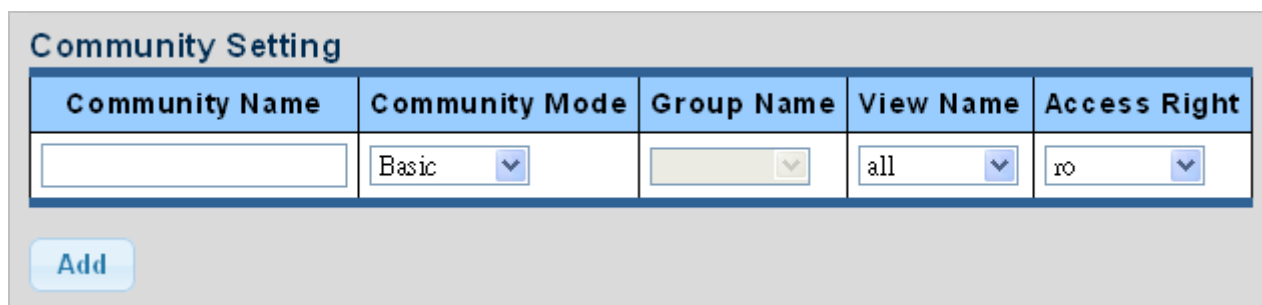
Figure 4-2-26 SNMP View Table Status Screenshot

The page includes the following fields:

Object	Description
• Group Name	Display the current SNMP access group name
• Security Model	Display the current security model
• Security Level	Display the current security level
• Read View Name	Display the current read view name
• Write View Name	Display the current write view name
• Notify View Name	Display the current notify view name
• Action	<p>Delete : Delete the access group entry.</p>

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 'Community Setting' interface. It features a table with five columns: 'Community Name', 'Community Mode', 'Group Name', 'View Name', and 'Access Right'. Each column has a corresponding input field or dropdown menu. Below the table is an 'Add' button.

Community Name	Community Mode	Group Name	View Name	Access Right
<input type="text"/>	Basic <input type="button" value="v"/>	<input type="text"/>	all <input type="button" value="v"/>	ro <input type="button" value="v"/>

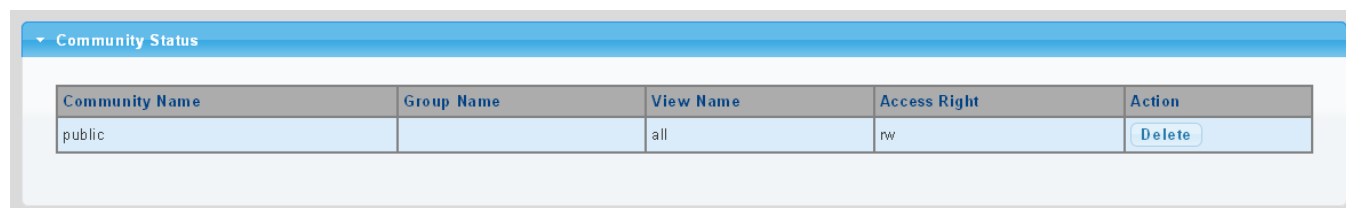
Figure 4-2-27 Community Setting Screenshot

The page includes the following fields:

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

Buttons

: Click to apply changes.




The screenshot shows the 'Community Status' interface. It features a table with five columns: 'Community Name', 'Group Name', 'View Name', 'Access Right', and 'Action'. The first row shows 'public' in the 'Community Name' column and 'Delete' in the 'Action' column.

Community Name	Group Name	View Name	Access Right	Action
public		all	rw	<input type="button" value="Delete"/>

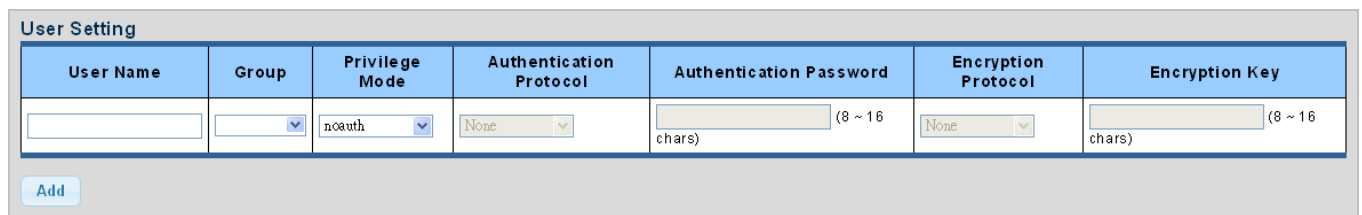
Figure 4-2-28 Community Status Screenshot

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
• 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.



User Name	Group	Privilege Mode	Authentication Protocol	Authentication Password	Encryption Protocol	Encryption Key
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> (8 ~ 16 chars)	<input type="text"/>	<input type="text"/> (8 ~ 16 chars)


Figure 4-2-29 SNMPv3 Users Configuration Screenshot

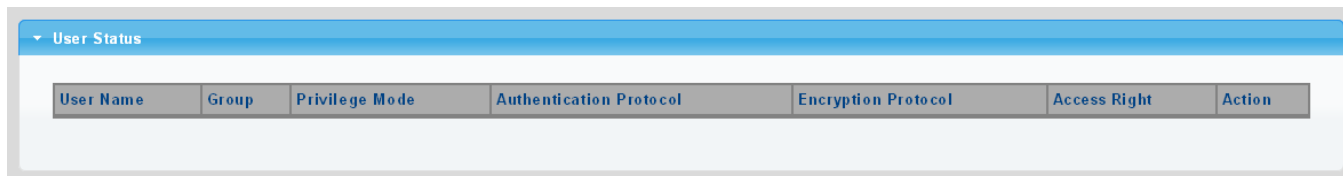
The page includes the following fields:

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 protocols, the allowed string length is 8 to 16.
• Encryption Protocol	<p>Indicates the privacy protocol that this entry should belong to. Possible privacy protocol are:</p> <ul style="list-style-type: none"> ■ None: None privacy protocol. ■ DES: An optional flag to indicate that this user using DES authentication protocol.
• Encryption Key	<p>A string identifying the privacy pass phrase.</p> <p>The allowed string length is 8 to 16.</p>

Buttons


: Click to add a new user entry.



User Status						
User Name	Group	Privilege Mode	Authentication Protocol	Encryption Protocol	Access Right	Action

Figure 4-2-30 SNMPv3 Users Status 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.



The screenshot shows the 'SNMPv1,2 Host Setting' form. It contains a table with the following fields:

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)

Below the table is an 'Add' button.

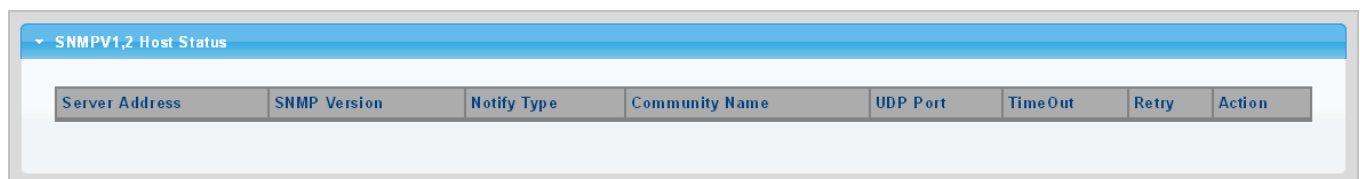
Figure 4-2-31 SNMPv1, 2 Notification Recipients Screenshot

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 from 1 to 300 .
• Retries	Indicates the SNMP trap inform retry times. The allowed range is from 1 to 255 .

Buttons

Add: Click to add a new SNMPv1, 2 host entry.



The screenshot shows the 'SNMPV1,2 Host Status' table. It has a header row with the following columns:

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

Figure 4-2-32 SNMPv1, 2 Host Status 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
• Retries	Display the current retry times
• Action	<div>Delete</div> : 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.

SNMPv3 Host Setting

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

Add

Figure 4-2-33 SNMPv3 Notification Recipients 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 from 1 to 300 .
• Retries	Indicates the SNMP trap inform retry times. The allowed range is from 1 to 255 .

Buttons

Add : Click to add a new SNMPv3 host entry.

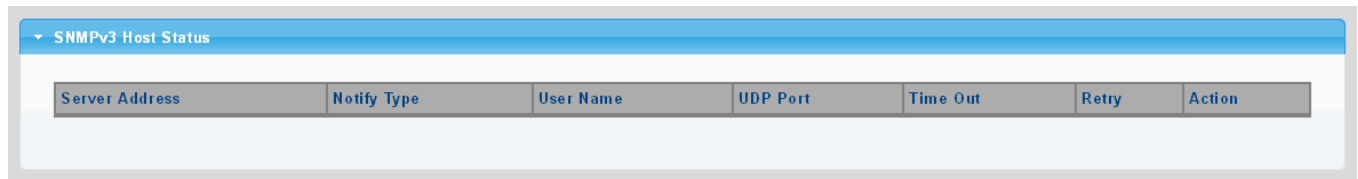


Figure 4-2-34 SNMPv3 Host Status Screenshot

The page includes the following fields:

Object	Description
• Server Address	Display the current server address
• Notify Type	Display 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
• Retries	Display the current retry times
• Action	<div>Delete</div> : 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.

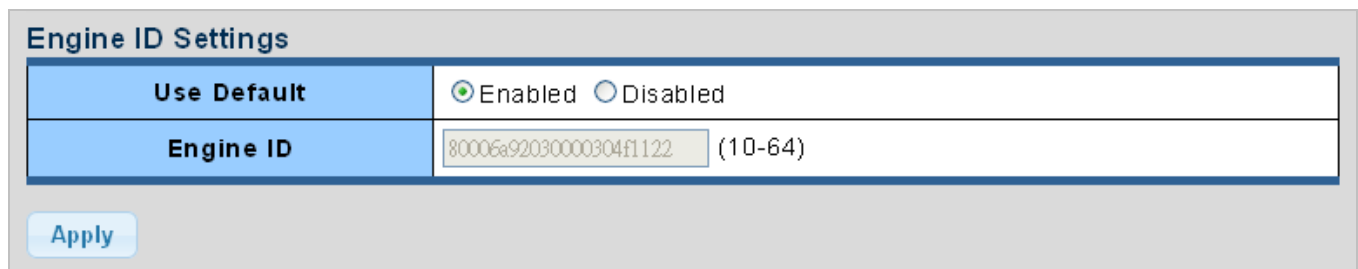


Figure 4-2-35 SNMPv3 Engine ID Setting Screenshot

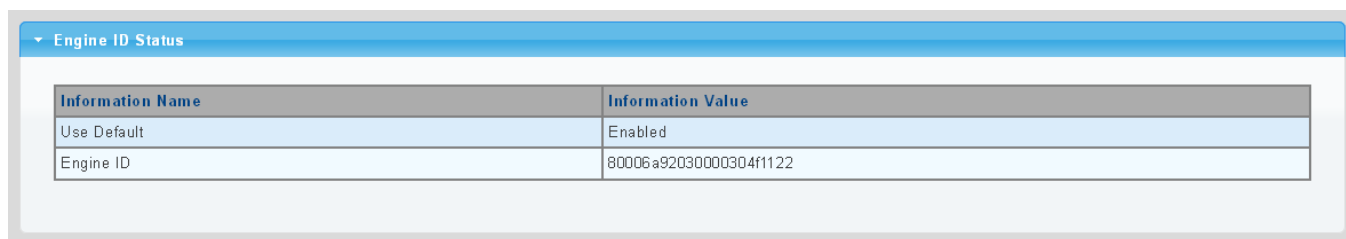
The page includes the following fields:

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.

Buttons



: Click to apply changes.



Engine ID Status	
Information Name	Information Value
Use Default	Enabled
Engine ID	80006a92030000304f1122

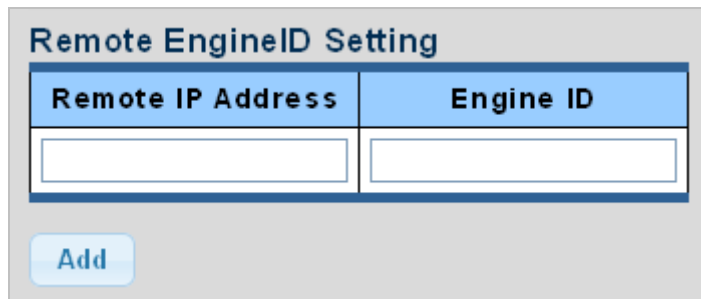
Figure 4-2-36 SNMPv3 Engine ID Status Screenshot

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.



Remote EngineID Setting

Remote IP Address	Engine ID
<input type="text"/>	<input type="text"/>


Add

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

The page includes the following fields:

Object	Description
• Remote IP Address	Indicates the SNMP remote engine ID address. It allows a valid IP address in dotted decimal notation ('x.y.z.w').
• Engine ID	An octet string identifying the engine ID that this entry should belong to.

Buttons

: Click to apply changes.

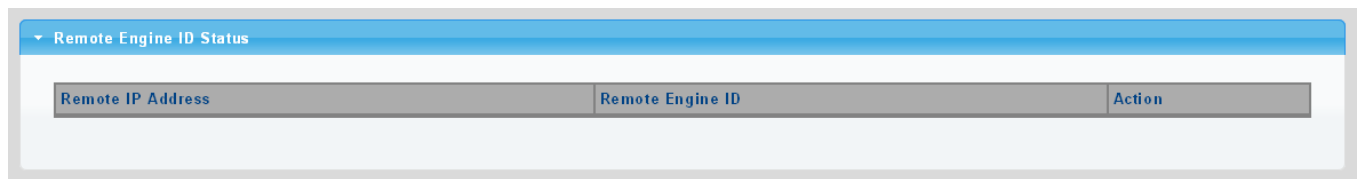



Figure 4-2-38 SNMPv3 Remote Engine ID Status Screenshot

The page includes the following fields:

Object	Description
• Remote IP Address	Display the current remote IP address
• Engine ID	Display the current engine ID
• Action	 : Delete the remote IP address entry

4.3 Port Management

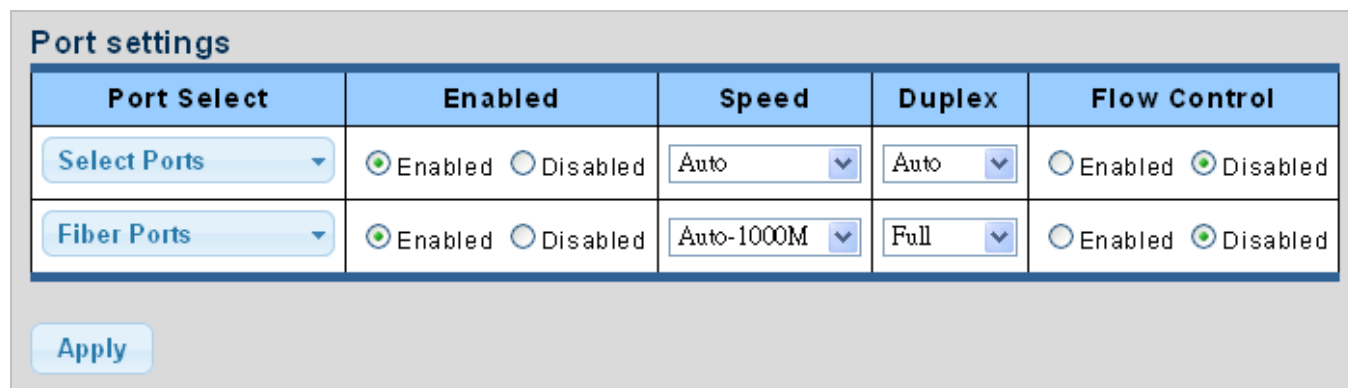
Use the Port Menu to display or configure the Managed Switch's ports. This section has the following items:

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

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.



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

Apply

Figure 4-3-1 Port Settings Screenshot

The page includes the following fields:

Object	Description
• Port Select	Select port number from 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.

<ul style="list-style-type: none"> • Speed 	<p>Select any available link speed for the given switch port. Draw the menu bar to select the mode.</p> <ul style="list-style-type: none"> ■ Auto - Setup Auto negotiation. ■ 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. When a fixed-speed setting is selected, that is what is used. Current Rx column indicates whether pause frames on the port are obeyed. Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.</p>

Buttons




: Click to apply changes.

▼ Port Status							
Port	Description	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
GE1	Edit	Enabled	UP	A-1000M	A-Full	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

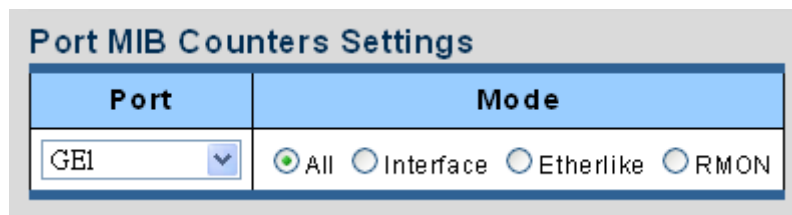
Figure 4-3-2 Port Status Screenshot

The page includes the following fields:

Object	Description
• Port	This is the logical port number for this row
• Description	Click  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](#) and [Figure 4-3-6](#) appear.



The screenshot shows a web interface titled "Port MIB Counters Settings". It contains a table with two columns: "Port" and "Mode". The "Port" column has a dropdown menu with "GE1" selected. The "Mode" column has four radio buttons: "All" (selected), "Interface", "Etherlike", and "RMON".

Figure 4-3-3 Port MIB Counters Screenshot

The page includes the following fields:

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

Interface Counters	Counters Value
Received Octets	0
Received Unicast Packets	0
Received Unknown Unicast Packets	0
Received Discards Packets	0
Transmit Octets	0
Transmit Unicast Packets	0
Transmit Unknown Unicast Packets	0
Transmit Discards Packets	0
Received Multicast Packets	0
Received Broadcast Packets	0
Transmit Multicast Packets	0
Transmit Broadcast Packets	0

Figure 4-3-4 Interface Counters Screenshot

Object	Description
• Received Octets	The total number of octets received on the interface, including framing characters.
• Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
• Received Unknown Unicast Packets	The number of packets received via the interface which is discarded because of an unknown or unsupported protocol.
• 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.
• Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
• 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.
• Transmit Unknown 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.
• Transmit Discards Packets	The number of inbound packets which is chosen to be discarded even though no errors have been detected to prevent from being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
• Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-) layer, is addressed to a multicast address at this sub-layer.

• Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-) layer, addressed to a broadcast address at this sub-layer.
• Transmit Multicast Packets	The total number of packets that higher-level protocols requested is transmitted and is addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
• Transmit Broadcast Packets	The total number of packets that higher-level protocols requested is transmitted, and addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

Ethernet-link Counters	Counters Value
Alignment Errors	0
FCS Errors	0
Single Collision Frames	0
Multiple Collision Frames	0
Deferred Transmissions	0
Late Collision	0
Excessive Collision	0
Frame Too Longs	0
Symbol Errors	0
Control In Unknow Opcodes	0
In Pause Frames	0
Out Pause Frames	0

Figure 4-3-5 Ethernet link Counters Screenshot

Object	Description
• Alignment Errors	The number of alignment errors (missynchronized data packets).
• FCS Errors	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.
• Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
• Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
• Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
• Late Collision	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
• Excessive Collision	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increase when the interface is

	operating in full-duplex mode.
• Frame Too Long	A count of frames received on a particular interface that exceeds the maximum permitted frame size.
• Symbol Errors	The number of received and transmitted symbol errors
• Control In Unknown Opcodes	The number of received control unknown opcodes
• In Pause Frames	The number of received pause frames
• Out Pause Frames	The number of transmitted pause frames

RMON Counters	Counters Value
Drop Events	0
Octets	0
Packets	0
Broadcast Packets	0
Multicast Packets	0
CRC / Alignment Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
64 Bytes Frame	0
65-127 Byte Frames	0
128-255 Byte Frames	0
256-511 Byte Frames	0
512-1023 Byte Frames	0
1024-1518 Byte Frames	0

Figure 4-3-6 RMON Counters Screenshot

Object	Description
• Drop Events	The total number of events in which packets were dropped due to lack of resources.
• Octets	The total number of octets received and transmitted on the interface, including framing characters.
• Packets	The total number of packets received and transmitted on the interface.
• Broadcast Packets	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.

• Multicast Packets	The total number of good frames received that were directed to this multicast address.
• CRC / Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
• Undersize Packets	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.
• Oversize Packets	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.
• 64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
• 65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets falls 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:

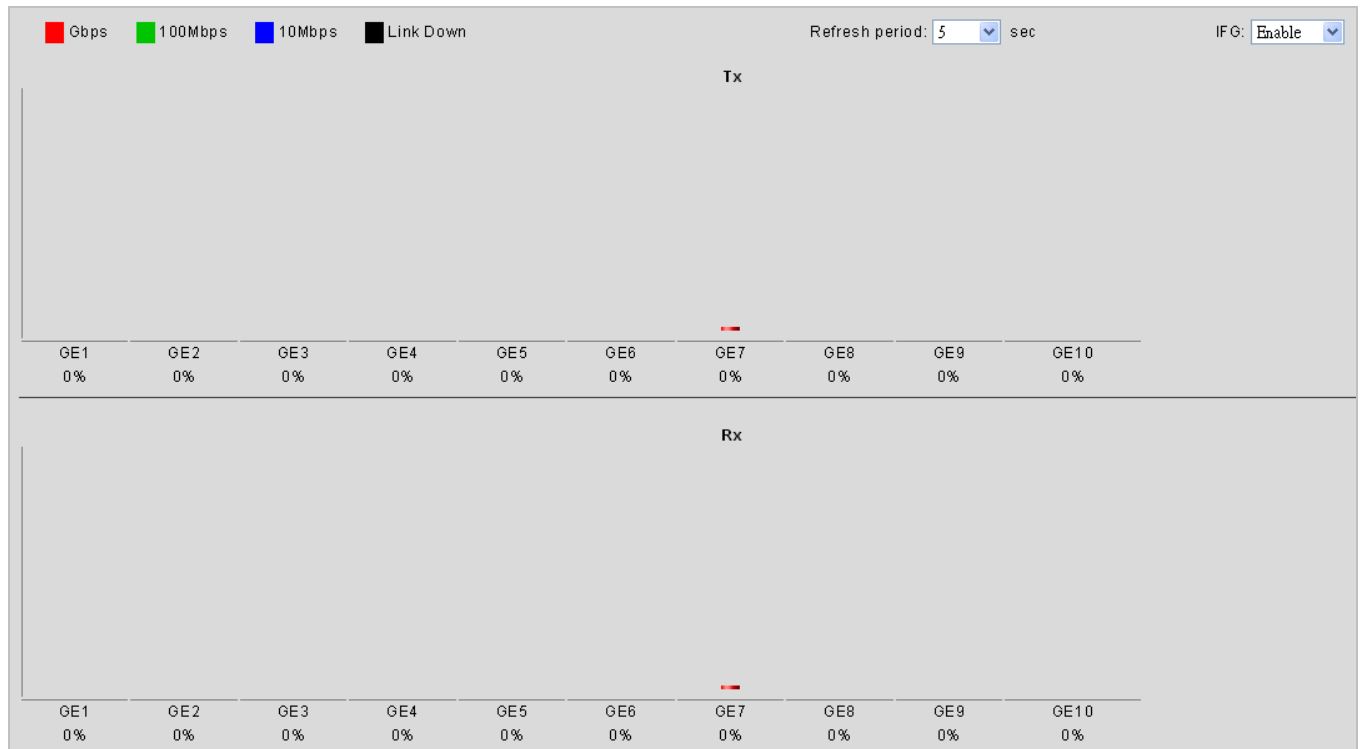


Figure 4-3-7 Port Bandwidth Utilization Screenshot

The page includes the following fields:

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

4.3.4 Port Mirroring

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

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

Port Mirror Application

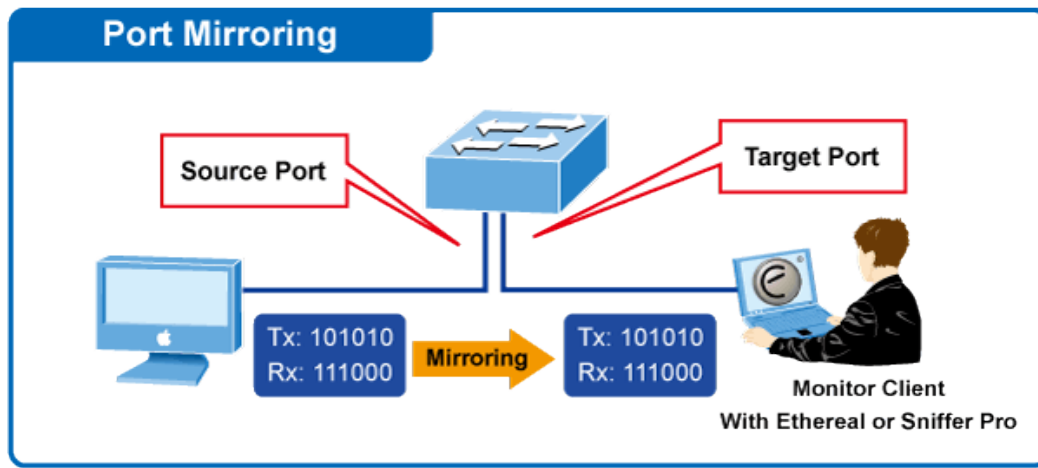


Figure 4-3-8 Port Mirror Application

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 <input type="button" value="v"/>
Monitor session state	Disable <input type="button" value="v"/>
Destination Port	GE1 <input type="button" value="v"/>
allow-ingress	Disable <input type="button" value="v"/>
Sniffer RX Ports	Select RX Ports <input type="button" value="v"/>
Sniffer TX Ports	Select TX Ports <input type="button" value="v"/>

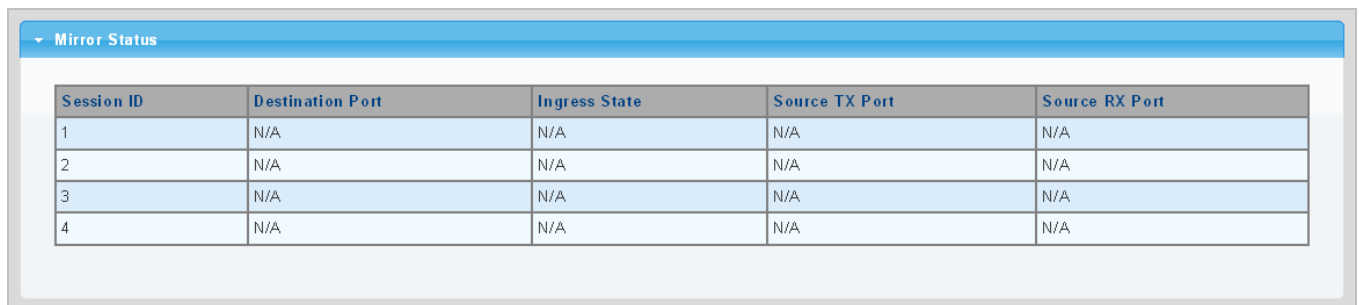
Figure 4-3-9 Port Mirroring Settings Screenshot

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 TX Ports	Frames transmitted from these ports are mirrored to the mirroring port. Frames received are not mirrored.
• Sniffer RX Ports	Frames received at these ports are mirrored to the mirroring port. Frames transmitted are not mirrored.

Buttons

: Click to apply changes.



Mirror Status				
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

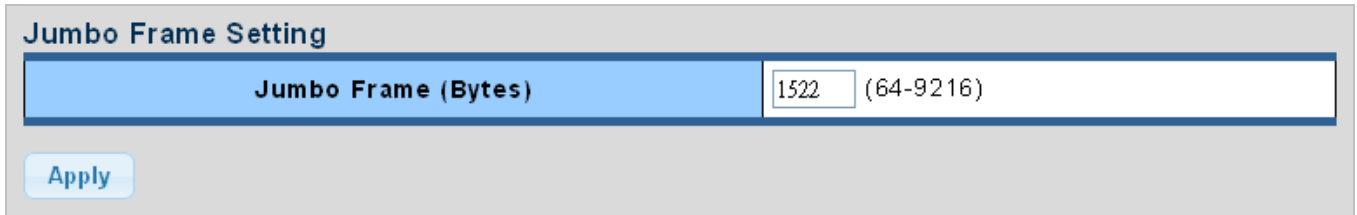
Figure 4-3-10 Mirroring Status Screenshot

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 screen in [Figure 4-3-11](#) and [Figure 4-3-12](#) appear.



The screenshot shows a web interface titled "Jumbo Frame Setting". It features a blue header bar with the title. Below the header, there is a form with a label "Jumbo Frame (Bytes)" and a text input field containing the value "1522". To the right of the input field, the range "(64-9216)" is displayed. Below the form, there is a blue button labeled "Apply".

Figure 4-3-11 Jumbo Frame Setting Screenshot

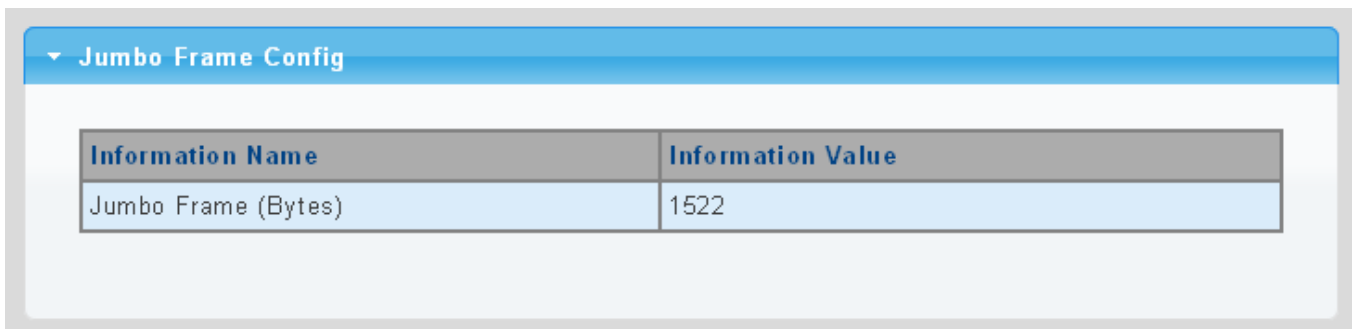
The page includes the following fields:

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

Buttons



: Click to apply changes.



The screenshot shows a web interface titled "Jumbo Frame Config". It features a blue header bar with the title. Below the header, there is a table with two columns: "Information Name" and "Information Value". The table contains one row with the value "1522" in the "Information Value" column.

Figure 4-3-12 Jumbo Frame Information 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.

Error Disabled Recovery

Recovery Interval	<input type="text" value="300"/> (Seconds)
BPDU Guard	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Self Loop	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Broadcast Flood	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Unknown Multicast Flood	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Unicast Flood	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
ACL	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Port Security Violation	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DHCP rate limit	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
ARP rate limit	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Apply

Figure 4-3-13 Error Disabled Recovery 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).
• 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

Buttons



: 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 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

This page provides disable that transitions a port into error disable 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 Screenshot

The displayed counters are:

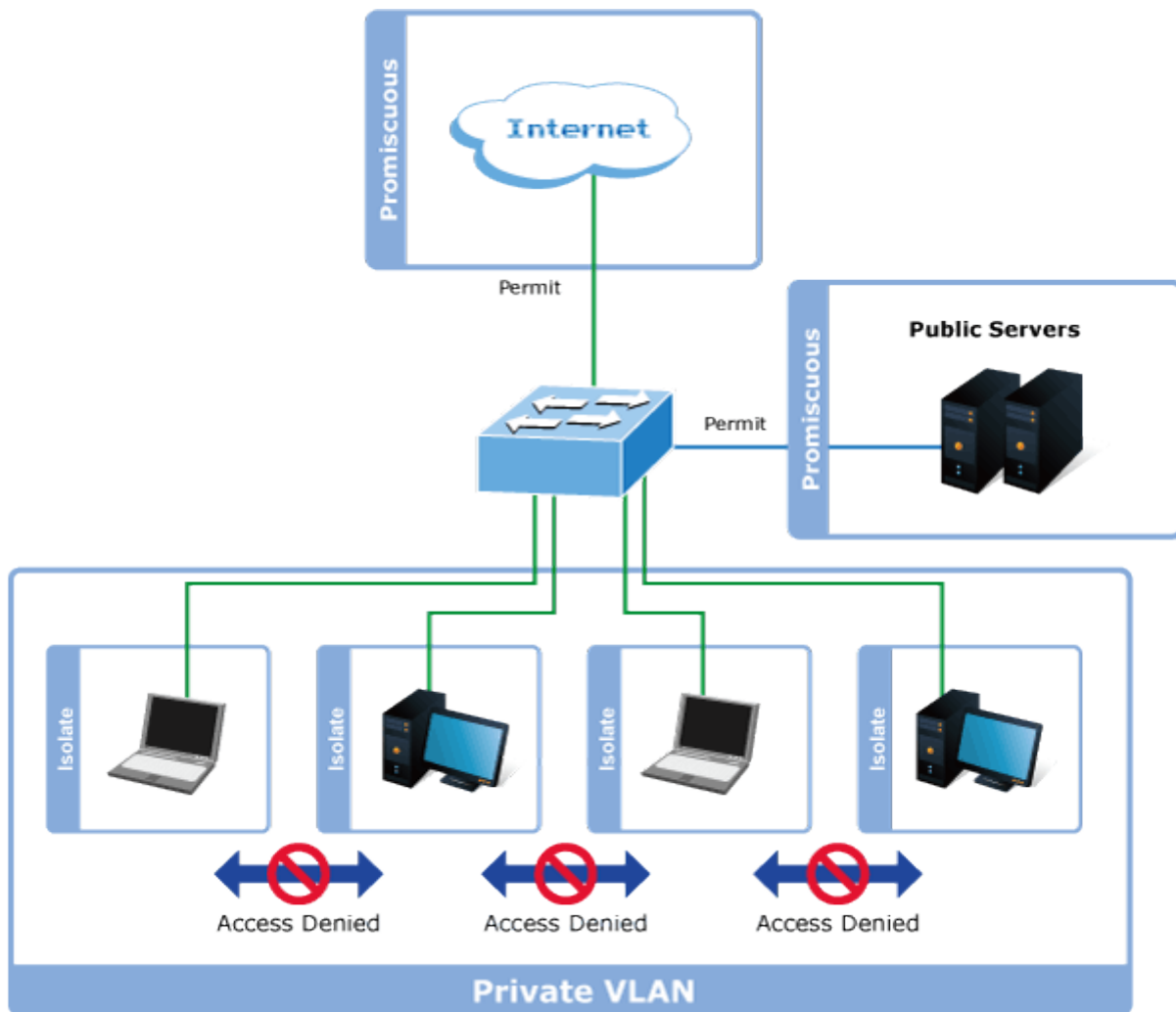
Object	Description
• Port Name	Display the port for error disable
• Error Disable Reason	Display the error disabled reason of the port
• Time Left (Seconds)	Display the time left

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

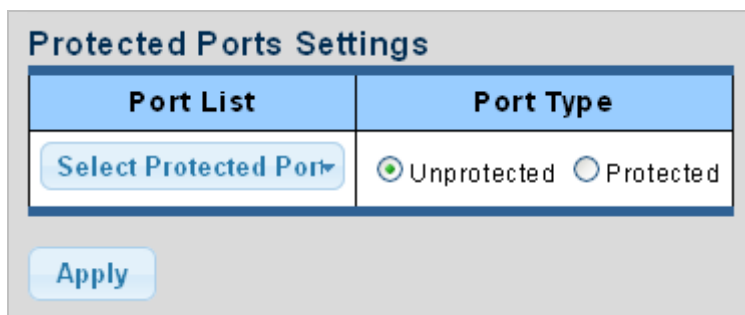


For protected port group to be applied, the Managed switch must first be configured for standard VLAN operation. Ports in a protected port group fall into one of these two groups:

- **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.



The screenshot shows a 'Protected Ports Settings' window. It contains two main sections: 'Port List' and 'Port Type'. The 'Port List' section has a dropdown menu labeled 'Select Protected Port'. The 'Port Type' section has two radio buttons: 'Unprotected' (which is selected) and 'Protected'. At the bottom of the window is an 'Apply' button.

Figure 4-3-16 Protected Ports Settings Screenshot

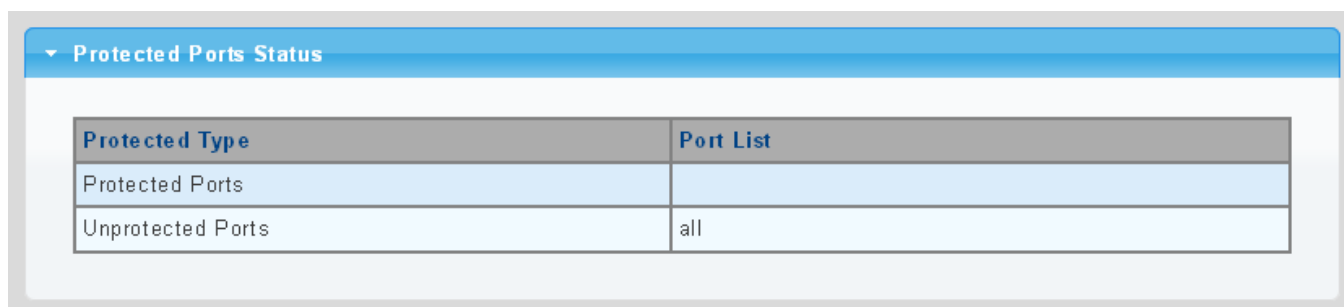
The page includes the following fields:

Object	Description
• Port List	Select port number from this drop-down list.
• Port Type	<p>Displays protected port types.</p> <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.

Buttons



: Click to apply changes.



The screenshot shows a 'Protected Ports Status' window. It contains a table with two columns: 'Protected Type' and 'Port List'. The table has two rows: 'Protected Ports' and 'Unprotected Ports'. The 'Unprotected Ports' row shows 'all' in the 'Port List' column.

Protected Type	Port List
Protected Ports	
Unprotected Ports	all

Figure 4-3-17 Port Isolation Status Screenshot

The page includes the following fields:

Object	Description
• Protected Ports	Display the current protected ports
• 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 screen in [Figure 4-3-18](#) and [Figure 4-3-19](#) appears.

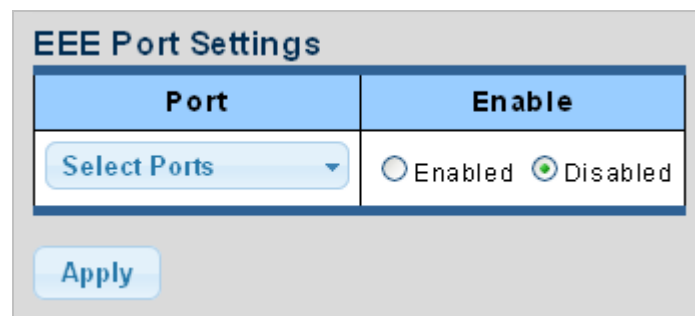


Figure 4-3-18 EEE Port Settings Screenshot

The page includes the following fields:

Object	Description
• Port	Select port number from this drop-down list
• Enable	Enable or disable the EEE function

Buttons

: Click to apply changes.

EEE Enable Status	
Port	EEE State
GE1	Disabled
GE2	Disabled
GE3	Disabled
GE4	Disabled
GE5	Disabled
GE6	Disabled
GE7	Disabled
GE8	Disabled

Figure 4-3-19 EEE Enable Status Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port
• EEE State	Display the current EEE state

4.3.10 SFP Module Information

Managed switch has supported the SFP module with **digital diagnostics monitoring (DDM)** function, this feature is also known as digital optical monitoring (DOM). You can check the physical or operational status of an SFP module via the SFP Module Information page. This page shows the operational status, such as the transceiver type, speed, wavelength, optical output power, optical input power, temperature, laser bias current and transceiver supply voltage in real time. You can also use the hyperlink of port no. to check the statistics on a specific interface.

4.3.10.1 SFP Module Status

The SFP Module Status screens in [Figure 4-3-20](#) and [Figure 4-3-21](#) appear.

Port Fiber Status

Port Selected

Port

GE1 ▼

Figure 4-3-20 Port Selected Screenshot with Sample Switch

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Port 	Select port number from this drop-down list



GE11 Fiber Port Status	
Fiber Status	Status Value
OE-Present	Insert
LOS	Loss
Transceiver Type	SFP/SFP+
Hot Plug	Support
Connect Type	LC
Fiber Type	Single Mode
Eth Compliance	1000BASE-LX
TX Distance	0(m)
Wave Length	1310(nm)
Baud Rate	1000M
Vendor OUI	0-90-65
Vendor Name	SANOANOCNOC OC
Vendor PN	SJ13J1311312312-
Vendor Rev	
Vendor SN	SJ13J1311312312-
Data Code	13-08-12
Temperature	64.718(°C)
Voltage	3.35(V)
Current	30.70(A)
Output power	0.27(mW)
Input power	0.00(mW)

Figure 4-3-21 Fiber Port Status Screenshot

The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> OE-Present 	Display the current SFP OE-present
<ul style="list-style-type: none"> LOS 	Display the current SFP LOS

4.3.10.1 SFP Module Detail Status

The SFP Module Detail Status screen in [Figure 4-3-22](#) appears.

Status Table							
Port	Temperature	Voltage	Current	Output Power	Input Power	Transmitter Fault	Loss of Signal
GE12	0.00	0.00	0.00	0.00	0.00	N/S	N/S

Figure 4-3-22 SFP Module Detail Status Screenshot with Sample Switch

The page includes the following fields:

Object	Description
• Port	The logical port for the settings contained in the same row
• Temperature	Display the current SFP temperature
• Voltage	Display the current SFP voltage
• Current	Display the current SFP current
• Output Power	Display the current SFP output power
• Input Power	Display the current SFP input power
• Transmit Fault	Display the current SFP transmits fault
• Loss of Signal	Display the current SFP loss of signal.
• Rate Ready	Display the current SFP rate ready.

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.

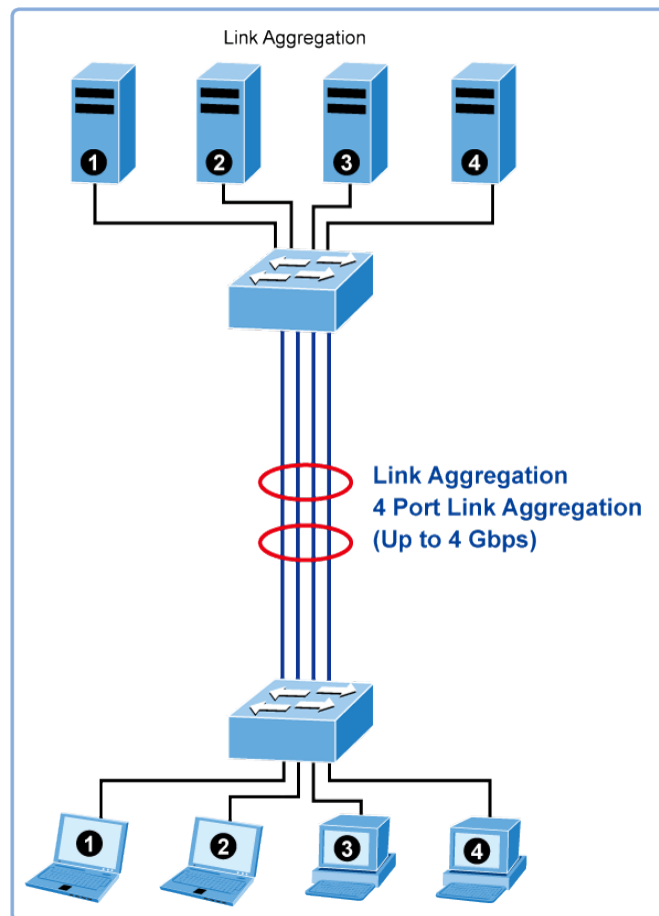


Figure 4-4-1 Link Aggregation

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. For more detailed 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.

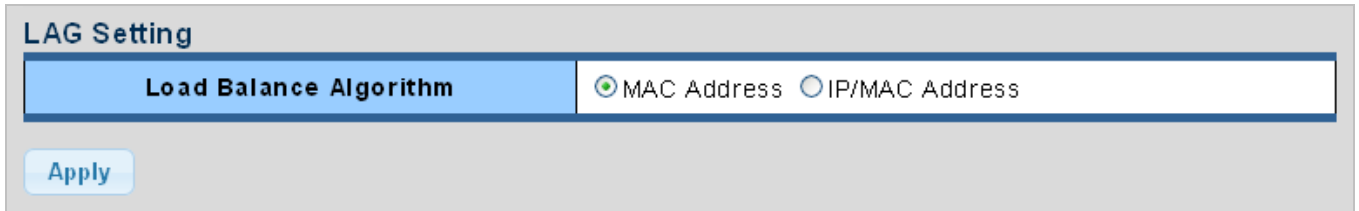
It allows a maximum of 8 ports to be aggregated at the same time. The Managed Switch supports Gigabit Ethernet ports (up to 8 groups). If the group is defined as an LACP static link aggregation group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports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

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.



The screenshot shows the 'LAG Setting' interface. It features a 'Load Balance Algorithm' tab and two radio buttons: 'MAC Address' (selected) and 'IP/MAC Address'. An 'Apply' button is located at the bottom left.

Figure 4-4-2 LAG Setting Screenshot

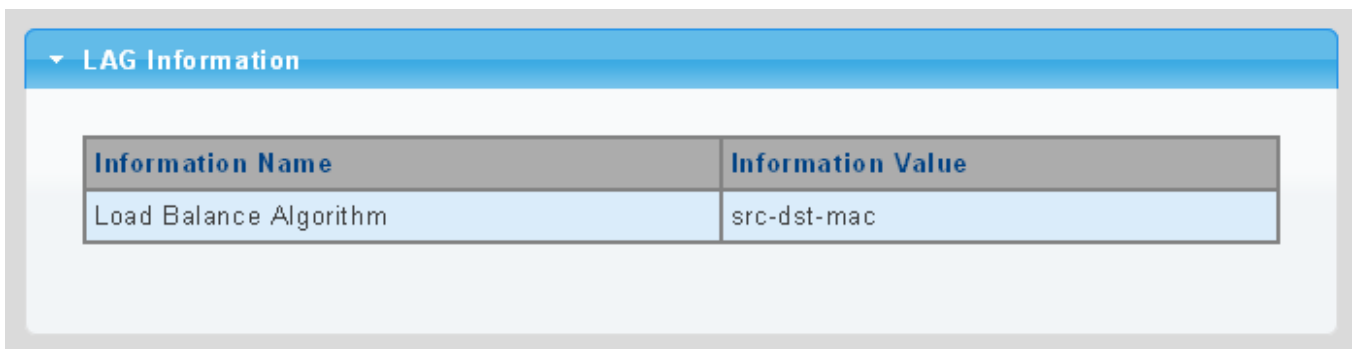
The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Load Balance Algorithm 	<p>Select load balance algorithm mode:</p> <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.

Buttons



: Click to apply changes.



The screenshot shows the 'LAG Information' section. It contains a table with two columns: 'Information Name' and 'Information Value'. The table lists 'Load Balance Algorithm' with the value 'src-dst-mac'.

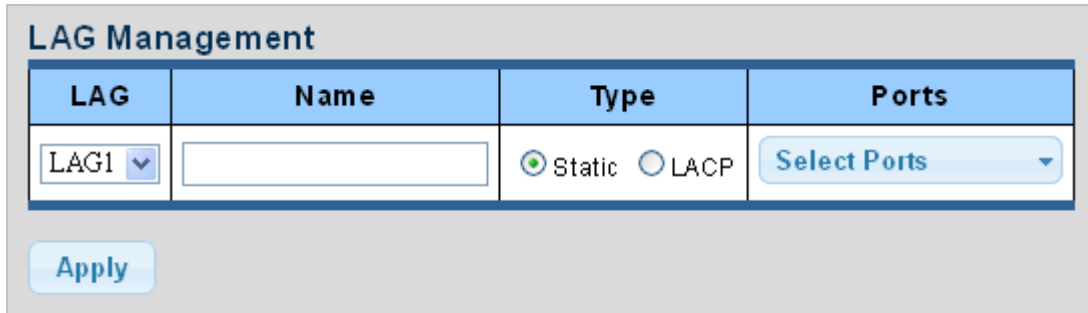
Figure 4-4-3 LAG Information Screenshot

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.

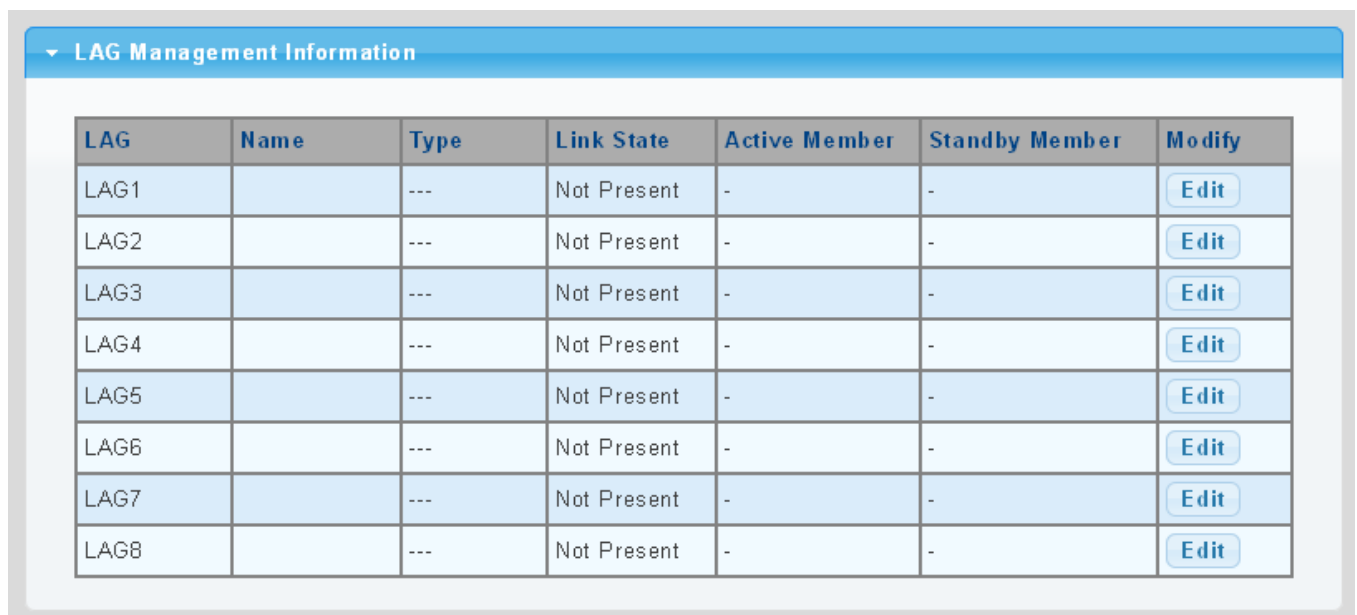


The screenshot shows the 'LAG Management' configuration interface. It features a table with four columns: 'LAG', 'Name', 'Type', and 'Ports'. The 'LAG' column has a dropdown menu currently set to 'LAG1'. The 'Name' column has an empty text input field. The 'Type' column has two radio buttons: 'Static' (which is selected) and 'LACP'. The 'Ports' column has a 'Select Ports' button with a dropdown arrow. Below the table is an 'Apply' button.

Figure 4-4-4 LAG Management Screenshot

The page includes the following fields:

Object	Description
• LAG	Select LAG number from this drop-down list
• Name	Indicates each LAG name
• 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 from this drop-down list to establish Link Aggregation




The screenshot shows the 'LAG Management Information' section, which contains a table listing the status of LAGs 1 through 8. Each row includes columns for LAG number, Name, Type, Link State, Active Member, Standby Member, and a Modify button.

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 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 configuration

4.4.3 LAG Port Setting

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

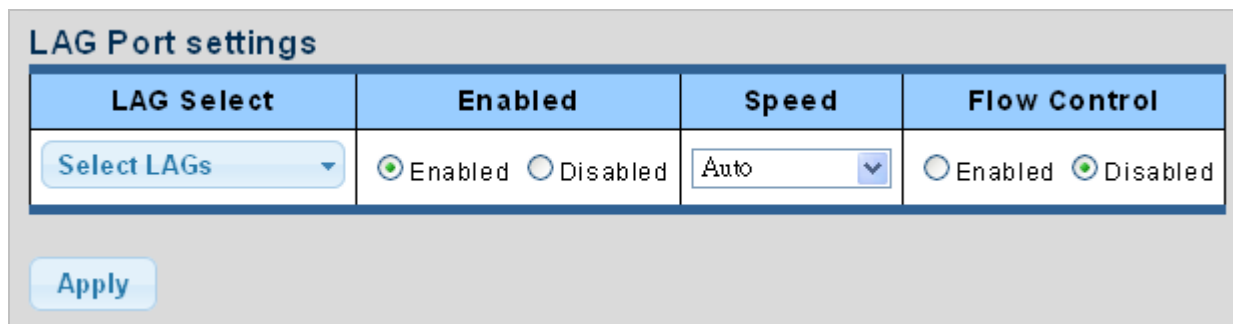


Figure 4-4-6 LAG Port Setting Information Screenshot

The page includes the following fields:

Object	Description
• LAG Select	Select LAG number from this drop-down list.
• Enable	Indicates the LAG state operation. Possible states are: Enabled - Start up the LAG manually. Disabled - Shut down 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 - Set up Auto negotiation. ■ Auto-10M - Set up 10M Auto negotiation. ■ Auto-100M - Set up 100M Auto negotiation.

	<ul style="list-style-type: none"> ■ Auto-1000M - Set up 1000M Auto negotiation. ■ Auto-10/100M – Set up 10/100M Auto negotiation. ■ 10M – Set up 10M Force mode. ■ 100M – Set up 100M Force mode. ■ 1000M – Set up 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. When a fixed-speed setting is selected, that is what is used. The current Rx column indicates whether pause frames on the port are obeyed. The current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.</p>

Buttons

Apply: 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 Screenshot

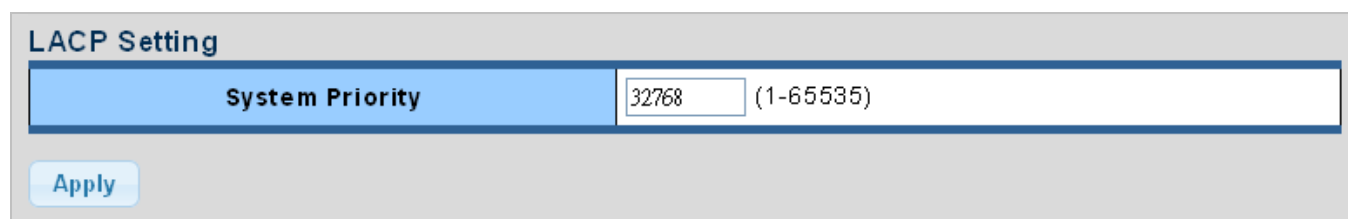
The page includes the following fields:

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
• 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.



The screenshot shows the 'LACP Setting' page. It features a blue header bar with the text 'LACP Setting'. Below this is a form with a blue background. The form has a label 'System Priority' and a text input field containing the value '32768'. To the right of the input field, the range '(1-65535)' is displayed. At the bottom left of the form is a blue button labeled 'Apply'.

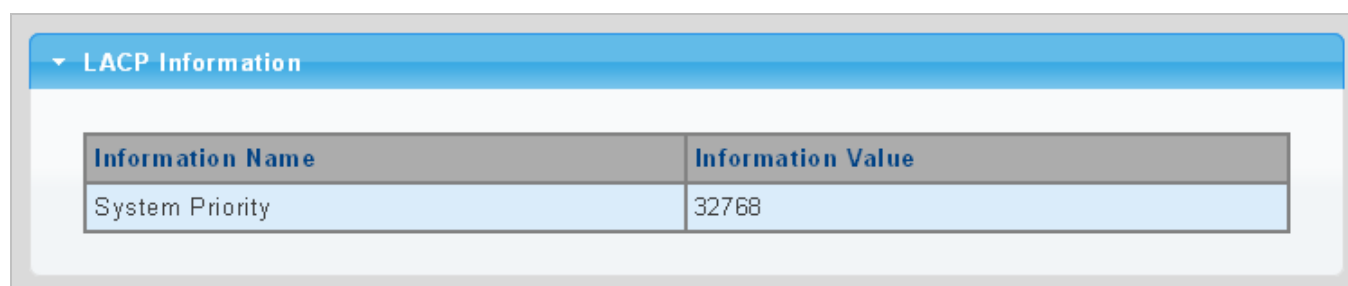
Figure 4-4-8 LACP Setting Screenshot

The page includes the following fields:

Object	Description
• 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.

Buttons

: Click to apply changes.



The screenshot shows the 'LACP Information' page. It features a blue header bar with the text 'LACP Information'. Below this is a table with two columns: 'Information Name' and 'Information Value'. The table contains one row with the value 'System Priority' in the first column and '32768' in the second column.

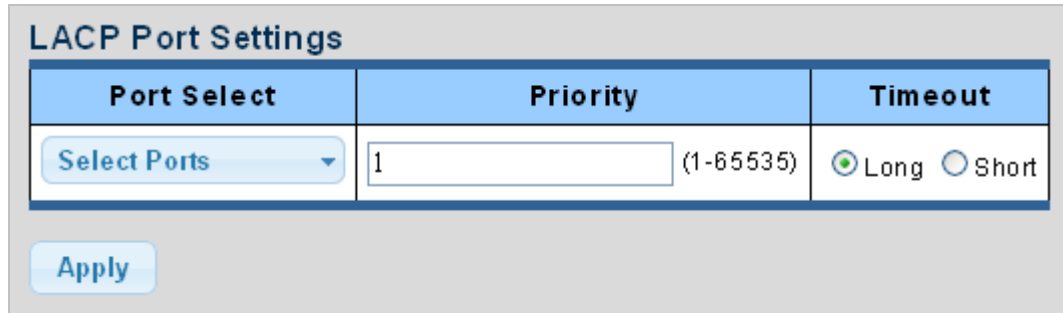
Figure 4-4-9 LACP Information Screenshot

The page includes the following fields:

Object	Description
• 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.



The screenshot shows the 'LACP Port Settings' interface. It features a table with three columns: 'Port Select', 'Priority', and 'Timeout'. The 'Port Select' column contains a dropdown menu labeled 'Select Ports'. The 'Priority' column contains a text input field with the value '1' and a range '(1-65535)'. The 'Timeout' column contains two radio buttons: 'Long' (selected) and 'Short'. Below the table is an 'Apply' button.

Figure 4-4-10 LACP Port Setting Screenshot

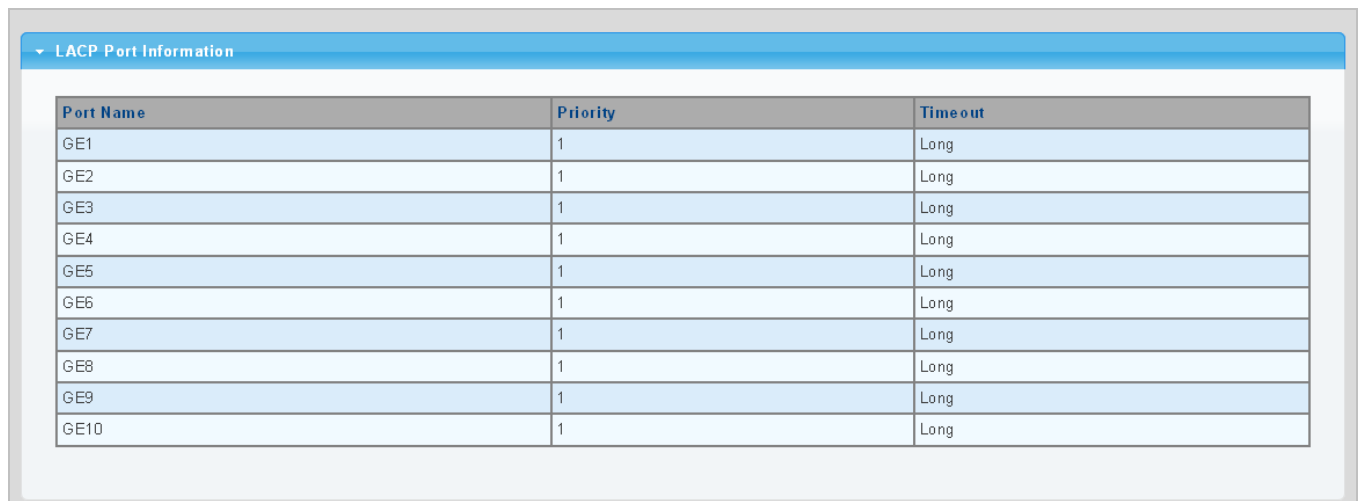
The page includes the following fields:

Object	Description
<ul style="list-style-type: none"> Port Select 	Select port number from this drop-down list to set LACP port setting.
<ul style="list-style-type: none"> Priority 	<p>The Priority 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 an LACP packet.</p>

Buttons



: Click to apply changes.



The screenshot shows the 'LACP Port Information' table. It has three columns: 'Port Name', 'Priority', and 'Time out'. The table lists 10 ports (GE1 to GE10) with a priority of 1 and a timeout of Long.

Port Name	Priority	Time out
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

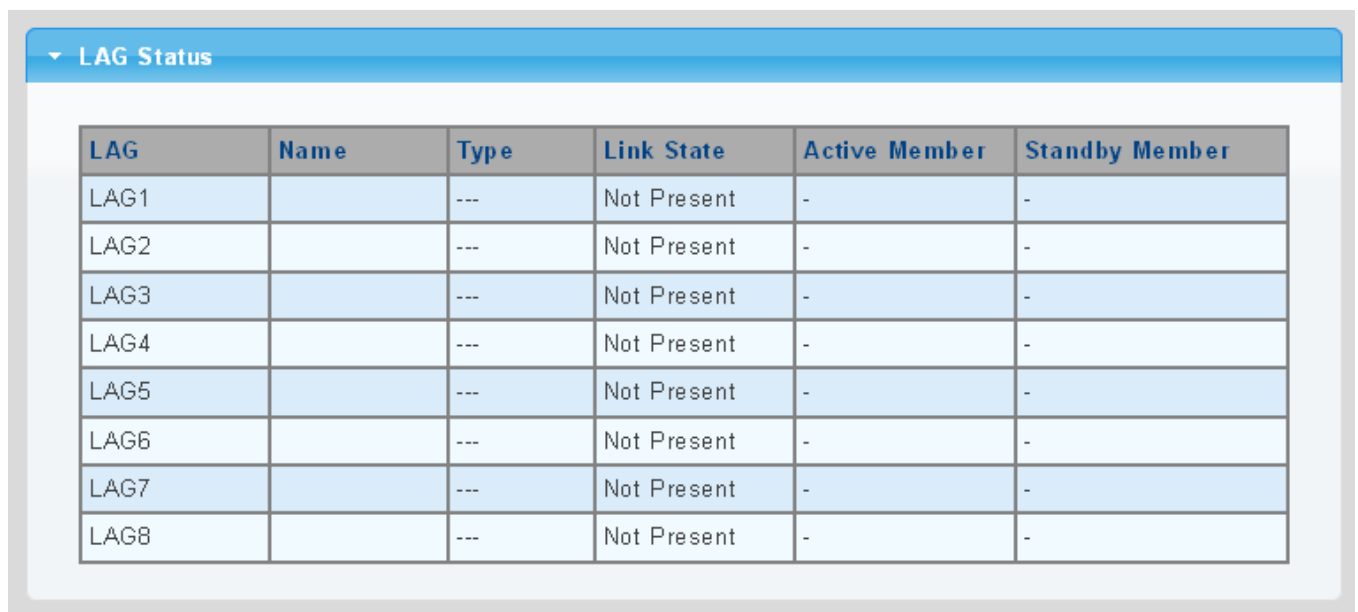
Figure 4-4-11 LACP Port Information Screenshot

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	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 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

LACP Information										
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 Screenshot

The page includes the following fields:

Object	Description
• Trunk	Display the current trunk 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 ■ “LACPDs” means LACP disabled state ■ “DFLT” means defaulted state ■ “CRRNT” means current state
• PrdTx	LACP periodic transmission state machine status of the port <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
• AtState	The actor state field of LACP PDU description. The field from left to right describes: “LACP_Activity”, “LACP_Timeout”,

	<p>"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 will show "_"; if the contents are true, the Web shows "A", "T", "G", "S", "C", "D", "F" and "E" for each content respectively.</p>

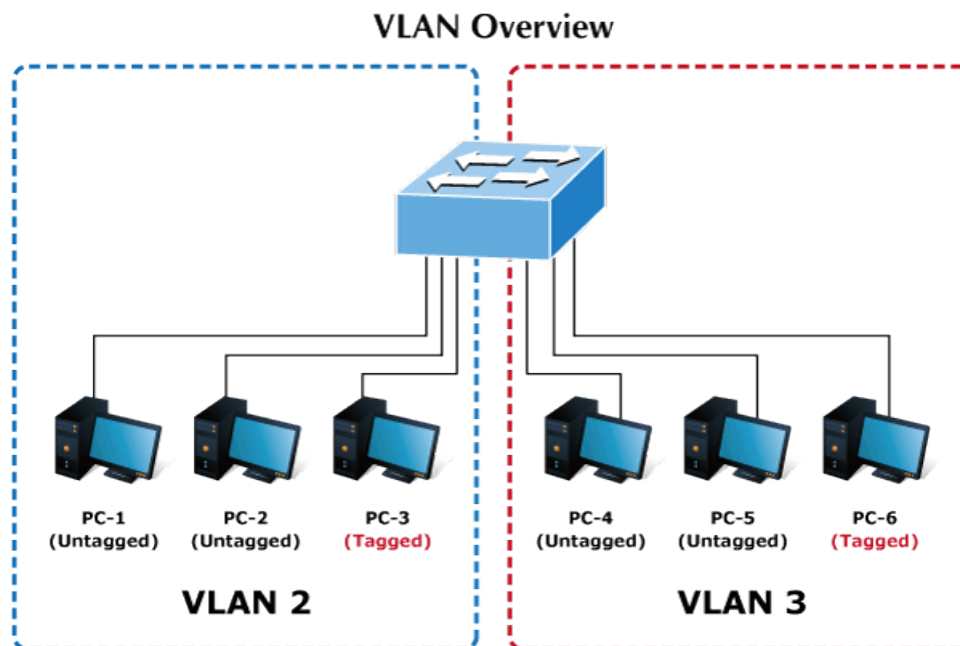
4.5 VLAN

4.5.1 VLAN Overview

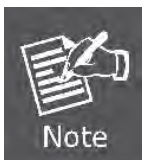
A **Virtual Local Area Network (VLAN)** is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different 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.

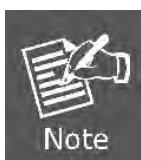
A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets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



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

■ IEEE 802.1Q Standard

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

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

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

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

Some relevant terms:

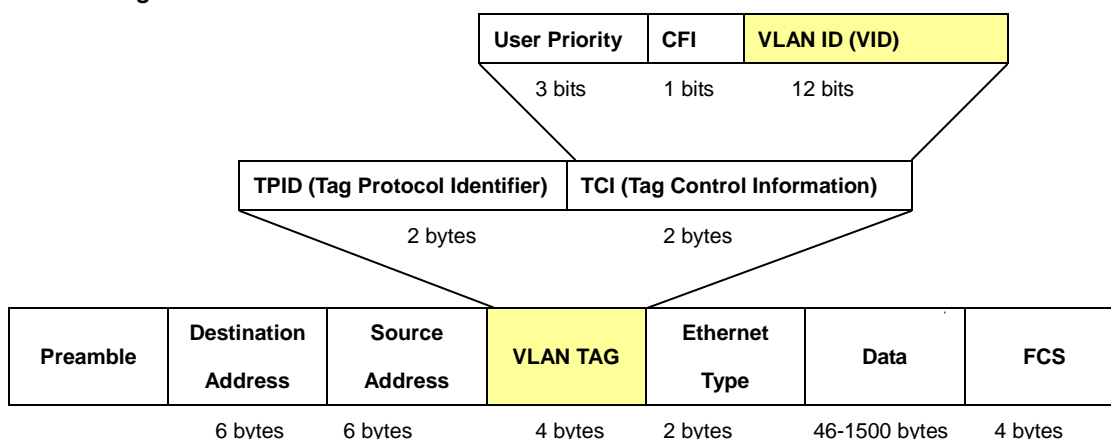
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

■ 802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of **0x8100** in the Ether Type field. When a packet's Ether Type field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of **VLAN ID (VID)**. The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

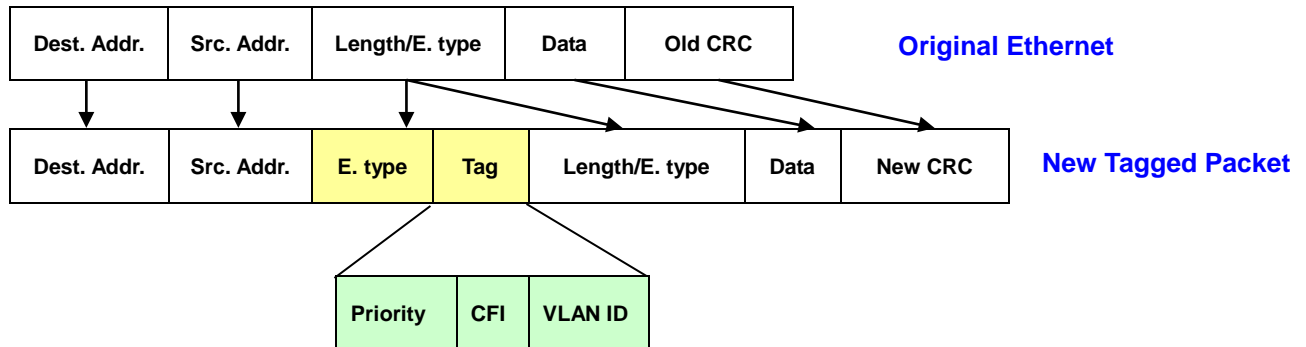
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



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

Adding an IEEE802.1Q Tag



■ Port VLAN ID

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

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

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

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

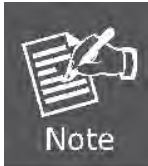
Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the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

■ Default VLANs

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

■ Assigning Ports to VLANs

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



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

■ VLAN Classification

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

■ Port Overlapping

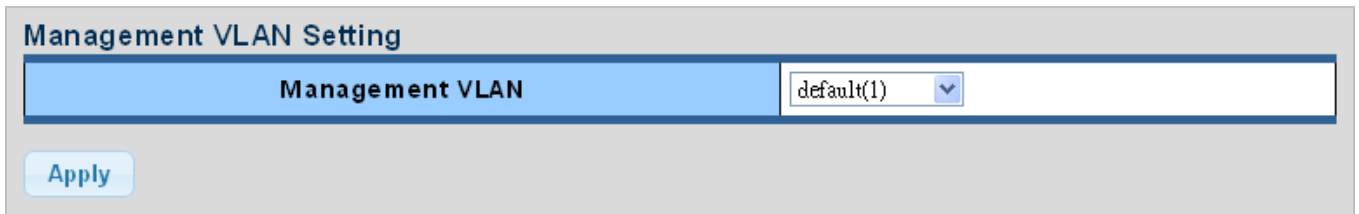
Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

■ Untagged VLANs

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

4.5.3 Management VLAN

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



The screenshot shows a web interface titled "Management VLAN Setting". It features a blue header bar with the title. Below the header, there is a form with a label "Management VLAN" and a dropdown menu showing "default(1)". An "Apply" button is located at the bottom left of the form.

Figure 4-5-1 Management VLAN Setting Screenshot

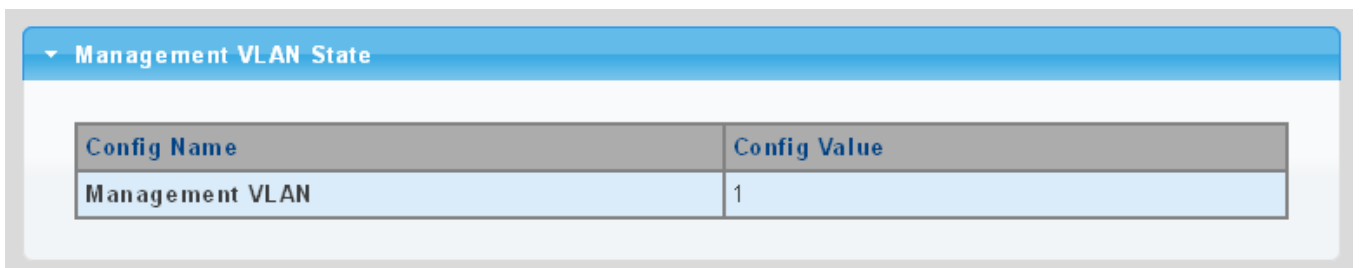
The page includes the following fields:

Object	Description
• Management VLAN	Provide the managed VLAN ID

Buttons



: Click to apply changes.



The screenshot shows a web interface titled "Management VLAN State". It features a blue header bar with the title. Below the header, there is a table with two columns: "Config Name" and "Config Value". The table contains one row with "Management VLAN" in the first column and "1" in the second column.

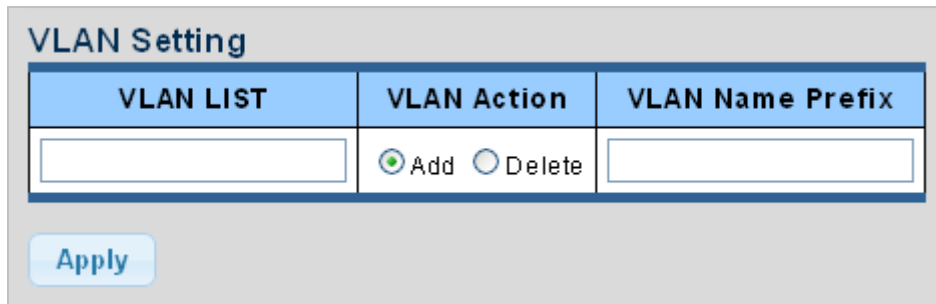
Figure 4-5-2 Management VLAN State Screenshot

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.




The screenshot shows a 'VLAN Setting' form. It contains three main input areas: 'VLAN LIST', 'VLAN Action', and 'VLAN Name Prefix'. The 'VLAN Action' section has radio buttons for 'Add' (selected) and 'Delete'. Below these inputs is an 'Apply' button.

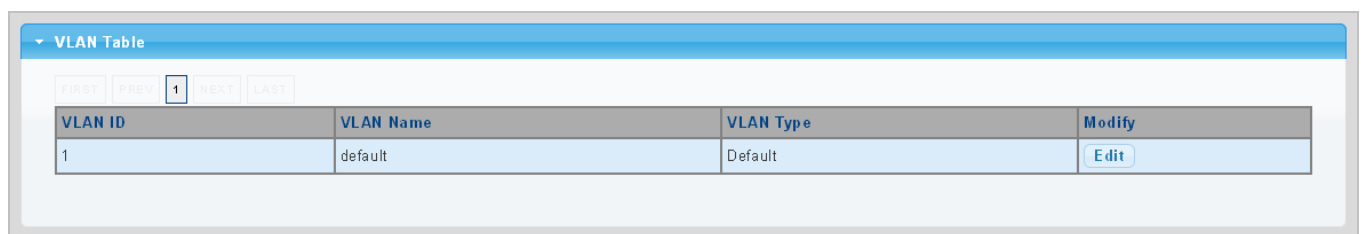
Figure 4-5-3 VLAN Setting Screenshot

The page includes the following fields:

Object	Description
• VLAN List	Indicates the ID of this particular VLAN.
• VLAN Action	This column allows users to add or delete VLAN s.
• VLAN Name Prefix	Indicates the name of this particular VLAN.

Buttons


: Click to apply changes.



The screenshot shows a 'VLAN Table' with a table of VLAN configurations. The table has columns for 'VLAN ID', 'VLAN Name', 'VLAN Type', and 'Modify'. There is one row with 'VLAN ID' 1, 'VLAN Name' 'default', and 'VLAN Type' 'Default'. The 'Modify' column has an 'Edit' button. Above the table are navigation buttons: 'FIRST', 'PREV', '1', 'NEXT', and 'LAST'.

Figure 4-5-4 VLAN Table 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 configuration

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.

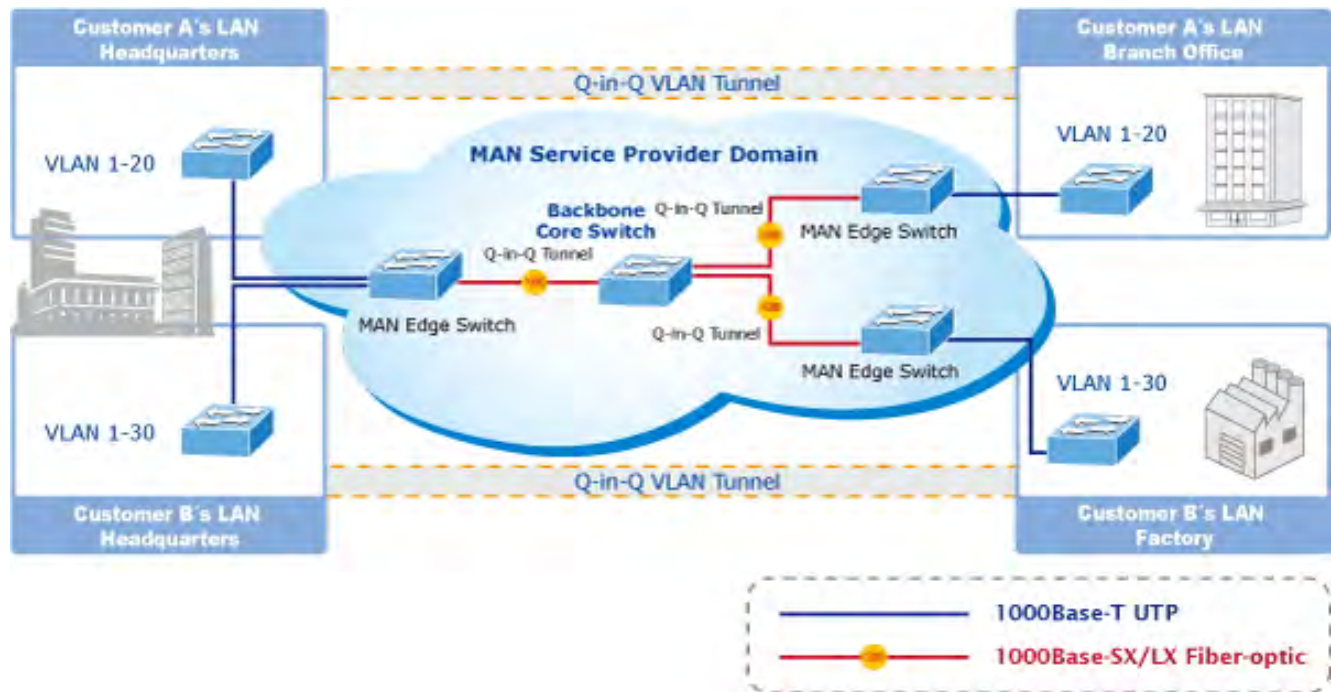
Frame Income Frame Leave	Income Frame is tagged	Income Frame is untagged
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remain untagged

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](#) and [Figure 4-5-6](#) appear.

Port Select	Interface VLAN Mode	PVID	Accepted Type	Ingress Filtering	Uplink	TPID
Select Ports	<input checked="" type="radio"/> Hybrid Tunnel <input type="radio"/> Access <input type="radio"/> Trunk <input type="radio"/>	1 (1 - 4094)	<input checked="" type="radio"/> All Only <input type="radio"/> Tag Only <input type="radio"/> Untag	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	0x8100

Apply

Figure 4-5-5 Edit Interface Setting Screenshot

The page includes the following fields:

Object	Description
• Port Select	Select port number from this drop-down list to set VLAN port setting.
• Interface VLAN Mode	<p>Set the port in access, trunk, hybrid and tunnel mode.</p> <ul style="list-style-type: none"> ■ Trunk means the port allows traffic of multiple VLANs. ■ Access indicates the port belongs to one VLAN only. ■ Hybrid means the port allows the traffic of multi-VLANs to pass in tag or untag mode. ■ Tunnel configures IEEE 802.1Q tunneling for a downlink port to another device within the customer network.
• PVID	<p>Allows you to assign PVID to selected port.</p> <p>The PVID will be inserted into all untagged frames entering the ingress port. The PVID must be the same as the VLAN ID that the port belongs to VLAN group, or the untagged traffic will be dropped.</p> <p>The range for the PVID is 1-4094.</p>
• 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>
• 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.

Buttons



: 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
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

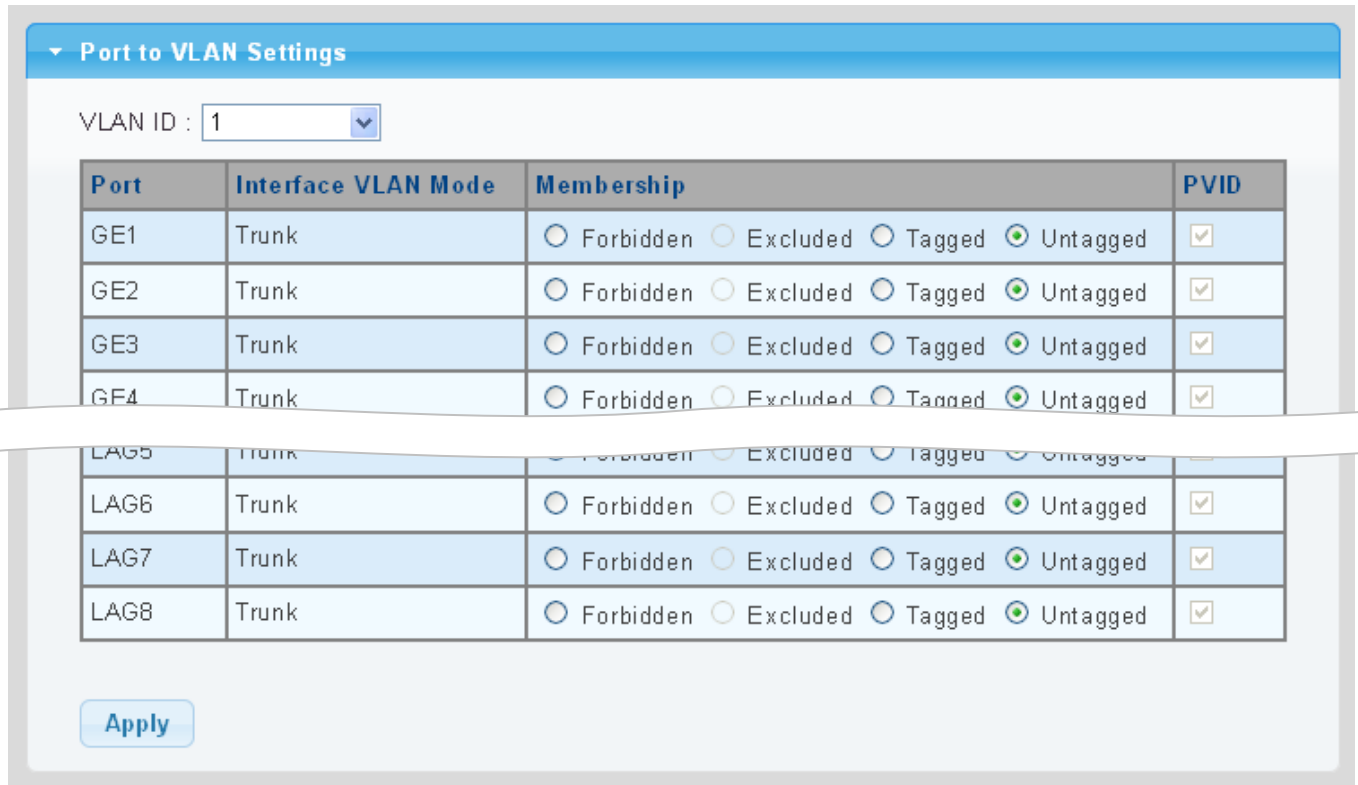
Figure 4-5-6 Edit Interface Setting Screenshot

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 you to add and delete port members of each VLAN. The screen in [Figure 4-5-7](#) appears.



Port to VLAN Settings

VLAN ID : 1

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"/>
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"/>

Apply

Figure 4-5-7 Port to VLAN Setting Screenshot

The page includes the following fields:

Object	Description								
• VLAN ID	Select VLAN ID from 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:								
	<table> <tr> <td>Forbidden:</td><td>Interface is forbidden from automatically joining the VLAN via GVRP.</td></tr> <tr> <td>Excluded:</td><td>Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.</td></tr> <tr> <td>Tagged:</td><td>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.</td></tr> <tr> <td>Untagged:</td><td>Interface is a member of the VLAN. All packets transmitted by the</td></tr> </table>	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
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								

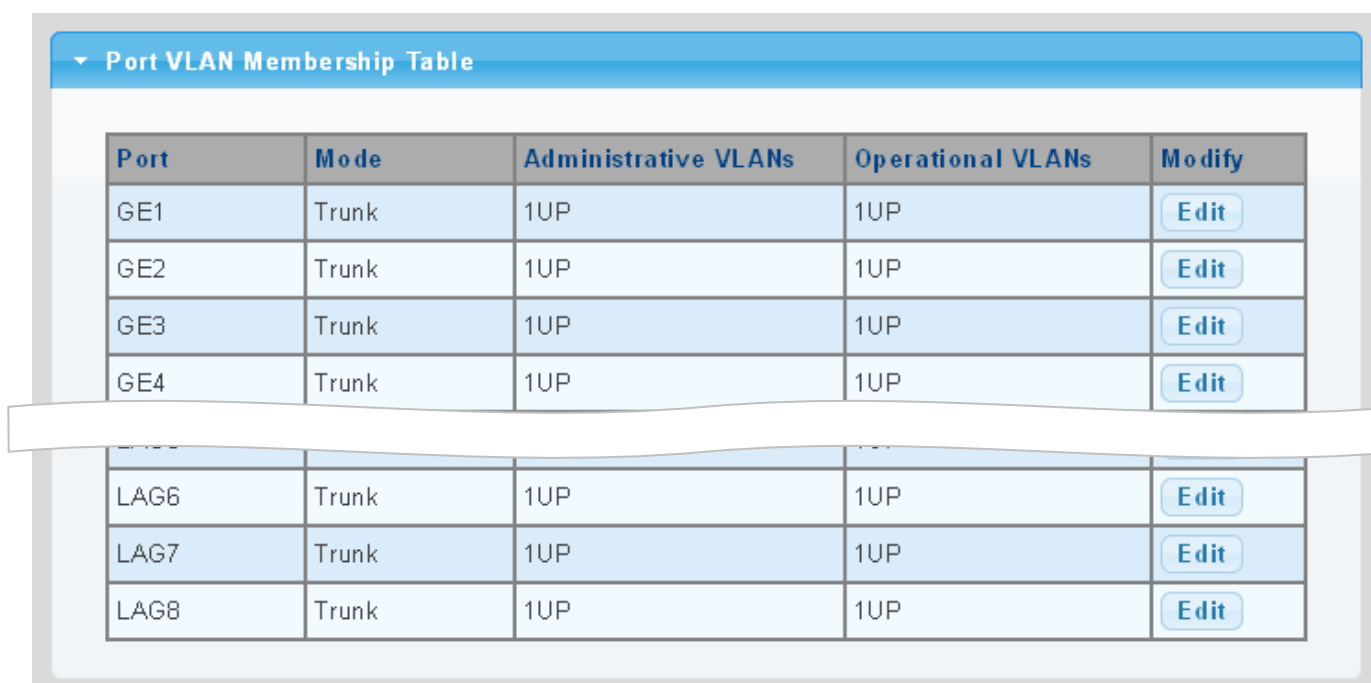
		port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
• PVID	Display the current PVID	

Buttons

Apply: 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 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
LAG6	Trunk	1UP	1UP	Edit
LAG7	Trunk	1UP	1UP	Edit
LAG8	Trunk	1UP	1UP	Edit

Figure 4-5-8 Port VLAN Membership Table 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 you to configure protocol-based VLAN Group Setting. The protocol-based VLAN screens in [Figure 4-5-9](#) and [Figure 4-5-10](#) appear.

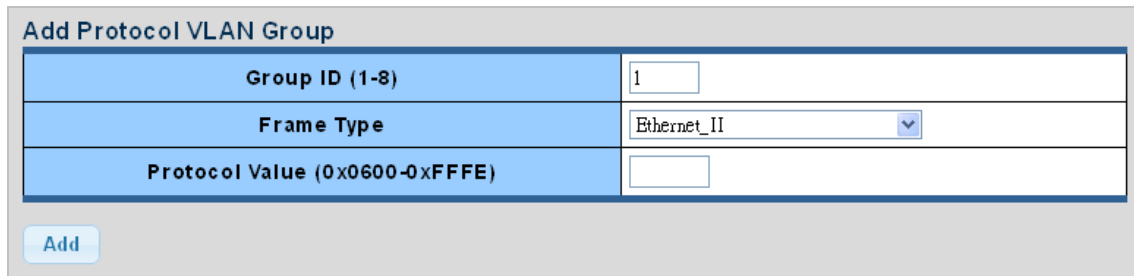



Figure 4-5-9 Add Protocol VLAN Group Screenshot

The page includes the following fields:

Object	Description
• Group ID	Protocol Group ID assigned to the Special Protocol VLAN Group.
• Frame Type	<p>Frame Type can have one of the following values:</p> <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 vary depending on the new frame type you selected.</p>
• Protocol Value (0x0600-0xFFFE)	<p>Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.</p> <p>Valid values for frame type range from 0x0600-0xfffe</p>

Buttons

: Click to apply changes.

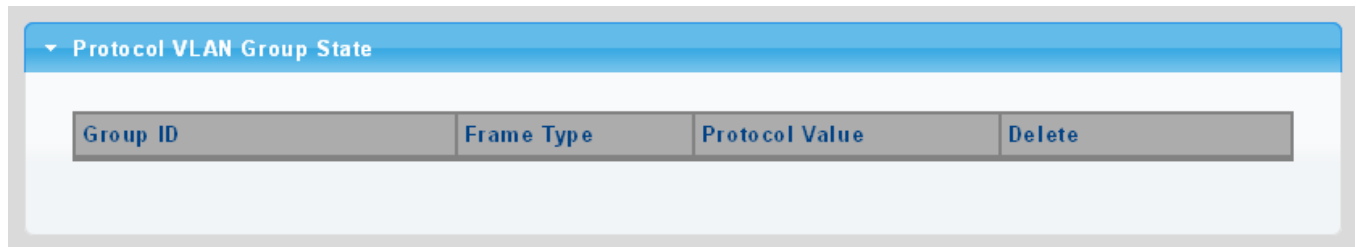



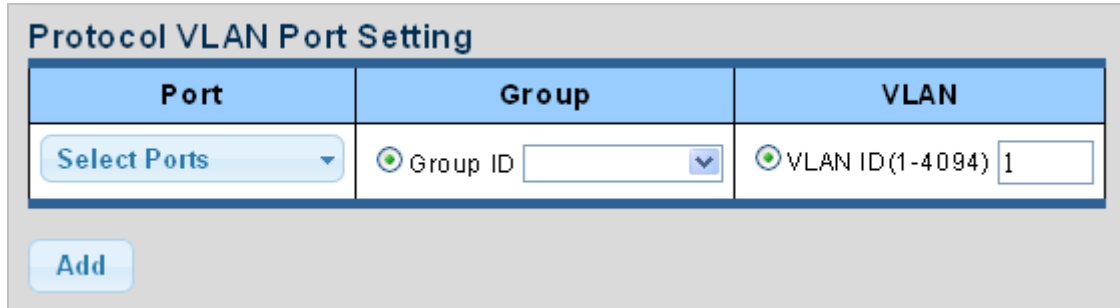
Figure 4-5-10 Protocol VLAN Group State Screenshot

The page includes the following fields:

Object	Description
• Group ID	Display the current group ID
• Frame Type	Display the current frame type
• Protocol Value	Display the current protocol value
• Delete	Click  to delete the group ID entry

4.5.9 Protocol VLAN Port Setting

This page allows you to map an 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.



The screenshot shows a form titled "Protocol VLAN Port Setting". It contains three main input fields: "Port" with a "Select Ports" dropdown, "Group" with a "Group ID" dropdown, and "VLAN" with a "VLAN ID(1-4094)" input field containing the value "1". Below these fields is an "Add" button.

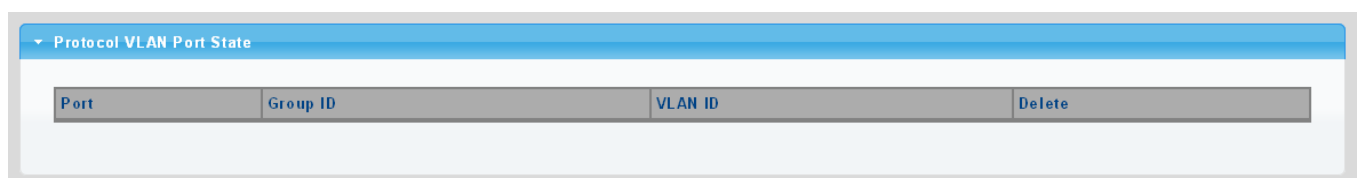
Figure 4-5-11 Protocol VLAN Port Setting Screenshot

The page includes the following fields:

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

Buttons

Add: Click to add protocol VLAN port entry.



The screenshot shows a table titled "Protocol VLAN Port State". The table has four columns: "Port", "Group ID", "VLAN ID", and "Delete".

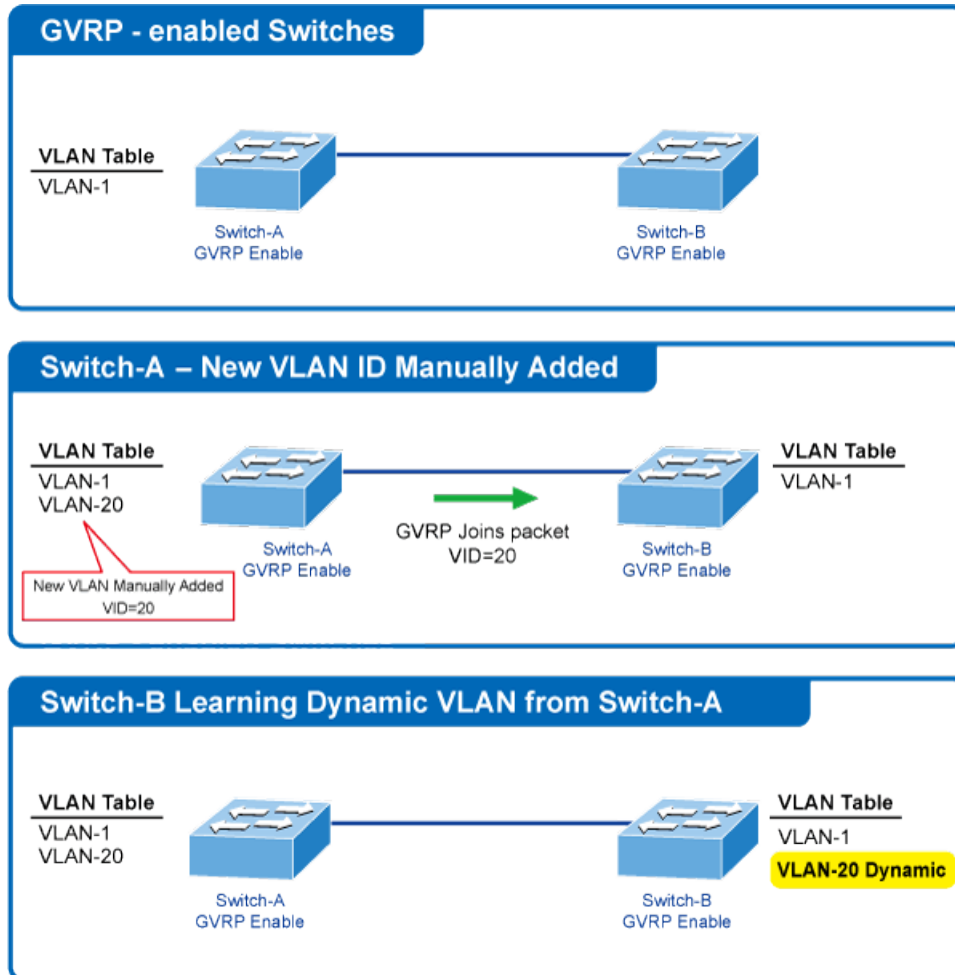
Figure 4-5-12 Protocol VLAN Port State Screenshot

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
• Delete	Click Delete to delete the group ID entry

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.

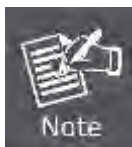
GVRP Global Setting	
GVRP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Join Timeout	<input type="text" value="20"/> (20-16375 centiseconds)
Leave Timeout	<input type="text" value="60"/> (45-32760 centiseconds)
LeaveAll Timeout	<input type="text" value="1000"/> (65-32765 centiseconds)

[Apply](#)

Figure 4-5-13 GVRP Global Setting Screenshot

The page includes the following fields:

Object	Description
• GVRP	Controls whether GVRP is enabled or disabled on this switch.
• Join Timeout	The interval between transmitting requests/queries to participate in a VLAN group. Range: 20-16375 centiseconds Default: 20 centiseconds
• Leave Timeout	The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. Range: 45-32760 centiseconds Default: 60 centiseconds
• LeaveAll Timeout	The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. Range: 65-32765 centiseconds; Default: 1000 centiseconds



Timer settings must follow this rule:

2 x (join timer) < leave timer < leaveAll timer

Buttons



: Click to apply changes.

GVRP Informations	
Information Name	Information Value
GVRP Status	Disabled
Join Timeout	200 millisecond
Leave Timeout	600 millisecond
LeaveAll Timeout	10000 millisecond

Figure 4-5-14 GVRP Global Setting Screenshot

The page includes the following fields:

Object	Description
• GVRP Status	Display the current GVRP status
• Join Timeout	Display the current join timeout parameter
• Leave Timeout	Display the current leave timeout parameter
• 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.

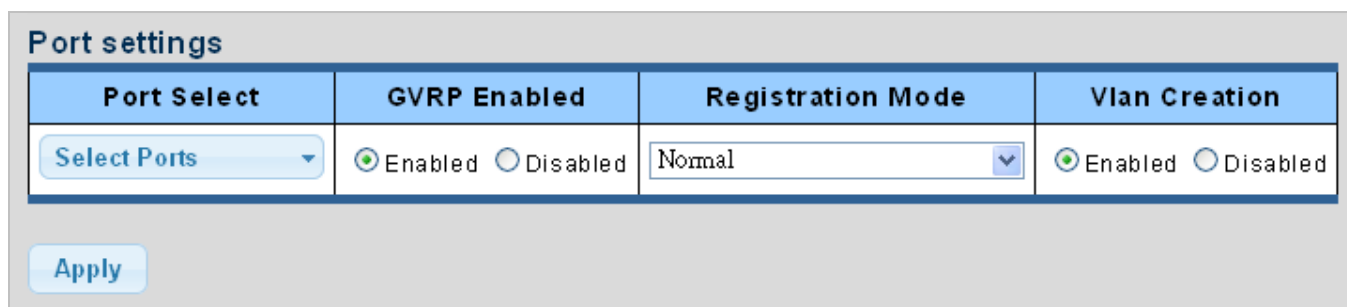


Figure 4-5-15 GVRP Global Setting Screenshot

The page includes the following fields:

Object	Description
• Port Select	Select port from this drop-down list to assign protocol VLAN port
• GVRP Enabled	Controls whether GVRP is enabled or disabled on port
• 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.
• 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.

GVRP Port Status			
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 Screenshot

The page includes the following fields:

Object	Description
• Port	The switch port number of the logical port
• Enable Status	Display the current GVRP port state
• Registration Mode	Display the current registration mode
• VLAN Creation Status	Display the current VLAN creation status

4.5.12 GVRP VLAN

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

GVRP VLAN Database			
VLAN ID	Member Ports	Dynamic Ports	VLAN Type

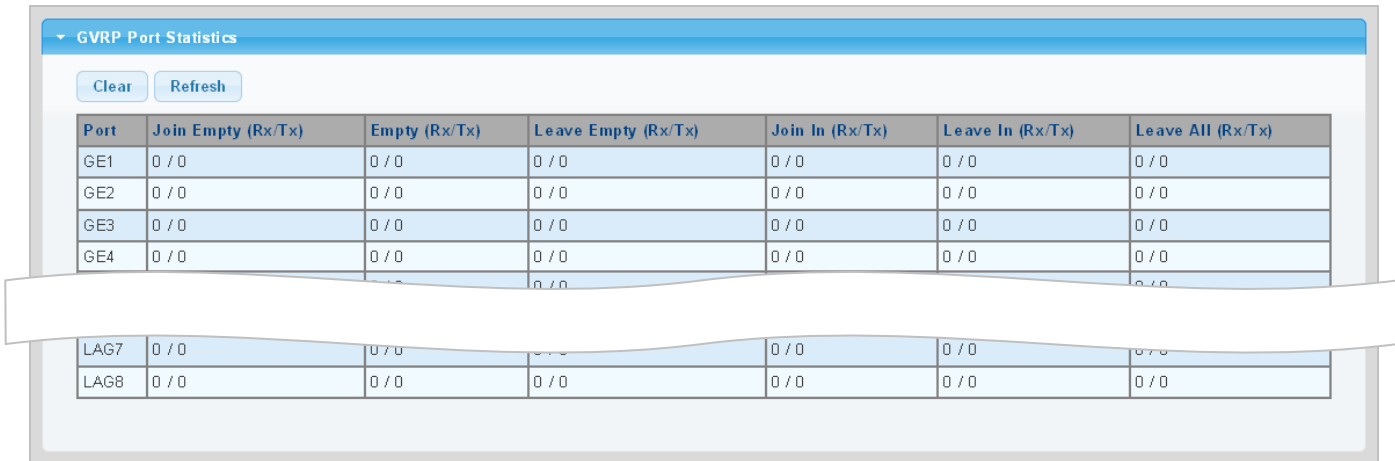
Figure 4-5-17 GVRP VLAN Database Status Screenshot

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.



GVRP Port Statistics						
<input type="button" value="Clear"/> <input type="button" value="Refresh"/>						
Port	Join Empty (Rx/Tx)	Empty (Rx/Tx)	Leave Empty (Rx/Tx)	Join In (Rx/Tx)	Leave In (Rx/Tx)	Leave All (Rx/Tx)
GE1	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
GE2	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
GE3	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
GE4	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
LAG7	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
LAG8	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0

Figure 4-5-18 GVRP Port Statistics 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

GVRP Port Error Statistics					
<div> <div>Clear</div> <div>Refresh</div> </div>					
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 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 handles Tagged and Untagged traffic flow for two VLANs. VLAN Group 2 and VLAN Group 3 are separated VLANs. Each VLAN isolates network traffic so only members of the VLAN receive traffic from the same VLAN members. The screen in [Figure 4-5-20](#) appears and [Table 4-5-2](#) describes the port configuration of the Managed Switches.

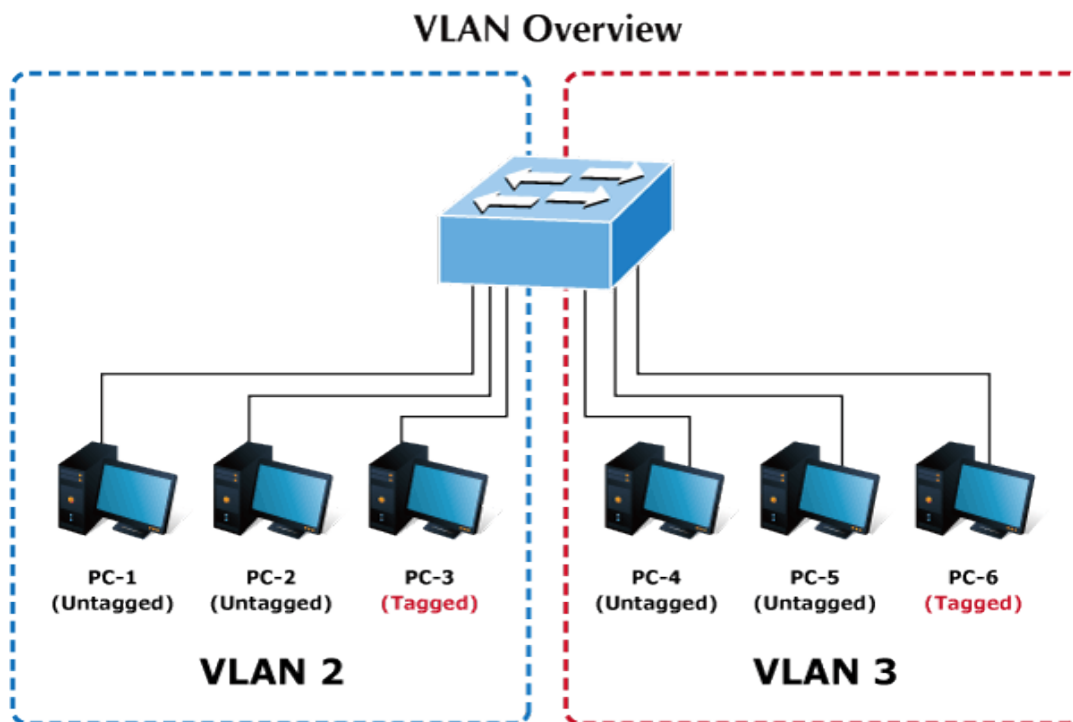


Figure 4-5-20 Two Separate VLAN Diagrams

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 is described as follows:

■ Untagged packet entering VLAN 2

1. When **PC-1** transmits an **untagged** packet entering **Port-1**, the Managed Switch will tag it with a **VLAN Tag=2**. **PC-2** and **PC-3** will receive the packet through **Port-2** and **Port-3**.
2. PC-4, PC-5 and PC-6 will receive no packet.

3. When the packet leaves **Port-2**, it will be stripped away by its tag becoming an **untagged** packet.
4. When the packet leaves **Port-3**, it will be kept as a **tagged** packet with **VLAN Tag=2**.

■ Tagged packet entering VLAN 2

1. When **PC-3** transmits a **tagged** packet with **VLAN Tag=2** entering **Port-3**, **PC-1** and **PC-2** will receive the packet through **Port-1** and **Port-2**.
2. When the packet leaves **Port-1** and **Port-2**, it will be stripped away by its tag becoming an **untagged** packet.

■ Untagged packet entering VLAN 3

1. When **PC-4** transmits an **untagged** packet entering **Port-4**, the switch will tag it with a **VLAN Tag=3**. **PC-5** and **PC-6** will receive the packet through **Port-5** and **Port-6**.
2. When the packet leaves **Port-5**, it will be stripped away by its tag becoming an **untagged** packet.
3. When the packet leaves **Port-6**, it will be kept as a **tagged** packet with **VLAN Tag=3**.



Note

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		
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 to 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 to each port:

VLAN ID = 2:

Port-1 and 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 and 5 = Untagged,

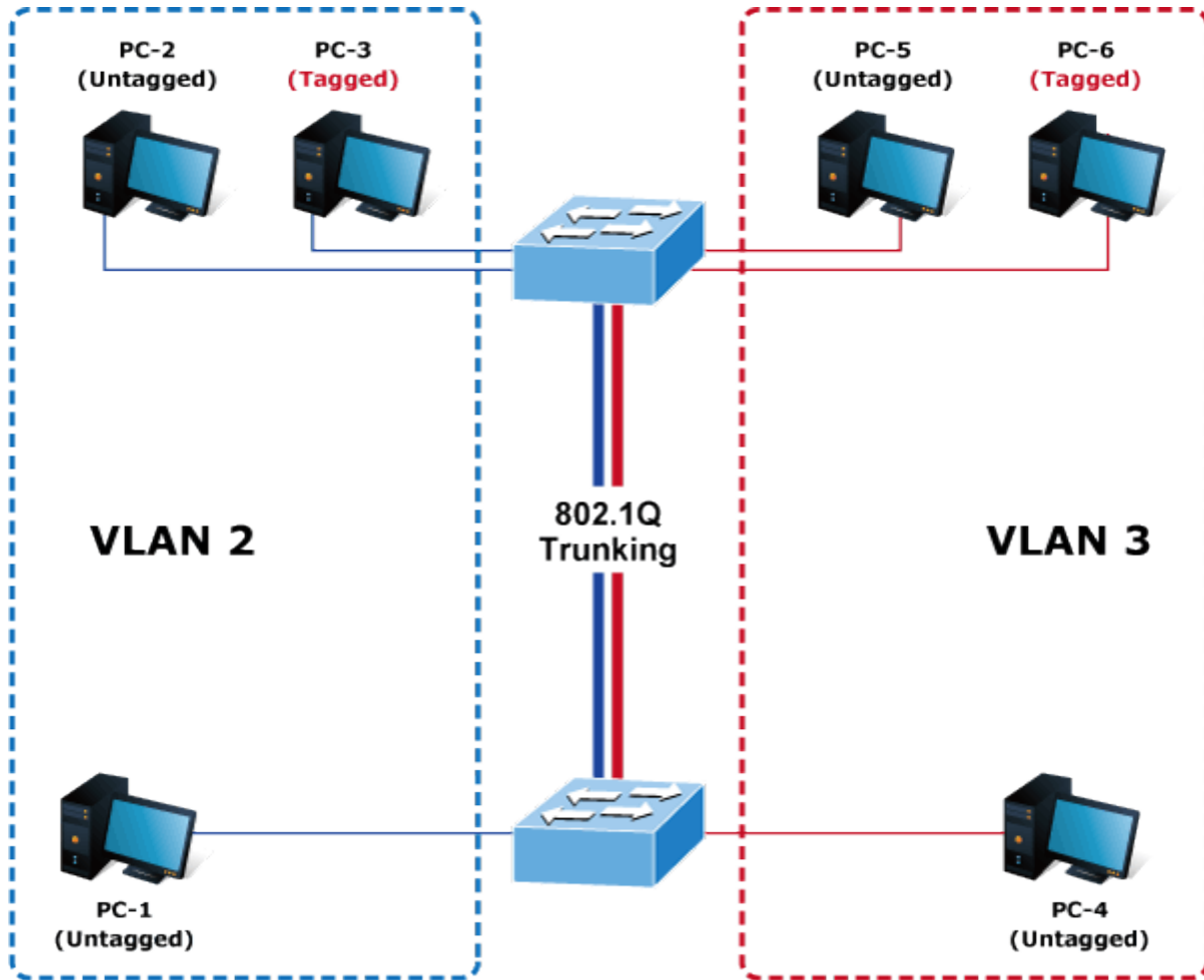
Port -6 = Tagged,

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 switches

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



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 to 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 to 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 and 2 = Untagged,

Port-3 and 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 and 5 = Untagged,

Port -6 and 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"/>