

OPERATING MANUAL

GSM2108 and GSM1008-2SFP



CORPORATE HEADQUARTERS

5001 American Blvd. W., Suite 605
Bloomington, MN 55437
Phone: 800.441.5319
Phone: 952.831.5603
Fax: 952.831.5605

MANUFACTURING/CUSTOMER SERVICE

945 37th Avenue, NW
Rochester, MN 55901
Phone: 800.328.2275
Phone: 507.252.1951
Fax: 507.285.1952

Web site: <http://www.watersnet.com>

TABLE OF CONTENTS

1.0	SPECIFICATIONS	4
2.0	PACKAGE CONTENTS.....	6
3.0	INTRODUCTION.....	6
3.1	HARDWARE FEATURES	6
3.2	SOFTWARE FEATURES.....	7
3.3	HARDWARE DESCRIPTION.....	8
3.4	REAR PANEL	9
3.5	OPTIONAL SFP MODULES	9
3.6	INSTALLATION.....	10
3.7	OPTIONAL SFP MODULES	10
3.8	POWER ON.....	10
3.9	SWITCH TOPOLOGY.....	10
4.0	NETWORK APPLICATIONS	13
4.1	USING THE RS-232 SERIAL PORT CONNECTION	13
4.2	CONFIGURING IP, SUBNET MASK AND DEFAULT GATEWAY.....	14
4.3	CONFIGURING THE SWITCH VIA THE WEB.....	15
4.4	IP ADDRESS ASSIGNMENT	16
4.4	IP ADDRESS ASSIGNMENT	16
5.0	WEB BASED MANAGEMENT	21
5.1	OVERVIEW OF WEB MANAGEMENT.....	22
5.2	SYSTEM INFORMATION.....	25
5.3	IP CONFIGURATION	26
5.4	TIME CONFIGURATION	28
5.5	ACCOUNT CONFIGURATION.....	30
5.6	MANAGEMENT POLICY.....	30
5.7	VIRTUAL STACK.....	33
5.8	PORT CONFIGURATION	35
5.8.1	PORT STATUS	35
5.8.2	PORT CONFIGURATION	38
5.8.3	SIMPLE COUNTER	39
5.8.4	DETAIL COUNTER	40
5.9	MIRROR CONFIGURATION	44
5.10	BANDWIDTH MANAGEMENT.....	44
5.11	QoS (QUALITY OF SERVICE) CONFIGURATION	46
5.12	SNMP CONFIGURATION	52
5.13	IGMP SNOOPING	54
5.14	MAXIMUM PACKET LENGTH.....	55
5.15	DHCP BOOT	55
5.16	VLANs.....	56
5.16.1	VLAN MODE	56
5.16.2	TAG-BASED GROUP.....	58
5.16.3	PORT-BASED GROUP.....	60
5.16.4	TAG RULE	62
5.17	MAC TABLE	63
5.18	GVRP CONFIGURATION.....	69
5.19	SPANNING TREE CONFIGURATION (STP) CONFIGURATION.....	73
5.19.1	STP STATUS	73
5.19.2	STP CONFIGURATION	75
5.19.3	STP PORT CONFIGURATION	76

5.20	TRUNKING CONFIGURATION	78
5.21	802.1X CONFIGURATION	83
5.22	ALARM CONFIGURATION	91
5.23	CONFIGURATION	93
5.23.1	SAVE/RESTORE	94
5.23.2	RESTORE DEFAULT	95
5.23.3	CONFIGURATION FILE	96
5.24	DIAGNOSTICS.....	97
5.25	TFTP SERVER	99
5.26	LOG DATA	100
5.27	FIRMWARE UPGRADE	101
5.28	REBOOT	102
5.29	LOGOUT	103
6.0	OPERATION OF CLI MANAGEMENT	104
6.1	LOGIN.....	104
6.2	COMMANDS OF CLI	105
7.0	MAINTENANCE.....	124
7.1	EXAMPLES	124
8.0	TROUBLESHOOTING.....	125
8.1	BEFORE CALLING FOR ASSISTANCE.....	125
8.2	RETURN MATERIAL AUTHORIZATION (RMA) PROCEDURE	126
8.3	SHIPPING AND PACKAGING INFORMATION.....	126
9.0	WARRANTY	128

1.0 Specifications

OPERATIONAL CHARACTERISTICS

MAC Address Table

8K

Switching Mode

Store-and-forward

Memory Buffer Size

144KB

Jumbo frame support

Performance

Non-blocking wire speed

Auto negotiation

Auto-MDIX

Back pressure flow control for half duplex

Flow control for full duplex

MANAGEMENT FUNCTIONS

Web-based, SNMP (v1, v2c), CLI, or Telnet

Port setting for duplex and speed

Port trunking (4 groups)

Port based and tagged VLANs (up to 256)

IGMP snooping

802.1x access control

GVRP/GARP

Port mirroring

Broadcast storm suppression

QoS

LACP

STP/RSTP

Enterprise MIB

RMON

NETWORK STANDARDS:

IEEE 802.3

IEEE 802.3u

IEEE 802.3ab

IEEE 802.3z

IEEE 802.3x

IEEE 802.1q

IEEE 802.1p

IEEE 802.1d/w

IEEE 802.1x

IEEE 802.3ad

EMI/SAFETY COMPLIANCE:

FCC Part 15 Class A & CE Mark Approval

NETWORK CABLE CONNECTORS (All Models):

RJ45 shielded female ports
10/100Mbps: CAT5 UTP or better
MM or SM with LC connectors

POWER SUPPLY:

Internal power supply
Input Voltage
100 to 240 VAC, 50 to 60Hz
Power Consumption
30 watts maximum

OPERATING ENVIRONMENT

Ambient Temperature:
32° to 122°F (0° to 50°C)
Ambient Humidity
0% to 90%

MECHANICAL:

Enclosure:
Rack mountable
Cooling Method: Fan cooled

PHYSICAL CHARACTERISTICS

Dimensions: GSM2108
5.2 x 8.54 x 1.73 in
132 x 217 x 44 mm
Dimensions: GSM1008-2SFP
4.72 x 7.56 x 1.38 in
120 x 192.35 mm

Weight: GSM2108
2.43lbs (1.1kg)
Weight: GSM1008-2SFP
1.75lbs (.79kg)

WARRANTY:

Limited Lifetime Made in USA

2.0 Package Contents

Examine the shipping container for obvious damage prior to installing this product. Notify the carrier of any damage that you believe occurred during shipment. Ensure that the items listed below are included. If an item is missing, please contact your supplier.

- 8 port 10/100/1000 Ethernet switch
- Modules (optional)
- Mounting Accessory for (19" rack shelf)
- User's manual
- AC power cord
- RS-232 Cable

3.0 Introduction

The Waters' GSM switch is an eight port managed switch which meets all IEEE802.3/u/x/z specifications. The switch has eight 10/100/1000Mbps ports and two SFP fiber slots. The switch can be managed through RS-232 serial port via direct connection or through an Ethernet port using CLI or Web-based management unit, associated with SNMP agent. With the SNMP agent, the network administrator can logon the switch to monitor, configure and control each port's activity through easy to use menu options. The switch features comprehensive and useful functions such as QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP/RMON, IGMP Snooping capability via the intelligent software. The switch is suitable for both metro-LAN and office applications.

Ports 7 and 8 provide two types of media --- copper and fiber. Ports 7 and 8 support either 10/100/1000Base-TX or 1000Base-SX auto-detected function.

For upgrading firmware, please refer to the Section 5.27 for more details. The switch will not stop operating while upgrading firmware and upon completion, the configuration is unchanged.

3.1 Hardware Features

The GSM switch provides the comprehensive features listed below for users to perform network administration functions efficiently and provide maximum network security.

- Conforms to IEEE 802.3, 802.3u, 802.3x, and 802.3ab and 802.3z
- Eight auto sensing 10/100/1000 ports
- Two 10/100/1000Mbps TP or 1000Mbps SFP Fiber dual media auto sense
- 144KB on-chip frame buffer
- Jumbo frame support
- Programmable classifier for QoS (Layer 4/Multimedia)
- 8K MAC address and 4K VLAN support (IEEE802.1Q)
- Per-port shaping, policing, and broadcast storm control
- IEEE802.1Q-in-Q nested VLAN support
- Full-duplex flow control (IEEE802.3x) and half-duplex backpressure
- Supports online plug/unplug of SFP modules
- Extensive front-panel diagnostic LEDs; System: Power, TP Port1-8: LINK/ACT, 10/100/1000Mbps, SFP Port 7, 8: SFP(LINK/ACT)

3.2 Software Features

The following lists management highlights of the GSM switch:

- Supports per port traffic counters
- Provides the status of each port and allows for port configuration
- Supports per port traffic monitoring counters
- Supports a snapshot of the system information upon login
- Supports static trunk function
- Three user login
- Maximum packet length can be up to 9216 bytes for jumbo frame application
- Supports DHCP broadcasting suppression
- Supports QoS for real time applications based on the information taken from layer 2 to layer 4 such as VoIP
- Supports port mirror function with ingress traffic
- Supports rapid spanning tree
- Supports 802.1x port security
- SNMP access can be disabled to prevent illegal SNMP access
- Trap event and alarm message can be transferred via email and mobile phone short message
- Supports network time synchronization and daylight saving
- Supports 120 event log records in the main memory and display on the local console

3.3 Hardware Description



Figure 3.1 GSM-2108 Switch

There are eight 10/100/1000 copper and two SFP fiber ports for optional removable modules on the front panel of the switch. The LEDs, located on the left side of the front panel, contains a power LED indicating the power status and the status of the eight working ports on the switch.

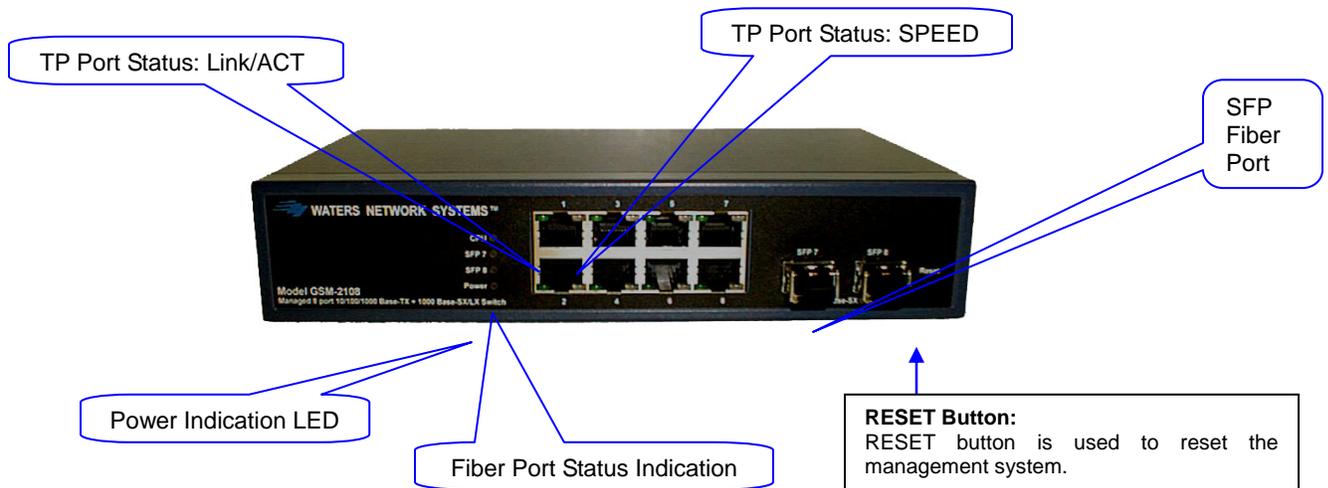


Figure 3.2 - Front view of GSM-2108 switch

The following table provides the status and description of the LEDs:

LED	Color	Function
System LED		
POWER	Green	Lit when +5V DC power is on and good
CPU LED	Green	Blinks when CPU is active
10/100/1000Ethernet TP Port 1 to 8 LED		
LINK/ACT	Green	Lit when connection with remote device is good Blinks when any traffic is present Off when cable connection is not good
10/100/1000Mbps	Green/ Amber	Lit green when 1000Mbps speed is active Lit amber when 100Mbps speed is active Off when 10Mbps speed is active
1000SX/LX Gigabit Fiber Port 7, 8 LED		
SFP(LINK/ACT)	Green	Lit when connection with the remote device is good Blinks when any traffic is present Off when module connection is not good

Table 3-1

3.4 Rear Panel

Located on the rear panel is the RS-232 DB-9 interface which is used for switch management configuration.



Figure 3.3 - Rear View of GSM-2108

3.5 Optional SFP Modules

If the SFP modules are installed, ports 7 and 8 can no longer be used for 10/100/1000 copper connection. The following lists the SFP modules that are available for the GSM2108 and GSM1008-2SFP switches:

- SFP-1000SX-LC – multimode fiber transceiver with LC connector
- SFP-1000LX-LC-10 – singlemode (10km) fiber transceiver with LC connector
- SFP-1000LX-LC-30 – singlemode (30km) fiber transceiver with LC connector

3.6 Installation

Choose a surface for your switch that is clean, smooth and near a power outlet. Make sure that there is enough clearance around the switch to allow attachment of cables, power cord and air circulation.

1. Plug in the power cord into the switch.
2. Install the proper cable for network connection.
3. Plug the power cord into the power source.

3.7 Optional SFP Modules

The SFP modules are hot swappable, so you can plug or unplug the modules before and after the switch is turned on. If you are installing the optional SFP fiber transceivers, follow these guidelines:

1. Verify that the SFP module is the correct module and conforms to the chassis.
2. Slide the module along the slot.
3. Seat the module against the slot socket/connector.
4. Install the proper cable for network connection.

3.8 Power On

Once the switch is on, the bootloader loads the firmware into the memory. It will take about 30 seconds. Once the firmware is loaded, the switch will flash all of the LEDs once and automatically perform a self test.

3.9 Switch Topology

Theoretically, the switch partitions the collision domain for each port so you may link switches without limitations. However, network extension (cascading levels & overall diameter) must follow IEEE 802.3/802.3u/802.3z and other 802.1 series protocol specifications, in which the limitations are the timing requirement from physical signals defined by 802.3 series specification of Media Access Control (MAC) and PHY, and layer 2 protocols such as 802.1d, 802.1q, and LACP.

The following table describes the cable and devices' bit-time delay (round trip):

1000Base-X TP, Fiber		100Base-TX TP		100Base-FX Fiber	
Round trip Delay: 4096		Round trip Delay: 512			
CAT5	11.12/m	CAT5	1.12/m	Fiber Cable:	1.0/m
Fiber	10.10/m	TP to fiber converter: 56			
Bit time unit: 1ns (1sec./1000 Mega bit)		Bit time unit: 0.01 μ s (1sec./100 Mega bit)			

Table 3-2

Sum up all elements' bit-time delay and the overall bit-time delay of wires/devices must be within Round Trip Delay (bit times) in a half-duplex network segment (collision domain). This will not be applied for full duplex operation. You may use the TP-Fiber module to extend the TP node distance over fiber optic and provide the long haul connection.

A hierarchical network with minimum levels of switching may reduce the timing delay between server and client station. Basically, with this approach, it will minimize the number of switches in any one path; will lower the possibility of network loop and will improve network efficiency. If more than two switches are connected in the same network, select one switch as Level 1 switch and connect all other switches to it at Level 2. It is recommended to connect the Server/Host to the Level 1 switch. This generally applies if no VLAN or other special requirements are applied.

Example 1: All switch ports are in the same local area network. All ports can access each other (See Figure 2-2).

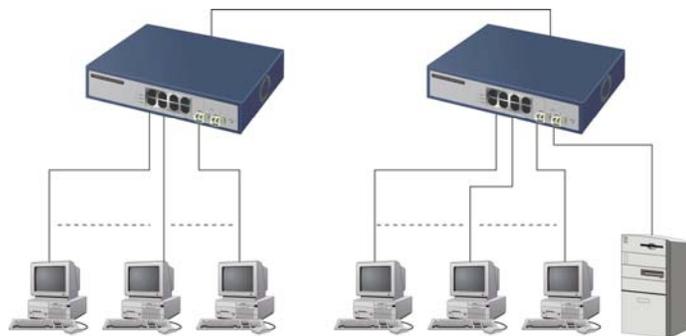


Figure 3.4 - No VLAN Configuration Diagram

If VLAN is enabled and configured, each node in the network that can communicate with each other directly is contained in the same VLAN area.

In Example 2, the VLAN area is defined by the configured VLAN. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical locations. The following diagram shows how the VLAN works.

Example 2a: Port-based VLAN (See Figure3-5).

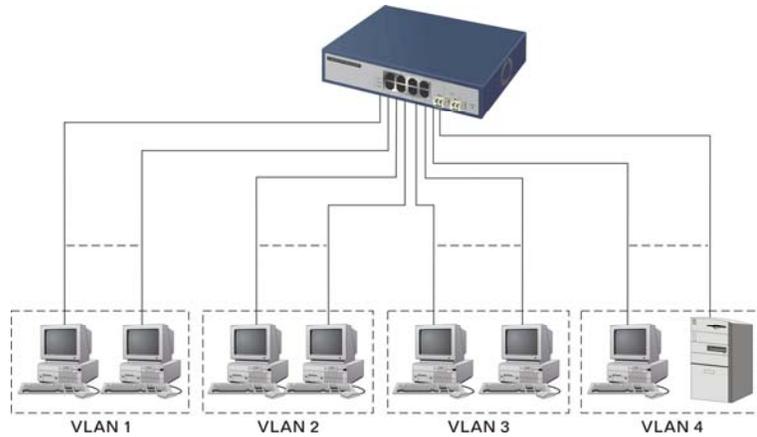


Figure 3-5 - Port-based VLAN Diagram

1. As a member of a VLAN, you cannot be a member of a VLAN in another switch.
2. As a member of a VLAN, you cannot access a member of another VLAN.
3. The switch manager has to assign different names for each VLAN group at one switch.

Case 2b: Port-based VLAN (See Figure3-6).

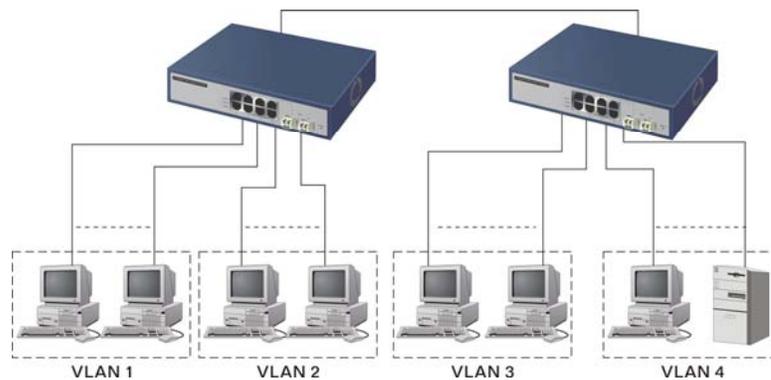


Figure 3-6 - Port-based VLAN Diagram

This is an example of how VLANs can be set up between two switches.

1. VLAN1 members cannot access VLAN2, VLAN3 and VLAN4 members.
2. VLAN2 members cannot access VLAN1 and VLAN3 members, but they can access VLAN4 members.
3. VLAN3 members cannot access VLAN1, VLAN2 and VLAN4.
4. VLAN4 members cannot access VLAN1 and VLAN3 members, but they can access VLAN2 members.

Example 3a: The same VLAN members can be at different switches with the same VID (See Figure 2-5).

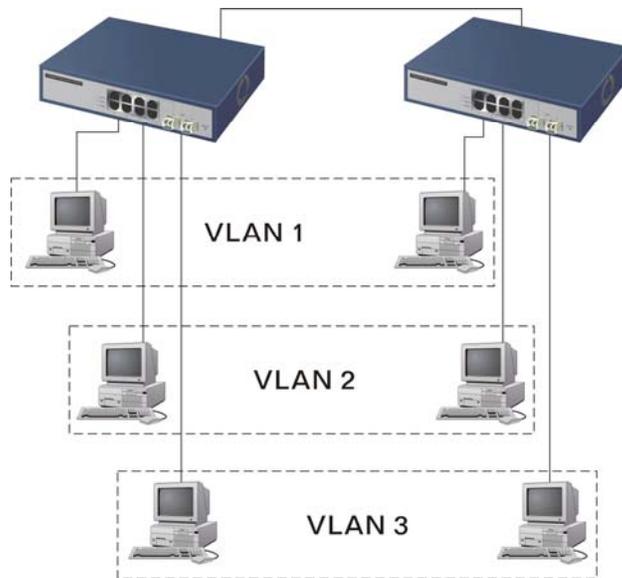


Figure 3.7 - Attribute-based VLAN Diagram

4.0 Network Applications

There are three ways to access switch management functions:

1. RS-232 serial port connection (CLI)
2. Telnet
3. Web

Note: Before accessing management functions through Telnet or the Web, you must modify the IP address, subnet mask, default gateway and DNS through the RS-232 connection.

4.1 Using the RS-232 Serial Port Connection

To configure the switch via the RS-232 serial port connection, follow these steps:

1. Connect the serial cable included with your switch to your workstation.
2. Connect the serial cable to console connector on the back of your switch.
3. Run the terminal emulator (Example: HyperTerminal) using the following settings.
 - a. Baud rate (bits per second): **57600**
 - b. Data bits: **8**
 - c. Parity: **N**
 - d. Stop bits: **1**
 - e. Flow control: **None**
4. When you complete the connection, press the **Enter** key.
5. Turn on the switch.
6. The default login is:
 - a. Username = **admin**
 - b. Password = **admin**

4.2 Configuring IP, Subnet Mask and Default Gateway

The default settings for your switch are listed in the following table:

Default Value	GSM2108/GSM1008
IP Address	192.168.1.1
Subnet	255.255.255.0
Default Gateway	192.168.1.254

Table 4-1

You may either change the IP address of the switch or change the IP address of your workstation. To change the IP address of the switch, via the console connection, you will have to use the CLI command listed below. A complete list of CLI commands is in Section 6.0 of this manual.

1. Once you have logged into the switch, you will see the following screen.

```
L2 Managed Switch - GEL2-SW8
Login: admin
Password:
GEL2-SW8# █
```

Figure 4.1 – Login Screen

2. To set the IP Address of the switch, use the following commands:

Syntax:

set ip <ip> <mask> <gateway>

Description:

To set the system IP address, subnet mask and gateway.

Argument:

<ip> : ip address

<mask> : subnet mask

<gateway> : default gateway

Possible value:

<ip> : 192.168.1.2 or others

<mask> : 255.255.255.0 or others

<gateway> : 192.168.1.253 or others

Example:

GEL2-SW8(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253

Once you have set the IP address of the switch, you must save the configuration. The CLI command is: **save start**.

A detailed list of CLI commands can be found in Section 6.0.

4.3 Configuring the Switch via the Web

You can configure and monitor the switch through:

- CLI
- Web browser
- SNMP manager. The user interface for SNMP is not covered at this time.

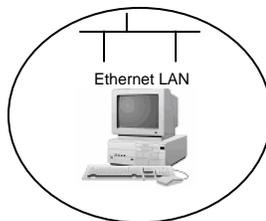


Assign an IP address,
For example:
IP = 192.168.1.100
Subnet Mask = 255.255.255.0
Default Gateway = 192.168.1.254

Figure 4.2 – Front View

Before you are able to communicate the IP address of the switch. Once these instructions:

1. Connect the switch with a UTP
Note: If the workstation connects setup the same subnet mask
2. Access your web browser or use the console connection.



with the switch, you must know you know the IP address, follow cable to your workstations. to the switch, you will have to between them.

Note: If you make changes to the configuration, you must **save** the configuration before rebooting the switch.

4.4 IP Address Assignment



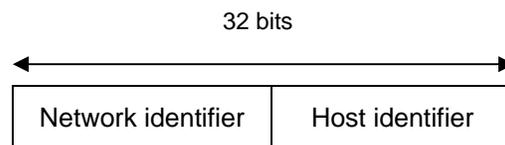
Figure. 4-3 - Login Screen via a Web browser

For IP address configuration, the following three parameters are required:

- IP address
- Subnet Mask
- Default Gateway and DNS.

IP Address:

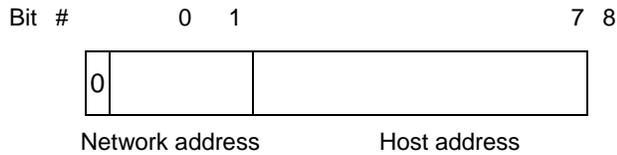
The address of the network device is used for internetworking communication. IP addresses are split into predefined address classes or categories. This is referred to as “classful” addressing because the address is split into three predefined classes, groupings or categories. Each IP address comprises two parts: network identifier (address) and host identifier (address). The network identifier identifies the network on which the host resides, while the host identifier identifies the particular host on the given network. The host identifier must be unique in the same LAN. Each class has its own network range between the network identifier and host identifier in the 32 bits address. IP address is known as IPv4.



With “classful” addressing, the IP address is divided into three classes: class A, class B and class C. The rest of IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. Each class has its address range described below.

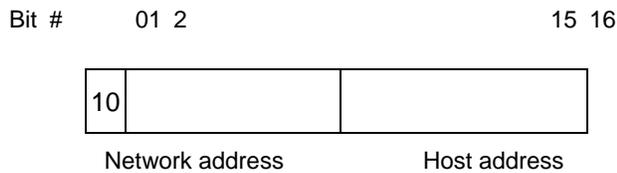
Class A:

Address is less than 126.255.255.255. There are a total of 126 networks can be defined because the address 0.0.0.0 is reserved for default route and 127.0.0.0/8 is reserved for loopback function.



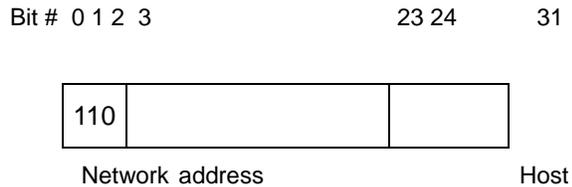
Class B:

IP address range between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed 16-bit host address. There are 16,384 (2^{14})/16 networks able to be defined with a maximum of 65534 ($2^{16} - 2$) hosts per network.



Class C:

IP address range between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed 8-bit host address. There are 2,097,152 (2^{21})/24 networks able to be defined with a maximum of 254 ($2^8 - 2$) hosts per network.



Class D and E:

Class D is a class with first 4 MSB (most significance bit) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to IANA (internet assigned numbers authority), there are three specific IP address blocks reserved and able to be used for extending internal networks. This is referred to as Private IP address and listed below:

Class A	10.0.0.0 --- 10.255.255.255
Class B	172.16.0.0 --- 172.31.255.255
Class C	192.168.0.0 --- 192.168.255.255

Please refer to RFC 1597 and RFC 1466 for more information.

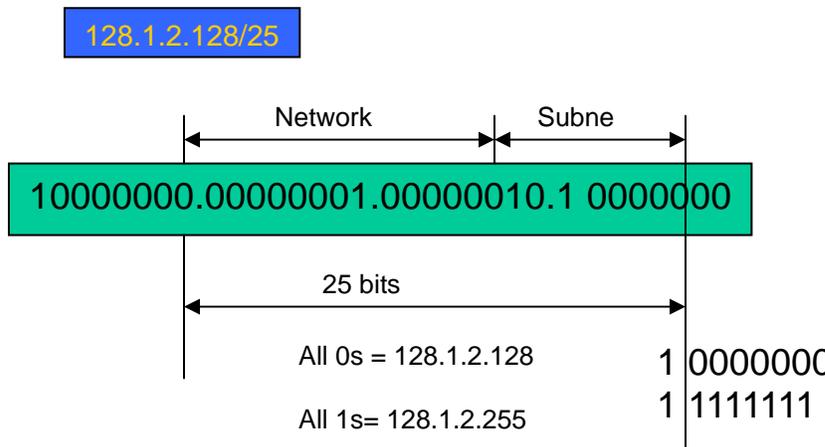
Subnet mask:

Subnet mask is the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address to the network prefix and the host address in bitwise basis. It is designed to utilize the IP address more efficiently and make it easier to manage IP

networks.

For a class B network, 128.1.2.3, the subnet mask 255.255.0.0 in default, in which the first two bytes are all 1s. This means more than 60 thousands of nodes in flat IP address will be at the same network. This is too large to manage practically. Now if we divide it into a smaller network by extending network prefix from 16 bits to, say 24 bits, its third byte is used to subnet this class B network. Now it has a subnet mask 255.255.255.0, in which each bit of the first three bytes is 1. It's now clear that the first two bytes is used to identify the class B network, the third byte is used to identify the subnet within this class B network and, of course, the last byte is the host number.

Not all IP addresses are available in the sub-netted network. Two special addresses are reserved. They are the addresses with all zero's and all one's. For example, an IP address 128.1.2.128, what will the reserved IP address look like? All 0s mean the network itself, and all 1s mean IP broadcast.



In this diagram, the subnet mask with 25-bit long, 255.255.255.128, contains 126 members in the sub-netted network. The length of network prefix equals the number of the bit with 1s in that subnet mask. With this, you can easily count the number of IP addresses matched. The following table shows the result.

Prefix Length	No. of IP matched	No. of Addressable IP
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

Table 4-2

According to the scheme above, a subnet mask 255.255.255.0 will partition a network with the class C. This means there will be a maximum of 254 effective nodes existing in this sub-netted network and is considered a physical network in an autonomous network. It owns a network IP address which may look like 168.1.2.0.

With the subnet mask, a bigger network can be divided into smaller pieces. If you want to have more than two independent networks in a LAN, the network must be partitioned. The subnet mask must be applied.

For different network applications, the subnet mask may look like 255.255.255.240. This means it is a small network accommodating a maximum of 15 nodes in the network.

Default Gateway:

For the routed packets, if the destination is not in the routing table, all traffic is put into the device with the designated IP address, known as default router. Basically, it is a routing policy. The gateway setting is used for Trap Events Host only in the switch.

For assigning an IP address to the switch, check the IP address of the network that will be connected to the switch. Use the same network address and append your host address.

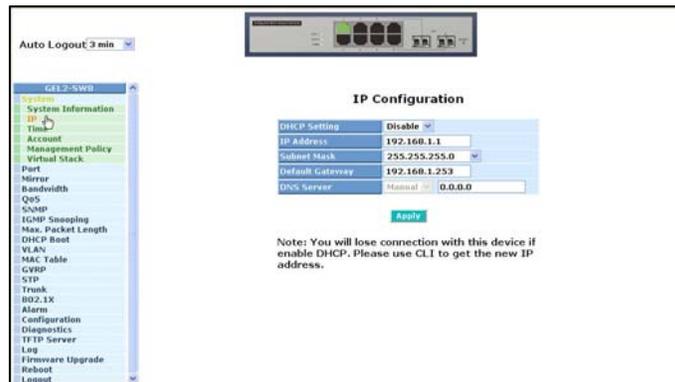


Figure 4.4 – IP Configuration

First, IP Address: as shown in the Figure 4.4, enter **192.168.1.1**, for example. An IP address such as 192.168.1.x must be set on your PC.

Second, Subnet Mask: as shown in the Figure 4.4, enter **255.255.255.0**. Any subnet mask such as 255.255.255.x is allowable in this case.

DNS:

The Domain Name Server translates the human readable machine name to IP address. Every machine on the Internet has a unique IP address. A server generally has a static IP address. To connect to a server, the client needs to know the IP of the server. However, generally the name is used to connect to the server. Thus, the switch DNS client program (such as a browser) will ask the DNS to resolve the IP address of the named server.

5.0 Web Based Management

This section illustrates the configuration and management of the GSM switch through a web interface. Management through the web interface allows you to easily access and monitor the switch through any port.

The default values of the managed switch are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	admin

Table 5-1

Once the GSM switch has been configured via the switch's serial interface, you are ready to use the web management function. You must be connected to the switch via one of the Ethernet ports.

Access your web browser, and type in <http://192.168.1.1> (or the assigned IP address) in the address field. The login screen will be displayed. (see Figure5-1) requesting the username and password for login authentication. The default username and password are both "**admin**". Click on the **Login** button. The login process now is completed.

If you forget the password, click the link **Forget Password** on the Web login screen (See Figure 5.1) or input "Ctrl+Z" in from the CLI's login screen. The system will display a serial number. Write down this serial number and contact your vendor. The vendor will provide you with a temporary password. Use this new password as ID and Password to temporarily login. This new password is a limited use password and will only allow you log into the system one time. Therefore, modify your password one you login to the system.

The switch supports a simple user management function allowing only one administrator to configure the system at a time. If there are two or more users using administrator's identity, the switch will allow the one who logs in first to configure the system. The rest of users, even with administrator's identity, can only monitor the system. Without administrator's identity, you can only monitor the system.

A maximum of three users are able to login simultaneously in the switch. To optimize the display effect, we recommend you use Microsoft IE 6.0 and above as your web browser.



Figure 5.1 – Login Screen

5.1 Overview of Web Management

Once you have logged into the switch, the opening screen displays the **System Information**. On the left side of the screen, the function tree for all of the management functions is displayed. We will explore these functions in this chapter.

The following information is listed on the opening screen:

- Model
- System Description
- Location
- Contact
- Device Name
- System Up Time
- Current Time
- BIOS Version
- Firmware Version
- Hardware-Mechanical Version
- Serial Number
- Host IP Address
- Host MAC Address
- Device Port
- RAM Size
- Flash Size

5.2 displays the **System Information** screen.

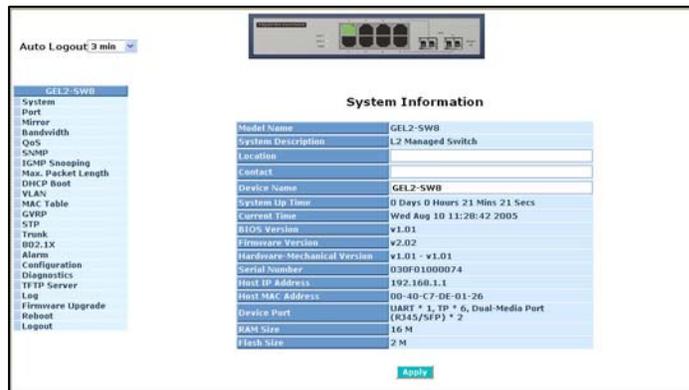


Figure 5.2 – System Information

The top of the screen displays the front panel of the switch. The linked ports will be displayed in green and the ports that are not connected will be dark. The optional modules will display a cover plate if no module exists and will show a module if a module is present. The image of module depends on the installed module. If the module port is not connected, the port be dark and, if linked, green.

The front panel displayed at the top of the screen provides clicking functions that allow you to view information about the switch. This is a very convenient function for browsing the information for a single port. To view a single port, click on the port and an information window will be displayed. (See Figure 5.3)

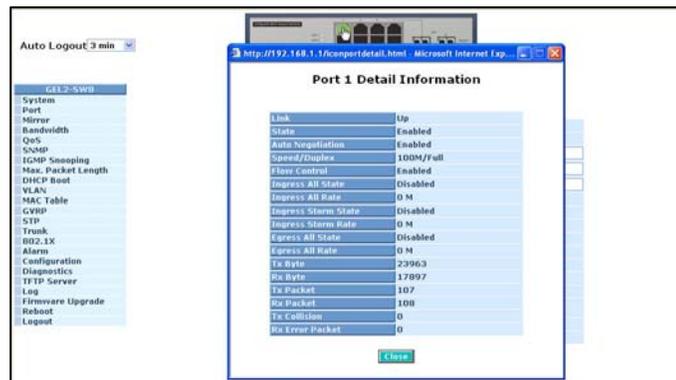


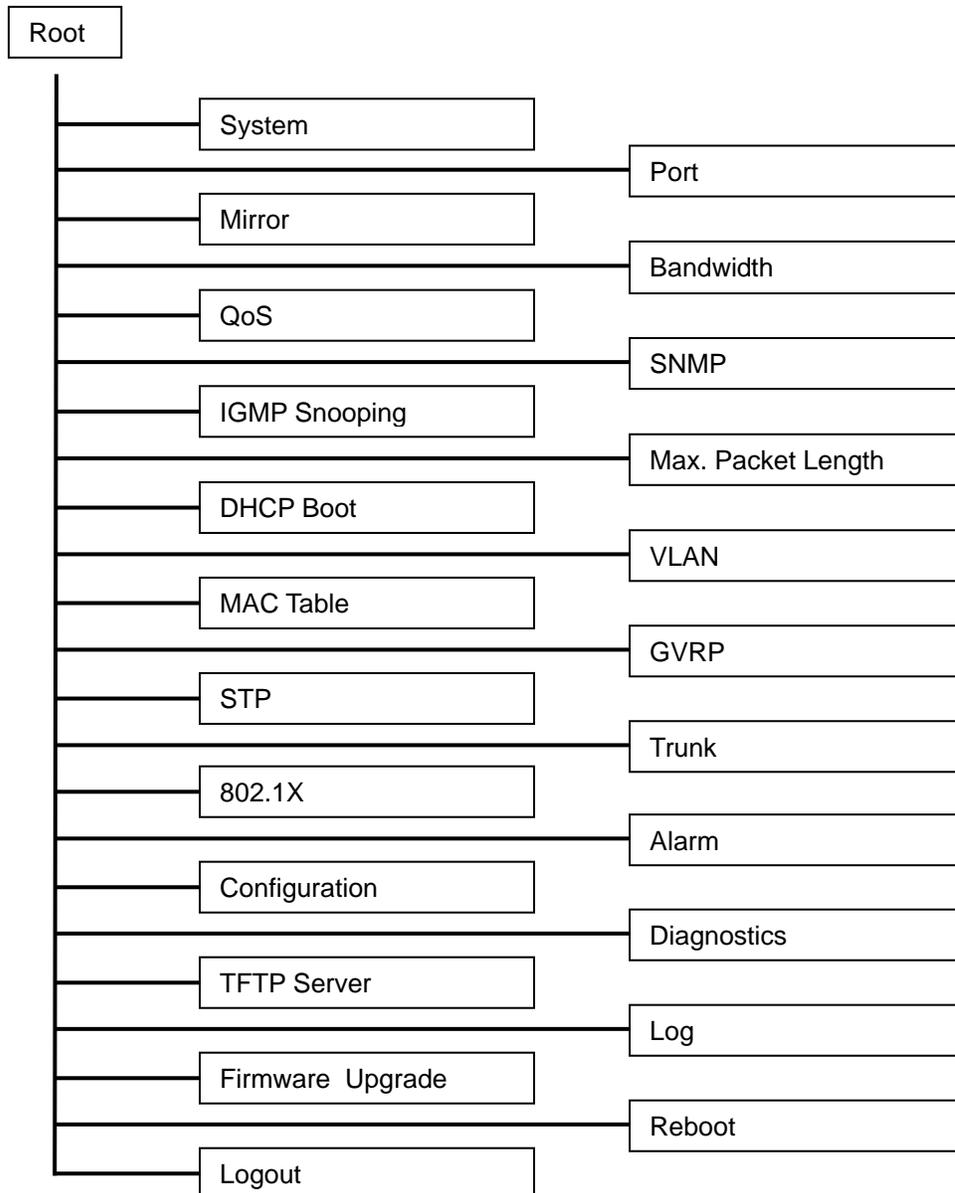
Figure 5.3 - Port detail information

5.3 shows basic information of the selected port. You will be able to view port status, traffic status and bandwidth rating for egress and ingress respectively.

On the left-top corner, there is a pull-down list for Auto Logout. For additional switch security, an auto-logout function is available to protect you from illegal users if you don't logout of the

management functions when you are finished. The **Auto Logout** default is set to three minutes. You may change the time by using the pull down list for Auto Logout. The system will automatically log out if there has been no activity during the time you choose. There is also an option for **OFF**. If OFF is selected, the management screen will remain on.

The left side of the screen displays the main menu tree for the web functions. This a hierarchical menu. When you make a selection, a sub menu may be displayed with additional function in the sub menu. The functions of each folder are described in this section. The following list is the full function tree for web user interface.



5.2 System Information

Function name:

System Information

Function description:

Show the basic system information.

Parameter description:

Model name:

The model name of this device.

System description:

Describes the device. "L2 Managed Switch".

Location:

The location where this switch is being used. User-defined.

Contact:

For the purpose of managing and maintaining the device, enter the contact person and phone to be used for help. You can configure this parameter through the device's user interface or SNMP.

Device name:

The name of the switch. User-defined. Default is GEL2-SW8.

System up time:

The time accumulated since this switch was powered up. The format is day, hour, minute and second.

Current time:

Show the system time of the switch. The format: day of week, month, day, hours: minutes: seconds, year. For instance, Wed, Apr. 23, 12:10:10, 2004.

BIOS version:

The version of the BIOS.

Firmware version:

The firmware version.

Hardware-Mechanical version:

The version of Hardware and Mechanical. The figure before the hyphen is the version of electronic hardware; the one after the hyphen is the version of mechanical.

Serial number:

The serial number is assigned by the manufacturer.

Host IP address:

The IP address of the switch.

Host MAC address:

It is the Ethernet MAC address of the management agent in this switch.

Device Port:

Show all types and numbers of the port in the switch.

RAM size:

The size of the DRAM in this switch.

Flash size:

The size of the flash memory in this switch.

5.3 IP Configuration

IP configuration is one of the most important configurations in the switch. Without the proper setting, the network manager will not be able to manage or view the device. The switch supports both manual IP address setting and automatic IP address setting via DHCP server. When IP address is changed, you must reboot the switch so the setting takes effect and uses the new IP for management access.

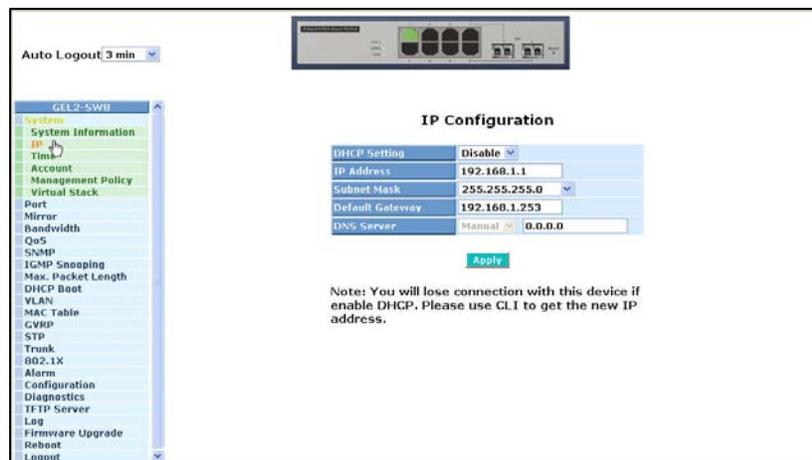


Figure 5.4 - IP - Address Configuration

Function name:

IP Configuration

Function description:

Set IP address, subnet mask, default gateway and DNS for the switch.

Parameter description:

DHCP Setting:

DHCP is the abbreviation of Dynamic Host Configuration Protocol. DHCP is **disabled** by default. In this menu, you may **enable** or **disable** DHCP.

The switch supports DHCP client used to get an IP address automatically if you set this function "Enable". When enabled, the switch will issue the request to the DHCP server to get an IP address. If the DHCP server is down or does not exist, the switch will issue the request and notify you that the IP address is being requested until the DHCP server is up. Before getting an IP address from DHCP server, the device will stop the booting process. If the field is set to "Disable", you will have to input the IP address manually. For more details about IP address and

DHCP, refer to **Section 4.4 - IP Address Assignment**.

Default: Disabled

IP address:

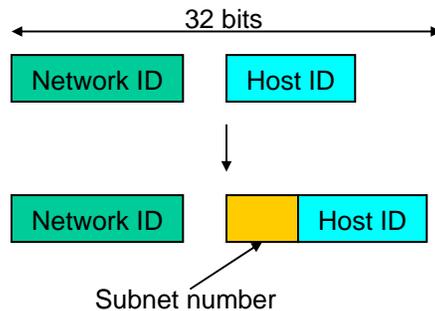
Users can configure the IP settings and enter new values if users set the DHCP function to "Disable". Click the **Apply** button to update.

When DHCP is disabled, Default: 192.168.1.1

If DHCP is enabled, this field is completed by the DHCP server and will not allow user manually set future IP addresses.

Subnet mask:

The purpose of the subnet mask is to get more network addresses. An IP device in a network must own its IP address, composed of Network address and Host address, otherwise communication with other devices cannot be made. The network classes A, B, and C are all too large to fit for almost all networks, so the subnet mask is introduced to solve this problem. Subnet mask uses some bits from host address and makes an IP address look at the Network address, Subnet mask number and host address. It is shown in the following figure. This reduces the total of IP numbers that a network is able to support by the power of 2.



The subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices resided in the same network it attaches.

Default gateway:

Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with undefined IP address in the routing table will be sent to this device unconditionally.

Default: 192.168.1.254

DNS:

The Domain Name Server is used to serve the translation between IP address and name address. The switch supports DNS client function to re-route the mnemonic name address to DNS server to get its associated IP address for accessing Internet. You can specify a DNS IP address for the switch. The switch can translate a mnemonic name address into an IP address.

There are two ways to specify the IP address of DNS. One is fixed mode, which manually specifies its IP address, the other is dynamic mode, which is assigned by DHCP server while DHCP is enabled. DNS can help you easily remember the mnemonic address name with the meaningful words in it. No assignment of DNS address is made by default.

Default: 0.0.0.0

5.4 Time Configuration

The switch provides a manual and automatic method to set the system time via NTP. Manual setting is simple. Input “Year”, “Month”, “Day”, “Hour”, “Minute” and “Second” within the valid value range indicated in each item. If you input an invalid value, for example, 61 in minute, the switch will clamp the figure to 59.

NTP is a well-known protocol used to synchronize the system time of the switch system time over a network. NTP, an internet draft standard formalized in RFC 1305, has been adopted on the system is version 3 protocol. The switch provides four built-in NTP server IP addresses residing in the Internet and an user-defined NTP server IP address. The time zone is Greenwich-centered which uses the expression form of GMT+/- xx hours.

Function name:

Time

Function description:

Set the system time by manual input or by synchronizing from Time servers. The function also supports daylight savings.

Parameter description:

Current Time:

Show the current time of the system.

Manual:

Use this function to adjust the time manually. Enter the valid figures in the fields of Year, Month, Day, Hour, Minute and Second respectively and press the **Apply** button. The time is adjusted. The valid figures for the parameter Year, Month, Day, Hour, Minute and Second are >=2000, 1-12, 1-31, 0-23, 0-59 and 0-59 respectively. Input the wrong figure and press the **Apply** button, the device will reject the time adjustment request. There is no time zone setting in Manual mode.

Default: Year = 2000, Month = 1, Day = 1
Hour = 0, Minute = 0, Second = 0

NTP:

NTP is Network Time Protocol and is used to synchronize the network time based Greenwich Mean Time (GMT). If used in the NTP mode and have selected a built-in NTP time server or manually specify an user-defined NTP server as well as Time Zone, the switch will synchronize the time shortly after pressing the **Apply** button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

Time Zone is an offset time off GMT. To set, select the time zone first and then perform time synchronization via NTP. The switch will combine this time zone and updated NTP time to arrive at the local time. The switch supports configurable time zone from -12 to +13 step 1 hour.

Default Time zone: +8 Hrs.

Daylight Saving:

Daylight saving is adopted in some countries. If set, it will adjust the time lag or advance in unit of hours, according to the starting date and the ending date. For example, if you set the daylight saving to be one hour, when the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time

since it passed over.

The switch supports valid configurable daylight saving time is $-5 \sim +5$ step one hour. The zero for this parameter means it need not have to adjust current time, equivalent to in-act daylight saving. You don't have to set the starting/ending date as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

Default for Daylight Saving: 0.

The following parameters are configurable for the function Daylight Saving and described in detail.

Daylight Saving Start :

This is used to set when to start performing the daylight saving time.

Month:

Range is 1 ~ 12.

Default: 1

Day:

Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0

Daylight Saving End :

This is used to set when to stop performing the daylight saving time.

Month:

Range is 1 ~ 12.

Default: 1

Day:

Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0

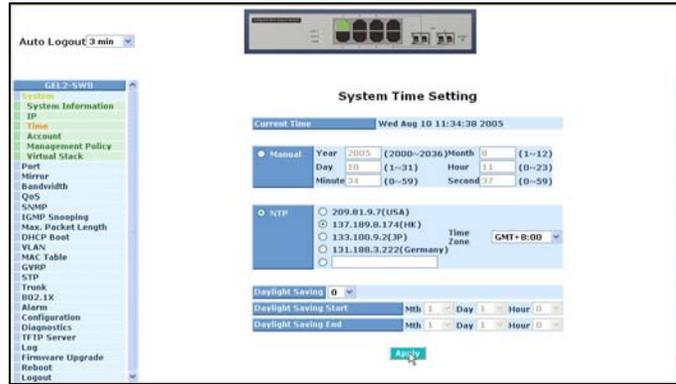


Figure 5.5 – System Time Setting

5.5 Account Configuration

Only the administrator can create, modify or delete the username and password. The administrator can modify other guest identities' password without confirming the password. Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and unable to be deleted. Up to four guest accounts can be created.

The default setting for user account is:

Username: **admin**
 Password: **admin**

The default setting for guest user account is:

Username: **guest**
 Password: **guest**



Figure 5.6 – Account Configuration

5.6 Management Policy

Through the management security configuration, the manager can perform the setup to control the switch and limit user to access the switch.

The following rules are provided for the management of the switch:

Rule 1: If no lists exists, all connections are accepted.

Accept

Rule 2: If “accept lists” exists, all connections will be denied except the connection inside the accepting range.

Accept Deny Accept Deny Accept

Rule 3: If “deny lists” exists, all connections will be accepted except the connection inside the denying range.

Deny Accept Deny Accept Deny

Rule 4: If both “accept and deny” lists exist, all connections will be denied except the connection inside the accepting range.

Accept Deny Deny Deny Accept

Rule 5: If both “accept and deny” lists exist, all connections will be denied except the connection inside of accepting range and NOT inside the denying range at the same time.



Deny| Acc | Deny | Acc | Deny

Function name:

Management Security Configuration

Function description:

The switch provides a Management Security Configuration function. With this function, the manager can easily control the mode that the is used to connect to the switch. According to the mode, users can be classified into two types: Those who are able to connect to the switch (Accept) and those who are unable to connect to the switch (Deny). Some restrictions also can be placed on the mode used to connect to the switch. For example, VLAN VID is able to be accepted or denied by the switch, the IP range of the user could be accepted or denied by the switch, a user port can be allowed or not allowed to connect with the switch, or the way the switch is controlled when

connected by via HTTP, Telnet or SNMP.



Figure 5.7 – Management Security Configuration

Parameter description:

Name:

A name is composed of any letter (A-Z, a-z) and digit (0-9) with maximal 8 characters.

VID:

The switch supports two options for managed valid VLAN VID, including **any** and **custom**. The default is **any**. **Custom** allows you to supply the VID number. The valid VID range is 1~4094.

IP Range:

The switch supports two options for managed valid IP Range, including **any** and **custom**. The default is **any**. **Custom** allows you to assign an effective IP range. The valid range is 0.0.0.0~255.255.255.255.

Incoming Port:

The switch supports two options for managed valid Port Range, including **any** and **Custom**. The default is **any**. **Custom** allows you to select the ports that should be used and the ports that should be restricted in the management security configuration.

Access Type:

The switch supports two options for managed valid Access Type, including **any** and **Custom**. The default is **any**. HTTP, Telnet and SNMP if **Custom** has been chosen, HTTP, Telnet and SNMP can be used to access and managing the switch.

Action:

The switch supports options for managed valid Action Type, including **deny** and **accept**. The default is **deny**. **Deny** restricts access switch management. **Accept** provides the authority to manage the switch.

Edit/Create:

A new entry of Management Security Configuration can be created after the initial parameters have been setup. Use the **Edit/Create** button.

Delete:

Removes the existed entry of management security configuration from the management security table.

5.7 Virtual Stack

Function name:

Virtual Stack

Function description:

Virtual Stack Management (VSM) is the group management function. VSM configuration automatically groups switches in the same LAN. One switch among the group will be the master device, and the others will become the slave devices.

VSM offers a simple centralized management function. It is not necessary to remember the address of all devices, because the manager is capable of managing the network with the address of the Master device. VSM is only available in Web UI. While one switch become the Master, two rows of buttons for the group device will appear on the top of the Web UI. You can use these buttons to connect to the Web UI of the devices of the group without logging into these devices.

The top-left button is only for Master device (See Figure3-9). The background color of the button you press will be changed to represent that the device is under your management.

Note: If you login via the console, the grouping will be removed temporarily.

The device of the group will be shown as station address (the last number of IP Address) + device name on the button (e.g. 196_GEL2-SW8). If no corresponding device exists, " ---- " will be displayed.

Once the devices successfully join the group, they can be managed via the Master device and cannot be managed via telnet/console/web individually.

Up to 16 devices can be grouped for VSM, however, only one Master is allowed to exist in each group. For Master redundancy, you may configure more than two devices as Master device, however, the Master device with the smaller MAC value will be the Master. All of these 16 devices can become the Master device and back up with each other .

Virtual Stack is **disabled** by default.

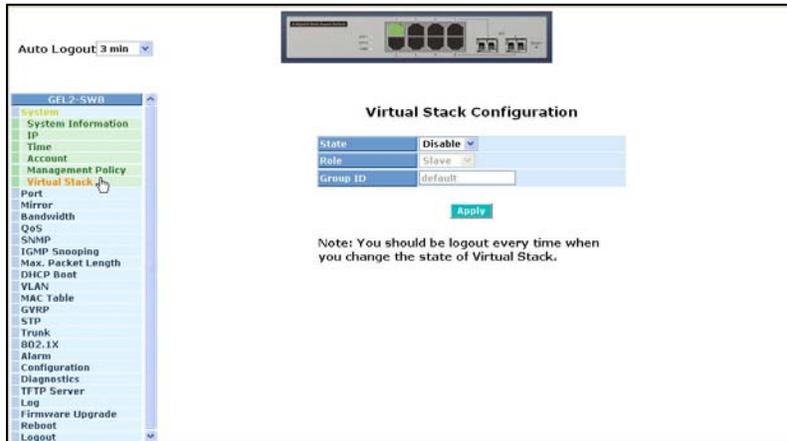


Figure 5.8 – Virtual Stack

Parameter description:

State:

Used for the activation or de-activation of VSM.

Role:

The role that the switch would like to play in virtual stack. Two types of roles, including master and slave are offered. The default is **Master**.

Group ID:

It is the group identifier (GID) which signs for VSM. Valid letters are A-Z, a-z, 0-9, “ - “ and “ _ ” characters. The maximum length is 15 characters.

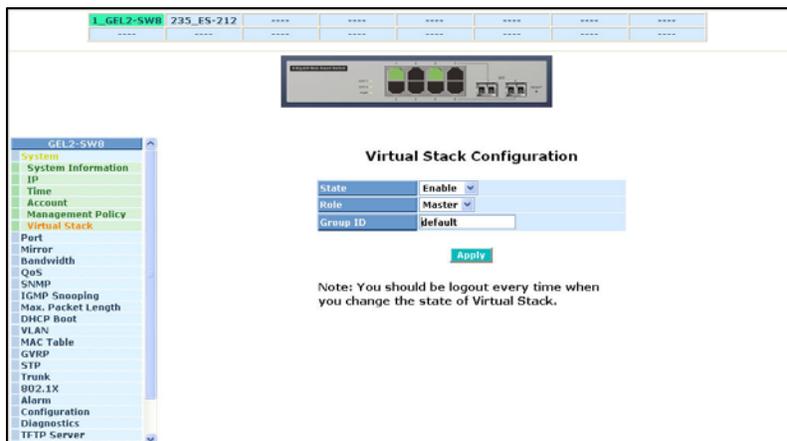
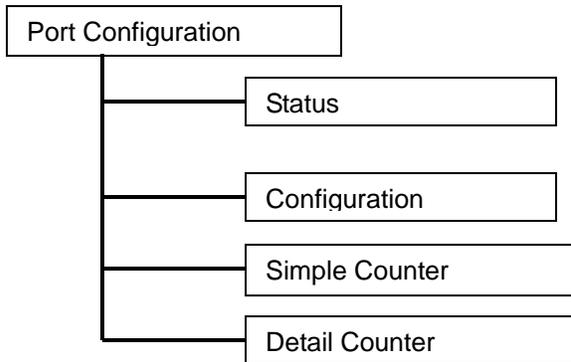


Figure 5.9 – Virtual Stack

5.8 Port Configuration

Port configuration includes the following functions:



5.8.1 Port Status

The port status function gathers the current status for all ports. The information is displayed by the order of port number, link status, port state, auto-negotiation status, speed/duplex and flow control. If a fiber module is installed in one or both of the slots, the current status for those ports will be displayed. See Figure 5.10.

Port No	Media	Link	State	Auto-Negot	Speed / Duplex	Flow Control
1	TP	Up	Enabled	Enabled	100M/Full	Enabled
2	TP	Down	Enabled	Enabled	10M/Half	Disabled
3	TP	Down	Enabled	Enabled	10M/Half	Disabled
4	TP	Down	Enabled	Enabled	10M/Half	Disabled
5	TP	Down	Enabled	Enabled	10M/Half	Disabled
6	TP	Down	Enabled	Enabled	10M/Half	Disabled
7	TP	Down	Enabled	Enabled	10M/Half	Disabled
8	TP	Down	Enabled	Enabled	10M/Half	Disabled

Figure 5.10 – Port Status

Function name:

Port Status

Function Description:

Port status reports the current status of all ports in the switch. The screen will be automatically refreshed approximately every five seconds as port parameters change.

Parameter Description:

Port No:

Displays the port number. The number is 1 – 8. Ports 7 and 8 may be fiber modules.

Media:

Shows the media type used in all ports. Port 7 and Port 8 are dual media ports, which support either fiber or UTP media with either Gigabit Ethernet or Fast Ethernet. If SFP modules are installed, Port 7 and/or Port 8 can no longer be used for a UTP connection. Since the fiber port could be multimode or singlemode, the information will be based on the actual media installed in the switch with reference to connector, distance, fiber mode, etc. The module port information is displayed in 5.11.

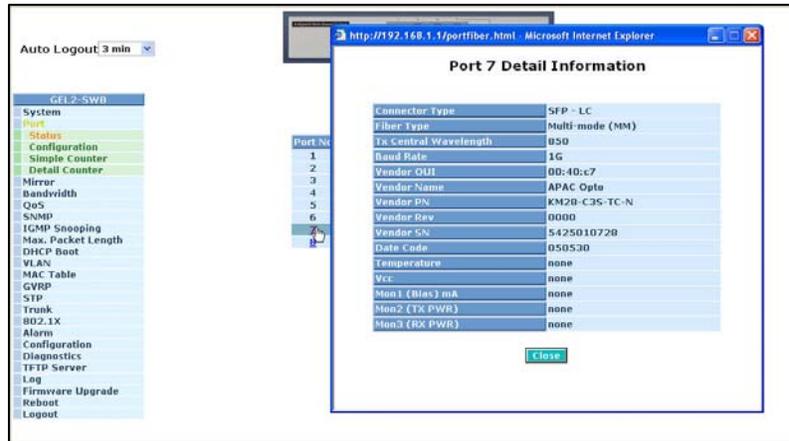


Figure 5.11 – Detailed Port Information

Link:

Displays an active or inactive port. If the link is connected to a working device, the link will show that it is "Up"; otherwise, it will show "Down". This is determined by the hardware on both devices of the connection.

No default value.

State:

Displays the communication function of the port is "Enabled" or "Disabled". When it is enabled, traffic can be transmitted and received via this port. When it is disabled, no traffic can be transferred through this port. Port State is configured by user.

Default: Enabled.

Auto Negotiation:

Displays the exchange mode of Ethernet MAC. There are two modes supported in the switch. They are auto-negotiation mode "Enabled" and forced mode "Disabled". When in "Enabled" mode, this function will be automatically negotiated by the hardware itself and exchange the capability of speed and duplex mode. The best communication mode will be used. When in "Disabled" mode, both parties must have the same setting of speed and duplex, otherwise, there will be no link. In this case, the link result is "Down".

Default: Enabled

Speed / Duplex Mode:

Displays the speed and duplex mode of all ports. There are three speeds 10Mbps, 100Mbps and 1000Mbps supported for TP media. Duplex mode is half duplex and full duplex. If the media is 1Gbps fiber, it is 1000Mbps only. The status of speed/duplex mode is determined by:

- Negotiation of both the local port and the link partner in “Auto Speed” mode
- User setting in “Force” mode. The local port has to be preset according to its capability.

Default: None, depends on the result of the negotiation.

Flow Control:

Show each port's flow control status.

There are two types of flow control in Ethernet, **backpressure** for half-duplex operation and **pause flow control** (IEEE802.3x) for full-duplex operation. The switch supports both.

Default: Disabled

Parameter description of Port 7 and Port 8:

Connector Type:

Displays the connector type (UTP, SC, ST, LC, etc.)

Fiber Type:

Displays the fiber mode (multimode or singlemode).

Tx Central Wavelength:

Displays the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.

Baud Rate:

Displays the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G and so on.

Vendor OUI:

Displays the manufacturer's OUI code which is assigned by IEEE.

Vendor Name:

Displays the company name of the module manufacturer.

Vendor P/N:

Displays the product name by module manufacturer.

Vendor Rev (Revision):

Displays the module revision.

Vendor SN (Serial Number):

Displays the serial number assigned by the manufacturer.

Date Code:

Displays the date this SFP module was made.

Temperature:

Displays the current temperature of SFP module.

Vcc:

Displays the working DC voltage of SFP module.

Mon1(Bias) mA:

Displays the Bias current of SFP module.

Mon2(TX PWR):

Displays the transmit power of SFP module.

Mon3(RX PWR):

Displays the receiver power of SFP module.

5.8.2 Port Configuration

Port Configuration is used to modify the setting by port. This function allows set and reset the functions described below.

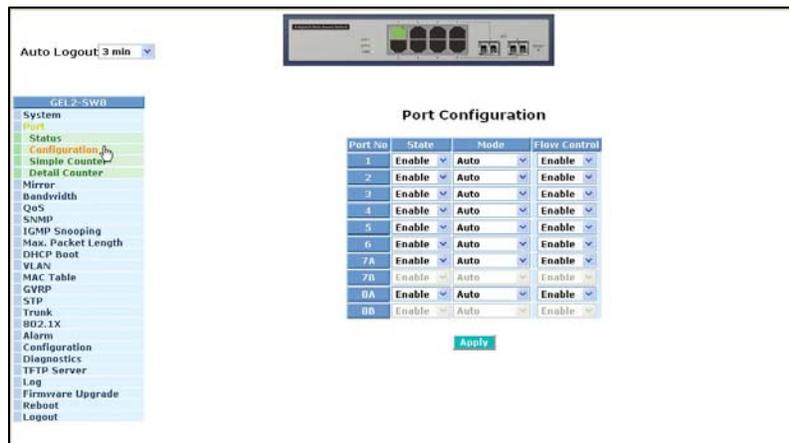


Figure 5.12 – Port Configuration

Function name:

Port Configuration

Function description:

Used to set the operation mode of each port. The switch supports three parameters for each port:

- State
- Mode
- Flow control.

Parameter description:

State:

The communication capability of the port is Enabled or Disabled. When enabled, traffic can be

transmitted and received via this port. When disabled, the port is blocked and no traffic can be transmitted through this port. Port State is configurable by the user. If you set a port's state to **Disable**, then that port cannot pass traffic, even though **Link** is displayed.

Default: **Enable**.

Mode:

Set the speed and duplex mode for the port. If the media is 1Gbps fiber, it will always be 1000Mbps and the duplex mode can only be full. If the media is TP, the speed/duplex mode is comprised of speeds of 10/100/1000Mbps and the duplex mode is either full or half duplex. The following table summarizes the function the media supports.

Media type	NWay	Speed	Duplex
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

In auto-negotiation mode, there is no default value. In forced mode, the default value depends on the setting.

Flow Control:

There are two modes to choose in flow control, including **Enable** and **Disable**. If flow control is set to Enable, both parties can send PAUSE frames to the transmitting device(s) in case the receiving port is too busy to handle the packets. When set to Disable, there will be no flow control in the port. Packets will be dropped if there is too much to handle.

Default: Enable.

5.8.3 Simple Counter

The function of the **Simple Counter** is to collect information and provide counting about the traffic of the port, whether the packet is good or bad.

In Figure 5.13, the screen shows all ports' counter information at the same time. Each data field is 20-digits. If counting is overflows, the counter will be reset and restart counting. The data is updated based on the time interval defined by the user. The valid range is three to ten seconds. The refresh interval is used to set the update frequency. Default update time is three seconds.

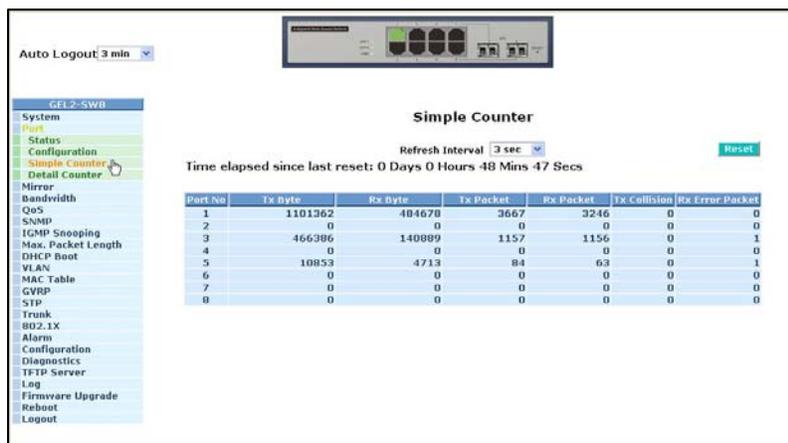


Figure 5.13 – Simple Counter

Function name:

Simple Counter

Function description:

Displays the summary counting of each port's traffic, including Tx Byte, Rx Byte, Tx Packet, Rx Packet, Tx Collision and Rx Error Packet.

Parameters description:

Tx Byte:

Total transmitted bytes.

Rx Byte:

Total received bytes.

Tx Packet:

The counting number of the packets transmitted.

Rx Packet:

The counting number of the packet received.

Tx Collision:

Number of collisions transmitting frames experienced.

Rx Error Packet:

Number of bad packets received.

5.8.4 Detail Counter

The function of the **Detail Counter** is to collect information and provide the counting for the traffic of the port, whether the packet is good or bad.

In Figure 5.14, the counter is displayed one port at a time. To see another port's counter, pull down the Select list. The figures for the port you have chosen will be displayed.

Each data field is 20-digits. If the counting overflows, the counter will be reset and counting will be restarted. The data is updated based on the time interval defined by the user. The valid range is three to ten seconds. The refresh interval is used to set the update frequency. Default update time is three seconds.



Figure 5.14 – Detailed Counter

Function name:

Detail Counter

Function description:

Displays the detailed counting number of each port's traffic. In Figure 5.14, the window shows all counter information for one port at a time.

Parameter description:

Rx Packets:

The counting number of the packets received.

RX Octets:

Total received bytes.

Rx High Priority Packets:

Number of Rx packets classified as high priority.

Rx Low Priority Packets:

Number of Rx packets classified as low priority.

Rx Broadcast:

Shows the counting number of the received broadcast packet.

Rx Multicast:

Shows the counting number of the received multicast packet.

Tx Packets:

The counting number of the packet transmitted.

TX Octets:

Total transmitted bytes.

Tx High Priority Packets:

Number of Tx packets classified as high priority.

Tx Low Priority Packets:

Number of Tx packets classified as low priority.

Tx Broadcast:

Shows the counting number of the transmitted broadcast packet.

Tx Multicast:

Shows the counting number of the transmitted multicast packet.

Rx 64 Bytes:

Number of 64-byte frames in good and bad packets received.

Rx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets received.

Rx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets received.

Rx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets received.

Rx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets received.

Rx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets received.

Tx 64 Bytes:

Number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets transmitted.

Tx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets transmitted.

Rx CRC/Alignment:

Number of alignment errors and CRC error packets received.

Rx Undersize:

Number of short frames (<64 Bytes) with valid CRC.

Rx Oversize:

Number of long frames(according to max_length register) with valid CRC.

Rx Fragments:

Number of short frames (< 64 bytes) with invalid CRC.

Rx Jabber:

Number of long frames(according to max_length register) with invalid CRC.

Rx Drops:

Frames dropped due to the lack of receiving buffer.

Rx Errors:

Number of the error packets received.

Tx Collisions:

Number of collisions transmitting frames experienced.

Tx Drops:

Number of frames dropped due to excessive collision, late collision, or frame aging.

Tx FIFO Drops:

Number of frames dropped due to the lack of transmitting buffer.

5.9 Mirror Configuration

Function name:

Mirror Configuration

Function description:

Mirror Configuration is used to monitor the traffic of the network. For example, if Port A and Port B are Monitoring Port and Monitored Port respectively, the traffic received by Port B will be copied to Port A for monitoring.

Note: When configuring the mirror function, it is recommended to avoid setting a port to be a sniffer port and an aggregated port at the same time.

Parameter description:

Mode:

Used for the activation or de-activation of Port Mirror function. Default is **disable**.

Monitoring Port:

Set up the port for monitoring. Valid port is Port 1~8 and default is Port 1.

Monitored Port:

Set up the port for being monitored. Select the check box () beside the port number. Valid ports are Port 1~8.



Figure 5.15 - Mirror

5.10 Bandwidth Management

Function name:

Bandwidth Management

Function description:

Bandwidth Management function is used to set up the limit of Ingress and Egress bandwidth for each port.

Note: Each port on the switch has a 16KB packet buffer. The packet buffer size will be reduced when the bandwidth rate limitation is enabled, which may cause the jumbo frame to not be forwarded. It is recommended to avoid enabling jumbo frame and bandwidth rating functions at the same time.



Figure 5.16 – Bandwidth Management Configuration

Parameter description:

Port Number:

Choose the port to use for bandwidth management. Valid range of the port is 1~8.

All Traffic for Ingress Rate Limiting (Policing):

Set up the limit of Ingress bandwidth for the port you chose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid range is 0~1000.

Broadcast & Multicast for Ingress Rate Limiting (Policing):

Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set in Data Rate field. The format of the packet limits to broadcast and multicast. Valid range is 0~1000.

All Traffic for Egress Rate Limiting (Shaping):

Set up the limit of Egress bandwidth for the port you choose. Packet transmission will be delayed if the rate exceeds the value you set in Data Rate field. Traffic may be lost if egress buffers run full. The format of the packet limits to unicast, broadcast and multicast. Valid range is 0~1000.

5.11 QoS (Quality of Service) Configuration

The switch provides the following powerful QoS functions:

- Per Port Priority
- VLAN Tag Priority
- IP TOS Classification
- IP TCP/UDP Port Classification
- IP DiffServe Classification

Click on **Configure** next to the desired QoS function. Once you have set the configurations, remember to click on **Apply** to save the settings.

With QoS configurations, the **Default Class** is either set to **high** or **low**. When you set one of the five QoS functions listed above, packets that do not belong to this QoS setting are viewed as **Default Class**.

For example, if you set QoS function as VLAN Tag Priority mode, and then choose Default Class as High, the priority of the packets with no tag will be considered as High priority. The initial value of the Default Class is High.



Figure 5.17 – QoS Configuration

The QoS functions listed in Figure 5.17 are listed below.

Function name:

Per Port Priority

Function description:

QoS priority can be assigned, including High and Low for each port. For example, if IP packets from Port 2 and Port 3 are transmitted at the speed of 1Gbps to Port 1, and the Class of Port 2 is set as High and Port 3 is set as Low, then the packets of Port 3 will be dropped when the congestion happens because Port 2 has a higher precedence of transmitting packets.

Parameter description:

Port No:

Choose the port (1~8) respectively with Priority Class on Per Port Priority function.

Class:

Set High Priority or Low Priority for each port respectively.

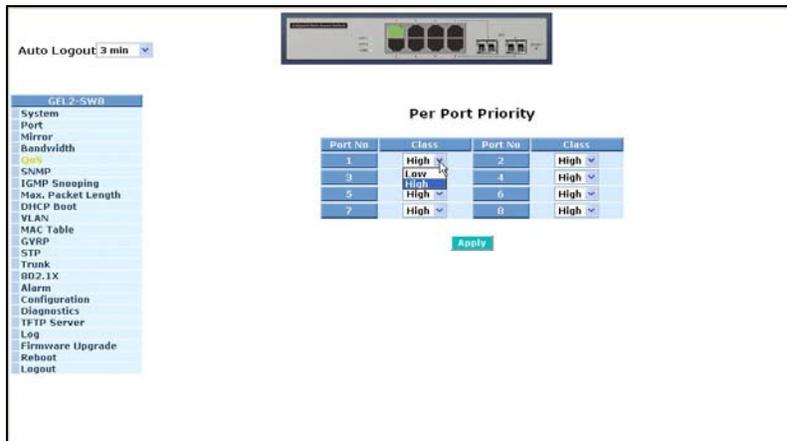


Figure 5.18 – Per Port Priority

Function name:

VLAN Tag Priority

Function description:

In VLAN tag, there are three bits belonging to priority. According to these three bits, we could arrange eight traffics – 0 0 0, 0 0 1, 0 1 0, 0 1 1, 1 0 0, 1 0 1, 1 1 0, 1 1 1. We can set High priority or Low priority for each traffic class. For instance, if we set VLAN-tagged priority 0 0 0 to high priority and VLAN-tagged priority 0 0 1 to Low Priority, and then include ports 1, 2, 3 in VLAN 2 that means the packets that have the value 0 0 0 in VLAN-tagged field and VID equals two from Port 2 and the packets that have the value 0 0 1 in VLAN-tagged field and VID equals two from Port 3 into the switch. The two kinds of packets are transmitted for Port 1 until the port results in congestion. The result is that the packets will be dropped partially from Port 3 because the packets belong to Low Priority. For the use of VLAN Tag Priority function, use the **Configure** button.

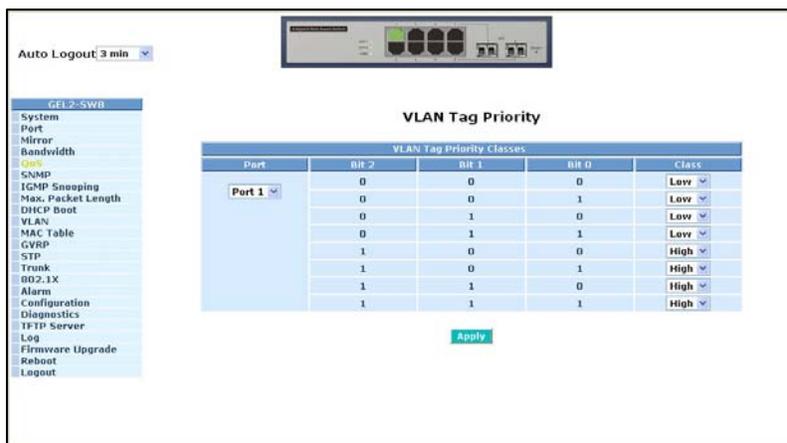


Figure 5.19 – VLAN Tag Priority

Parameter description:

Quality of Service (QoS) VLAN Tag Configuration:

Used for setting up the QoS belongs to VLAN operation.

Port:

Set the ports (1~8) respectively to allow the VLAN Tag QoS function to work. Use **Select All** to set all the ports at the same time.

Bit 0, Bit 1, Bit 2:

According to the arrangement of VLAN-tagged priority, eight types of traffic can be formed, including 0 0 0, 0 0 1, 0 1 0, 0 1 1, 1 0 0, 1 0 1, 1 1 0 and 1 1 1.

Class:

Set High Priority or Low Priority for each port respectively for the eight types of traffic.

Function name:

IP ToS Classification

Function description:

Another QoS function is the application of Layer 3 on network framework. This focus is on the TOS field of the IP header. There are three bits in TOS field. Bit 5~7 of TOS field will be used. According to these three bits, we could arrange eight traffics – 0 0 0, 0 0 1, 0 1 0, 0 1 1, 1 0 0, 1 0 1, 1 1 0, 1 1 1. As long as we change bit 5~7 of TOS field of IP header, we will create the eight traffic packets. High priority or Low priority can be set for each traffic class. For instance, if we set TOS 0 0 0 to high priority and TOS 0 0 1 to Low Priority the packets that have bit 5~7 of TOS Field are 0 0 0 from Port 2 and the packets that have bit 5~7 of TOS Field are 0 0 1 from Port 3. The two kinds of packets are transmitted for Port 1 until the port results in congestion. The result is that the packets will be dropped partially from Port 3 because the packets belong to Low Priority.

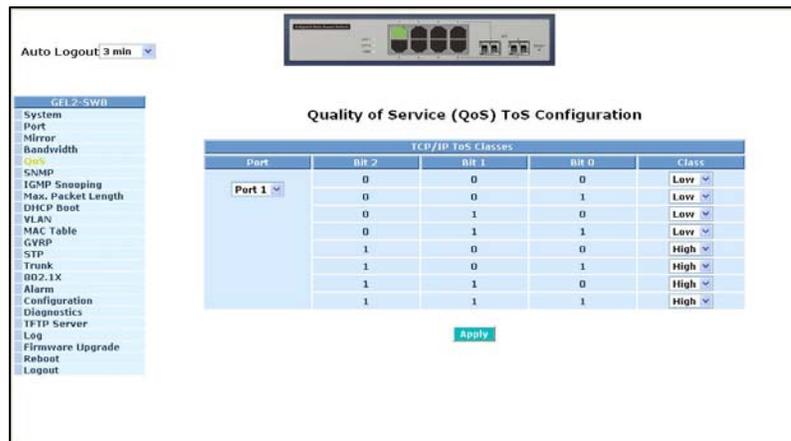


Figure 5.20 – QoS ToS Configuration

Parameter description:

Quality of Service (QoS) ToS Configuration:

Used for setting the QoS in Layer 3.

Port:

Set the ports (1~8) respectively to allow the TOS QoS function to work. Use **Select All** to set all the ports at the same time.

Bit 0, Bit 1, Bit 2:

According to the arrangement of Bit 5 ~ Bit 7 in TOS Field of IP Header, eight types of traffic can be formed, including 0 0 0, 0 0 1, 0 1 0, 0 1 1, 1 0 0, 1 0 1, 1 1 0 and 1 1 1.

Class:

Set High Priority or Low Priority for each port respectively for the eight types of traffic.

Function name:

IP TCP/UDP Port Classification

Function description:

In the L4 QoS Configuration, one of the following seven special network transmission events can be chosen:

Parameter description:

Disable IP TCP/UDP Port Classification:

Belongs to the QoS in L4. Select the option button and click **Apply**. Click **Advance** set special TCP/UDP port for QoS.

Down prioritize web browsing, e-mail, FTP and news:

Belongs to the QoS in L4. Select the option button and click **Apply**. Click **Advance** to set special TCP/UDP port for QoS.

Prioritize IP Telephony (VoIP):

Belongs to the QoS in L4. Select the option button and click **Apply**. Click **Advance** to set special TCP/UDP port for QoS.

Prioritize iSCSI:

Belongs to the QoS in L4. Select the option button and click **Apply**. Click **Advance** to set special TCP/UDP port for QoS.

Prioritize web browsing, e-mail, FTP transfers and news:

Belong to the QoS in L4. Select the option button and click **Apply**. Click **Advance** to set special TCP/UDP port for QoS.

Prioritize Streaming Audio/Video:

Belongs to the QoS in L4. Select the option button and click **Apply**. Click **Advance** to set special TCP/UDP port for QoS.

Prioritize Databases (Oracle, IBM DB2, SQL, Microsoft):

Belongs to the QoS in L4. Select the option button and click **Apply**. Click **Advance** to set special TCP/UDP port for QoS.

Advanced Mode:

Display the TCP/UDP port number in L4 QoS. In the **Disable IP TCP/UDP Port Classification** mode, you can randomly choose a TCP/UDP port number that L4 QoS will affect. As to other special L4 QoS events, special TCP/UDP port number will take action. You can add or modify the port number at random. For instance, if you choose **Down prioritize web browsing, e-mail,**

FTP and news as the QoS of L4 and enter the “Advanced Mode”, then we can see that special port numbers 80, 280, 443, 25, 110, 20, 21, 69, 119, 2009 have already been configured. You can also modify these port numbers. See Figure 5.21.

Special TCP/UDP class:

There are two modes for selection, including Low and High.

Default class (all other TCP/UDP ports):

There are two modes for selection, including Low and High.

Port:

You can set the ports (1~8) respectively to allow the Special TDP/UDP class function to work. To set all ports at the same time, select **All**.

Special UDP/TCP Port Selection:

The following are port numbers defined by the following specific networks in L4:

- Down prioritize web browsing, e-mail, FTP and news:
 - port number 80,280,443,25,110,20,21,69,119,2009
- Prioritize IP Telephony (VoIP):1718,1719,1720
- Prioritize iSCSI:3225,3260,3420
- Prioritize web browsing, e-mail, FTP transfers and news:
 - 80,280,443,25,110,20,21,69,119,2009
- Prioritize Streaming Audio/Video: 2979,1755,7070,7071,554,8000
- Prioritize Databases (Oracle, IBM DB2, SQL, Microsoft):
66,1571,1575,523,118,156,3306,1232,1433,1434

Once you have selected **Configure** for **IP TCP/UDP Port**, you can choose either the **Advanced Mode** or the **Simple Mode**.



Figure 5.21 - Advanced Mode

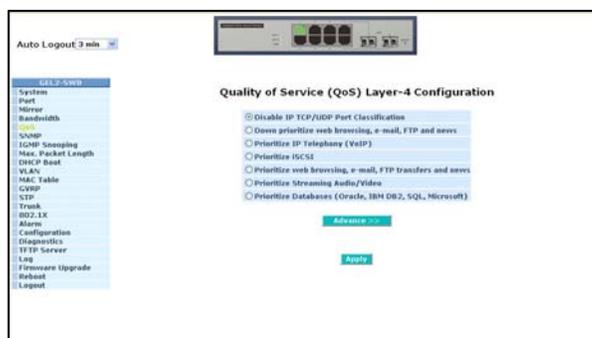


Figure 5.22 - Simple Mode

Simple Mode:

Select **Simple** to return to the screen that all L4 port number will disappear (See Figure 5.22).

Function name

IP Diffserv Classification

Function description:

In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

IP Diffserve Classification function, can form total 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packet. Sixty-four types of Class that belong to High or Low Priority can be set.

Parameter description:

IP Differentiated Services (DiffServ) Configuration:

Used to set the IP Differentiated Services Configuration QoS.

Diffserv:

Display 64 (0~63) DiffServ Priority items.

Class:

64 types of traffic. Can set High Priority or Low Priority for each port respectively.

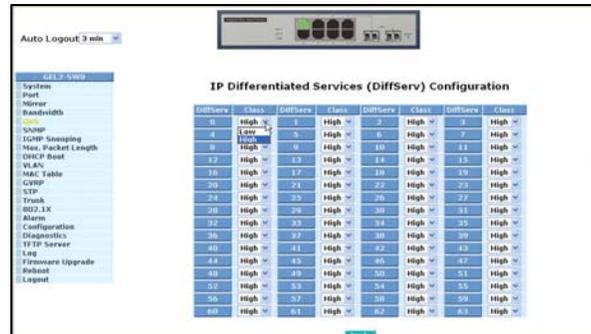


Figure 5.23 – IP Differentiated Services

5.12 SNMP Configuration

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage devices equipped with the SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent. This protocol traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax.

SNMP is passive except for the issuing the trap information. The switch supports a function to turn on or off the SNMP agent. If you set the field SNMP to **Enable**, the SNMP agent will be launched. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If SNMP is set to **Disable**, the SNMP agent will not be activated. The related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

Function name:

SNMP Configuration

Function description:

This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once the setting has been completed, click **Apply** and the setting will take effect.

Parameters description:

SNMP:

The term SNMP is used for the activation or de-activation of SNMP. Default is Enable.

Get/Set/Trap Community:

Community name is used as the password for authenticating if the requesting network management unit belongs to the same community group. If they don't have the same community name, they don't belong to the same group. Hence, the requesting network management unit cannot access a device with a different community name via SNMP protocol;

If they both have the same community name, they can talk each other.

Community name is user-definable with a maximum length of 15 characters and is case sensitive. No blank spaces are permitted in the community name string. Any printable character is allowed.

The community name for each function works independently. Each function has its own community name. The community name for GET only works for the GET function and can't be applied to other function such as SET and Trap.

Default SNMP function: **Enable**

Default community name for GET: **Public**

Default community name for SET: **Private**

Default community name for Trap: **Public**

Default Set function: **Enable**

Default trap host IP address: **0.0.0.0**

Default port number: **162**

Trap:

There are six supported trap hosts. Each has its own community name and IP address and is user-definable. To create a trap host means to create a trap manager by assigning an IP address to the host the trap message. In other words, the trap host is a network management unit with SNMP manager receiving the trap message from a switch with SNMP agent issuing the trap message. Six trap hosts can prevent the important trap message from being lost.

For each public trap, the switch supports the trap event Cold Start, Warm Start, Link Down, Link Up and Authentication Failure Trap. They can be enabled or disabled individually. When enabled, the corresponded trap will actively send a trap message to the trap host when a trap occurs. If all public traps are disabled, no public trap message will be sent. The Enterprise (no. 6) trap is classified as private trap, which is listed in the Trap Alarm Configuration function folder.

Default for all public traps: **Enable**.



Figure 5.24 - Community and trap host setting

5.13 IGMP Snooping

IGMP snooping is used to establish the multicast groups to forward multicast packets to member ports. IGMP snooping avoids wasting the bandwidth while IP multicast packets are running over the network. A switch that does not support IGMP snooping cannot tell a multicast packet from broadcast packet, so it treats them as broadcast packets. Without IGMP snooping, the multicast packet forwarding function is no different from broadcast packets.

A switch with IGMP snooping supports the functions of query, report and leave. A type of packet exchanged between IP multicast router/switch and IP multicast host can update the information of the multicast table when a member (port) joins or leaves an IP multicast destination address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who had joined a specified IP multicast group.



Figure 5.25 – IGMP Snooping

Function name:

IGMP Snooping

Function description:

IGMP is used to snoop the status of IP multicast groups and display its associated information in both tagged VLAN and non-tagged VLAN networks. Enabling IGMP with either passive or active mode, you can monitor the IGMP snooping information, which contains the multicast member list with the multicast groups, VID and member port.

Parameter description:

IGMP snooping mode selection:

The switch supports three kinds of IGMP Snooping status, including “Passive”, “Active” and “Disable”.

Disable:

Use “Disable” mode to disable IGMP Snooping function.

Default: Disable

Active:

In Active mode, IGMP snooping will periodically issue the Membership Query message to all attached hosts and gather the membership report message to update the database of the multicast table. This also reduces the unnecessary multicast traffic.

Passive:

In passive snooping mode, IGMP snooping will not periodically poll the hosts in the groups. The switch will send a Membership Query message to all hosts only when it has received a Membership Query message from a router.

IP Address:

Shows all multicast groups IP addresses that are registered on this device.

VLAN ID:

Shows VLAN ID for each multicast group.

Member Port:

Shows member ports that join each multicast group.

5.14 Maximum Packet Length

Function name:

Max. Packet Length

Function description:

The switch is capable of handling with 9k jumbo frames.

Parameter description:

Jumbo Frame(bytes):

Set up the maximum length of the packet that each port of the switch can accept. Maximum length can be up to 1532 bytes or 9216 bytes. The default is 1532 bytes.



Figure 5.26 - Maximum Packet Length

5.15 DHCP Boot

The DHCP Boot function is used to spread the request broadcast packet into a bigger time frame to prevent the traffic congestion due to broadcast packets from many network devices which may seek its NMS, boot server, DHCP server and predefined connections in case the whole building or block loses power. When this happens, the switch has to be rebooted. Switches or other network devices on the LAN will try their best to find the server to return to their services or try to set up the predefined links. Many broadcast packets will be issued.

The switch supports a random delay time for DHCP and boot delay for each device. This suppresses the broadcast storm while all devices are booting at the same time. The maximum user-defined delay time is 30 seconds. If DHCP Broadcasting Suppression function is enabled, the delay time is set randomly, ranging from 0 to 30 seconds. The exact delay time is computed by the switch itself. The default is **Disable**.



Figure 5.27 – DHCP Boot

5.16 VLANs

The switch supports Tag-based VLAN (802.1q) and Port-based VLANs. 256 active VLANs are supported and VLAN ID can range from 1~4094. VLAN configuration is used to partition your LAN into small segments based on your LAN requirements. By properly configuring VLANs, you can improve security and increase performance.

5.16.1 VLAN Mode

Function name:

VLAN Mode Setting

Function description:

The VLAN Mode Selection function includes five modes: Port-based, Tag-based, Metro Mode, Double-tag and Disable. Choose a mode by using the drop-down list and selecting an item. Click **Apply** and the settings will take effect immediately.

Parameter description:

VLAN Mode:

Disable:

Stop VLAN function on the switch. In this mode, no VLAN is applied to the switch. This is the default setting.

Port-based:

Port-based VLAN is defined by port. Any packet coming in or out from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1 contains port members Ports 1, 2, 3 & 4, and if you are connected to Port 1, you can communicate with Port 2-4. If you are connected to Port 5, you cannot

communicate with those ports. Each port-based VLAN must be assigned a group name. This switch can support up to a maximum of 8 port-based VLAN groups.

Tag-based:

Tag-based VLAN identifies its member by VID. Tag-based VLANs are different from port-based VLANs. If there are additional rules in ingress filtering list or egress filtering list, the packet will be screened with filtering criteria to determine if it can be forwarded. The switch supports 802.1q.

Each tag-based VLAN must be assigned a VLAN name and VLAN ID. Valid VLAN ID is 1-4094. You may create total up to 64 Tag VLAN groups.

Metro Mode:

The Metro Mode is a quick configuration VLAN environment method on Port-based VLAN. You can create 14 or 15 port-based VLAN groups.

Double-tag:

Double-tag mode belongs to the tag-based mode, however, it would treat all frames as the untagged ones, which means that tag with PVID will be added into all packets. Then, these packets will be forwarded as Tag-based VLAN. So, the incoming packets with tag will become the double-tag ones.



Figure 5.28 – VLAN Mode

Up-link Port:

This function is enabled only when metro mode is chosen in VLAN mode.

Port 7:

Except Port 7, the switch ports cannot transmit packets with each other. Each port groups a VLAN with Port 7, thus, seven groups consisting of two members are formed.

Port 8:

Except Port 8, the switch ports cannot transmit packets with each other. Each port groups a VLAN with Port 8, thus, seven groups consisting of two members are formed.

Ports 7 and 8:

Except Port 7 and Port 8, the switch ports cannot transmit packets with each other. Each port groups a VLAN with Port 7 and Port 8, thus, total six groups consisting of three members are formed.



Figure 5.29 – VLAN Mode

5.16.2 Tag-based Group

Function name:

Tag-based Group Configuration

Function description:

Displays tag-based VLAN groups. Use this option to create, edit and delete a tag-based VLAN groups. Add a new VLAN group by inputting a new VLAN name and VLAN ID.

Parameter description:

VLAN Name:

Valid letters are A-Z, a-z, 0-9, “ - “ and “ _ ” characters. The maximal length is 15 characters.

VID:

VLAN identifier. Each tag-based VLAN group has a unique VID used in tag-based and Double-tag mode.

SYM-VLAN:

While the SYM-VLAN function of the group is enabled, all packets with this group VID will be dropped if they are transmitted from the ports that do not belong to this group.

Member:

Used to enable or disable a member port. **Enable** means the port is a member of the VLAN. Select the check box () beside **Port X** to enable it.

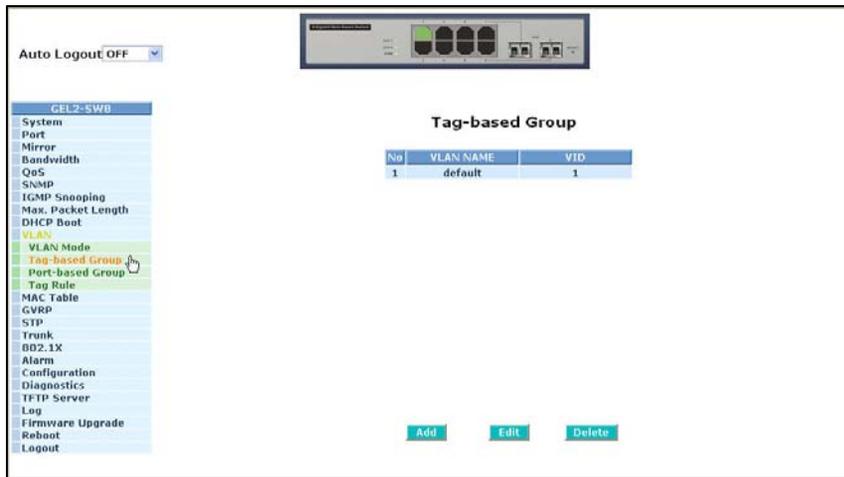


Figure 5.30 – Tag-based Group

Add Group:

Create a new Tag-based VLAN. Input the VLAN name and the VID. Configure the SYM-VLAN function and choose the member by selecting the check box beside the port number. Press **Apply** so the settings will take effect.



Figure 5.31 – Tag-based VLAN

Delete Group:

Press **Delete** to remove the selected group entry from the tag-based group table.

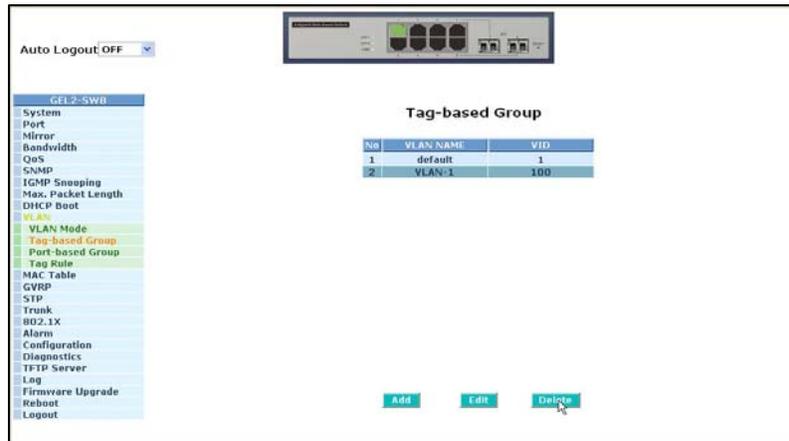


Figure 5.32 – Tag-based Group

Edit a group:

Select a group entry and select **Edit**. This allows you to modify the group's description, SYM-VLAN and member set.

5.16.3 Port-Based Group

Function name:

Port-based Group Configuration

Function description:

Displays the information for the existing port-based VLAN groups. Use this function to create, edit and delete a port-based VLAN group. Add a new VLAN group by inputting a new VLAN name.

Parameter description:

VLAN Name:

Valid letters are A-Z, a-z, 0-9, “ - “ and “ _ ” characters. The maximum length is 15 characters.

Member:

Used to enable or disable a member port. **Enable** means the port is a member of the VLAN. Select the check box () beside the port x to enable it.

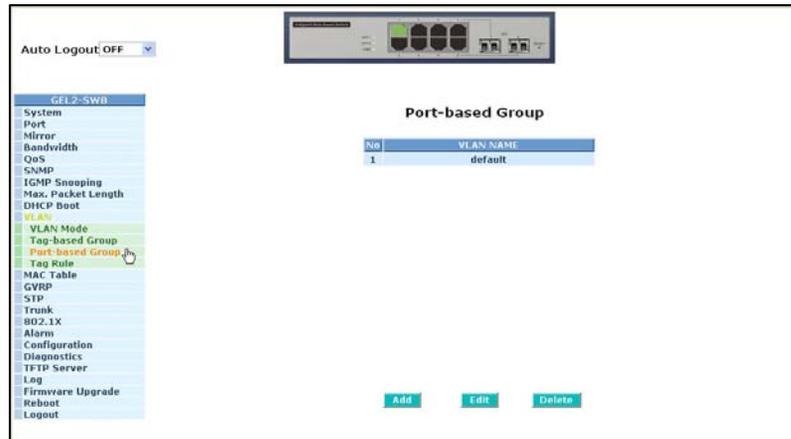


Figure 5.33 – Port-based Group

Add Group:

Create a new port-based VLAN. Input the VLAN name and choose the group member by selecting the check box beside the port number. Select **Apply** so the setting will take effect.

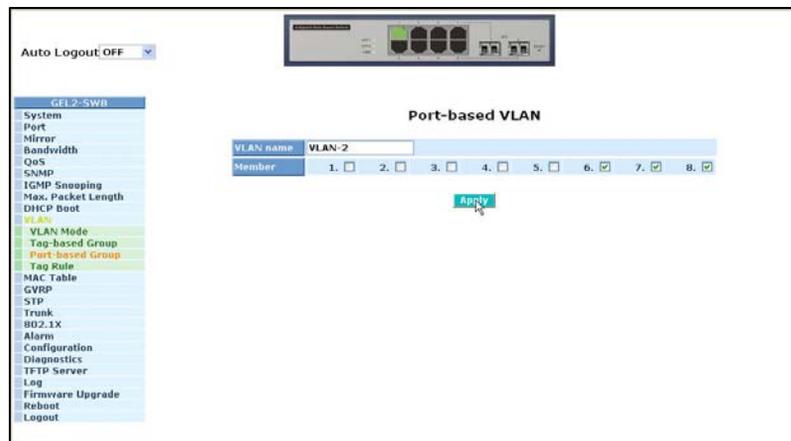


Figure 5.34 – Port-based VLAN

Delete Group:

Use **Delete** to remove the selected group entry from the port-based group table.

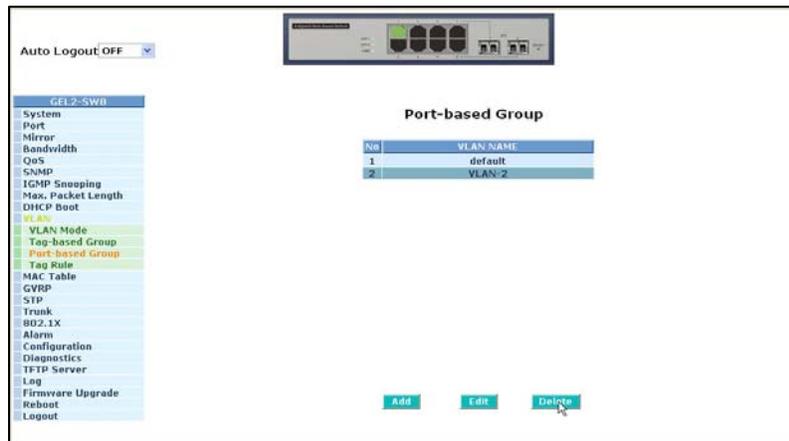


Figure 5.35 – Port-based Group

Edit a group:

To edit a group entry, use **Edit**. This allows you to modify a group's description and member set.

5.16.4 Tag Rule

Function name:

Tag Rule

Function description:

With the VLAN Tag Rule Setting, input a VID number to each port. The range of VID number is from 1 to 4094. You can choose ingress filtering rules for each port. There are two ingress filtering rules which can be applied to the switch:

- Ingress Filtering Rule 1: Forward only packets with VID matching this port's configured VID.
- Ingress Filtering Rule 2: Drop untagged frame. Select the role of each port as Access, Trunk, or Hybrid.

Parameter description:

Port 1-8:

Port number.

PVID:

This PVID range will be 1-4094. Before you set number x as PVID, you have to create a tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet. The packet then will be forwarded as the tagged packet with VID y.

Rule 1:

Forward only packets with VID matching this port's configured VID. You can apply Rule 1 to filter unwanted traffic. In Rule 1, in order to determine whether or not to forward a packet, the port checks to see if it is a member of the VLAN. For example, if port 1 receives a tagged

packet with VID=100 (VLAN name=VLAN100), and if rule 1 is enabled, the switch will check if port 1 is a member of VLAN100. If it is, the received packet is forwarded; otherwise, the received packet is dropped.

Rule 2:

Drop untagged frame. You can configure a given port to accept all frames (Tagged and Untagged) or only tagged frames. If you choose all frames, the packets with tagged or untagged will be processed. If you choose only tagged frames, only the packets carrying VLAN tag will be processed. The remainder of the packets will be discarded.

Note: For example, if rule 1 is enabled, port 1 receives an untagged packet, the switch will apply the PVID of port 1 to tag this packet. The packet then will be forwarded. But if the PVID of port 1 is 100 and port 1 is not member of VLAN 100, the packet will be dropped.

Role:

This is an egress rule of the port. You can choose Access, Trunk or Hybrid. Trunk means the outgoing packets must carry VLAN tag header. Access means the outgoing packets carry no VLAN tag header. If packets have double VLAN tags, one will be dropped and the other will still be left. Hybrid, is similar to Trunk, and both of them will tag-out. When the port is set to Hybrid, its packets will be untagged out if the VID of the outgoing packets with tag is the same as the one in the field of Untag VID of this port.

Untag VID:

Valid range is 1~4094. Works only when Role is set to Hybrid.



Figure 5.36 – VLAN Tag Rule

5.17 MAC Table

MAC Table Configuration gathers many functions, including MAC Table Information, MAC Table Maintenance, Static Forward, Static Filter and MAC Alias, which cannot be categorized to some function type. They are described below.

Function name:

MAC Table Information

Function Description:

Displays the static or dynamic learning MAC entry and the state for the selected port.

Parameter description:

Port:

Select the port.

Search:

Set up the MAC entry.

The default is ??-??-??-??-??-??

MAC:

Displays the MAC address of the entry selected from the searched MAC entries table.

Alias:

Set up the Alias for the selected MAC entry.

Set Alias:

Save the Alias of MAC entry you set up.

Search:

Find the entry that meets your setup.

Previous Page:

Move to the previous page.

Next Page:

Move to the next page.

Alias:

The Alias of the searched entry.

MAC Address:

The MAC address of the searched entry.

Port:

The port that exists in the searched MAC Entry.

VID:

VLAN Group that MAC Entry exists.

State:

Displays the method for this MAC entry. It may show "Dynamic MAC" or "Static MAC".



Figure 5.37 – MAC Table Information

Function Name:

MAC Table Maintenance

Function Description:

This function allows the user to set up the processing mechanism of the MAC Table. An idle MAC address exceeding MAC address age-out time will be removed from the MAC Table. The range of age-out time is 10-65535 seconds, and the setup of this time will have no effect on static MAC addresses.

Parameter description:

Aging Time:

Deletes a MAC address which is idling for a period of time from the MAC Table, which will not affect static MAC address. Range of MAC address aging time is 10-65535 seconds. The default aging time is 300 seconds.

Flush:

Remove all entries that do not belong to the static MAC entry from the MAC table.



Figure 5.38 – MAC Maintenance

Function Name:

Static Forward

Function Description:

Static Forward is a function that allows the user in the static forward table to access a specified port of the switch. The static forward table associated with a specified port of a switch is set up by manually inputting MAC address and an alias' name.

When a MAC address is assigned to a specific port, all of the switch's traffic is sent to this MAC address will be forwarded to this port.

For adding a MAC address entry in the allowed table, fill in four parameters: MAC address, associated port, VID and Alias. Select the existing MAC address entry, and select **Delete** for removal.

Parameter description:

MAC:

Six-byte Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,

00 – 40 - C7 - D6 – 00 - 01

Port No:

Port number of the switch. It is 1~8.

VID:

VLAN identifier. This will be filled only when tagged VLAN is used. Valid range is 1 ~ 4094.

Alias:

Assigned MAC alias name.

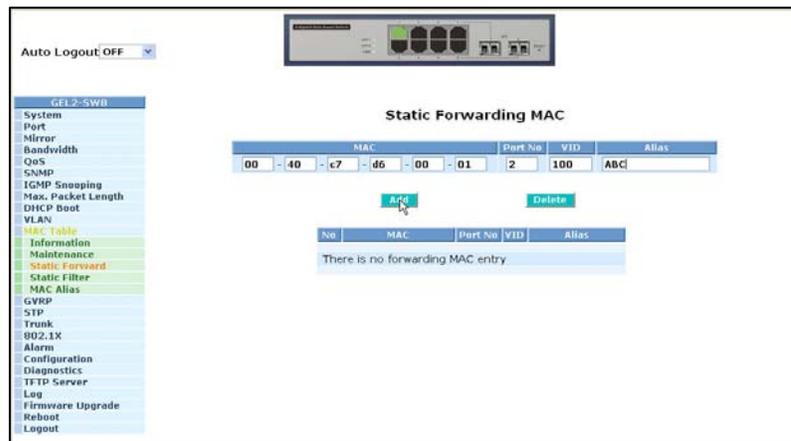


Figure 5.39 – Static Forwarding MAC

Function name:

Static Filter

Function Description:

Static Filter is a function that denies the packet forwarding if the packet's MAC Address is listed in the filtering Static Filter table. Maintain the table by filling in MAC Address, VID (VLAN ID) and Alias fields individually. You can delete the entry by using **Delete**.

Parameter description:

MAC:

Six-byte Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,

00 - 40 - C7 - D6 - 00 - 02

VID:

VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.

Alias:

Assigned MAC alias name.

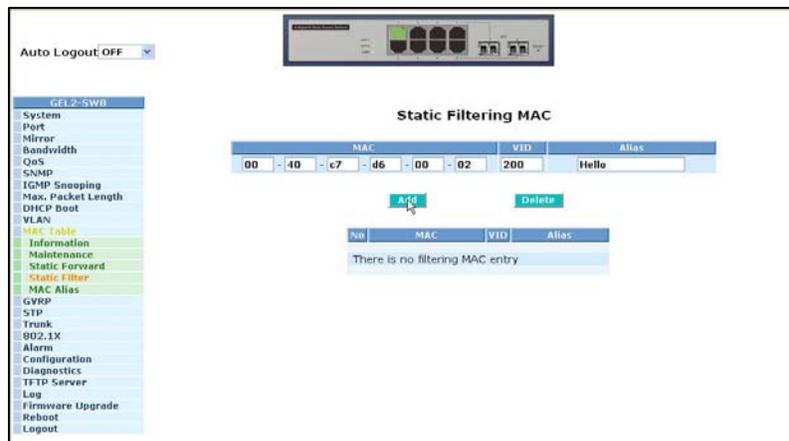


Figure 5.40 – Static Forwarding MAC

Function name:

MAC Alias

Function description:

MAC Alias function is used to assign MAC address an English name. This will help identify which MAC address belongs to a user in the illegal access report. At the initial time, all pairs of the existing alias name and MAC address are shown.

There are three MAC alias functions in this function folder, including MAC Alias Add, MAC Alias Edit and MAC Alias Delete. Use **Create/Edit** to add/modify a new or an existing alias name for a specified MAC address, or mark an existing entry for deletion. Alias name must be composed of A-Z, a-z and 0-9 only and has a maximal length of 15 characters.

Function name:

MAC Alias Create/Edit or Delete

Function description:

In the MAC Alias function, MAC Alias Add/Edit function is used to let you add or modify an association between MAC address and an English name. Select **Create/Edit** to add a new record with name.

Select the MAC Alias Delete function to remove an alias name from a MAC address. You can select an existing MAC address or alias name for removal.



Figure 5.41 – MAC Alias

Parameter description:

MAC Address:

Six-byte Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,

00 – 40 - C7 - D6 – 00 - 01

Alias:

MAC alias name you assign.

Note: If there are too many learned MAC addresses, it is recommended to input the MAC address and alias name directly.

5.18 GVRP Configuration

GVRP is an application based on the Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the group membership information of the VLANs. GVRP provides the VLAN registration service through a GARP application. The GARP Information Declaration (GID) is used to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machine maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate these information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

GVRP cannot be enabled unless the VLAN mode is set to Tag based.

GVRP is disabled by default.

The following three functions are supported with GVRP:

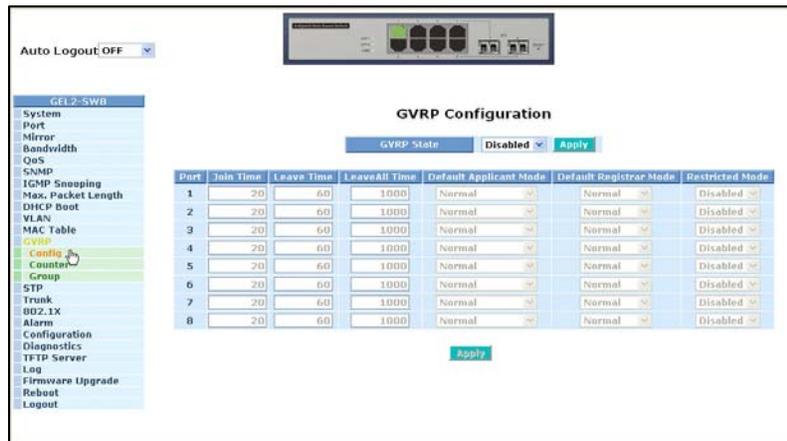


Figure 5.42 – GVRP Configuration

Function name:

GVRP Config

Function description:

The function of GVRP Config is used to configure each port's GVRP operation mode. There are seven parameters to be configured which are described below.

Parameter description:

GVRP State Setting:

This function allows you to enable or disable the GVRP function. Use the drop down list and select the **Downward** arrow key to choose **Enable** or **Disable**. Select **Apply** and the function will take effect immediately.

Join Time:

Used to declare the Join Time in unit of centisecond. Valid time range: 20 –100 centisecond, Default: 20 centisecond.

Leave Time:

Used to declare the Leave Time in unit of centisecond. Valid time range: 60 –300 centisecond, Default: 60 centisecond.

Leave All Time:

A registered device will be de-registered at the end of this time period. If someone still issues a new join, then a registration will be kept in the switch. Valid range: 1000-5000 unit time, Default: 1000 unit time.

Default Applicant Mode:

There are two modes that indicate the type of participant: normal participant and non-participant.

Normal:

In the **normal participant** mode, the switch participates normally in GARP protocol exchanges. The default setting is **Normal**.

Non-Participant:

In the **non-participant** mode, the switch does not send or reply any GARP messages. The switch listens for messages and reacts for the received GVRP BPDU.

Default Registrar Mode:

There are three types of parameters for **registrar** mode: registrar administrative control value, normal registrar, fixed registrar and forbidden registrar.

Normal:

The Registrar responds normally to incoming GARP messages. The default setting is Normal.

Fixed:

The Registrar ignores all GARP messages, and all members remain in the registered (IN) state.

Forbidden:

The Registrar ignores all GARP messages, and all members remain in the unregistered (EMPTY) state.

Restricted Mode:

This function is used to restrict dynamic VLAN be created when this port received GVRP PDU. There are two modes: disable and enable.

Disabled:

In this mode, the switch dynamic VLAN will be created when this port received GVRP PDU. The default setting is Normal.

Enabled:

In this mode, the switch does not create dynamic VLAN when this port received GVRP PDU. Except received dynamic VLAN message of the GVRP PDU is an existed static VLAN in the switch. This port will be added into the static VLAN members dynamically.

Function name:

GVRP Counter

Function description:

GVRP counters are divided into Received and Transmitted categories which allows you monitor the GVRP actions. They are GARP packets.

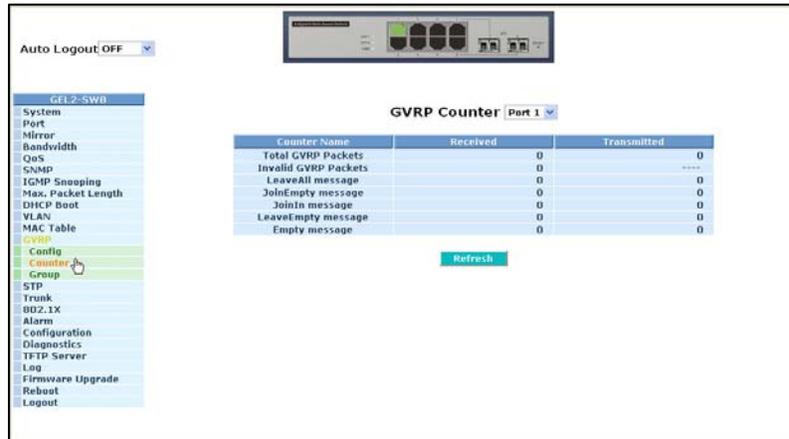


Figure 5.43 – GVRP Counter

Parameter description:

Received:

Total GVRP Packets:

Total GVRP BPDU received by the GVRP application.

Invalid GVRP Packets:

Number of invalid GARP BPDU received by the GARP application.

LeaveAll Message Packets:

Number of GARP BPDU with Leave All message received by the GARP application.

JoinEmpty Message Packets:

Number of GARP BPDU with Join Empty message received by the GARP application.

JoinIn Message Packets:

Number of GARP BPDU with Join In message received by the GARP application.

LeaveEmpty Message Packets:

Number of GARP BPDU with Leave Empty message received by the GARP application.

Empty Message Packets:

Number of GARP BPDU with Empty message received by the GARP application.

Transmitted:

Total GVRP Packets:

Total GARP BPDU transmitted by the GVRP application.

Invalid GVRP Packets:

Number of invalid GARP BPDU transmitted by the GVRP application.

LeaveAll Message Packets:

Number of GARP BPDU with Leave All message transmitted by the GARP application.

JoinEmpty Message Packets:

Number of GARP BPDU with Join Empty message transmitted by the GARP application.

JoinIn Message Packets:

Number of GARP BPDU with Join In message transmitted by the GARP application.

LeaveEmpty Message Packets:

Number of GARP BPDU with Leave Empty message transmitted by the GARP application.

Empty Message Packets:

Number of GARP BPDU with Empty message transmitted by the GARP application.

Function name:

GVRP Group Information

Function description:

To show the dynamic group member and their information.

Parameter description:

VID:

VLAN identifier. When a GVRP group is created, each dynamic VLAN group owns its VID. Valid range is 1 ~ 4094.

Member Port:

Those are the members belonging to the same dynamic VLAN group.

Edit Administrative Control:

When you create a GVRP group, use the Administrative Control function to change the Applicant Mode and Registrar Mode of a GVRP group member.

Refresh:

Refresh function allows you to see current GVRP group status.



Figure 5.44 – GVRP VLAN

5.19 Spanning Tree Configuration (STP) Configuration

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1D) used to avoid loops in switched networks. When STP is enabled, only one path is active between any two nodes on the network at a time. Once Spanning Tree Protocol has been enabled, advanced functions can be configured. It is recommended that STP is enabled to ensure a single active path on the network.

5.19.1 STP Status

Function name:

STP Status

Function description:

Spanning Tree Status displays the current status of 12 parameters. The 12 parameters are described below:

Parameter description:

STP State:

Displays the current STP Enabled / Disabled status. Default is “Disabled”.

Bridge ID:

Displays the switch’s bridge ID which is the MAC address of this switch.

Bridge Priority:

Displays the switch’s current bridge priority setting. Default is 32768.

Designated Root:

Displays the root bridge ID of this network segment. If this switch is a root bridge, the “Designated Root” will show this switch’s bridge ID.

Designated Priority:

Displays the current root bridge priority.

Root Port:

Displays port number connected to root bridge with the lowest path cost.

Root Path Cost:

Displays the path cost between the root port and the designated port of the root bridge.

Current Max. Age:

Displays the current root bridge maximum age time. Maximum age time is used to monitor STP topology. When a bridge does not receive a hello message from root bridge until the maximum age time is counted down to 0, the bridge will treat the root bridge as malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges.

All bridges in the LAN will re-learn and determine the root bridge. Maximum Age time is assigned by root bridge in unit of seconds. Default is 20 seconds.

Current Forward Delay:

Displays the current root bridge forward delay time. The value of Forward Delay time is set by root. The Forward Delay time is defined as the time spent from Listening state moved to Learning state or from Learning state moved to Forwarding state of a port in bridge.

Hello Time:

Displays the current hello time of the root bridge. Hello time is a time interval specified by root bridge. It is used to request all other bridges periodically sending hello message to the bridge attached to its designated port.

STP Topology Change Count:

STP Topology Change Count expresses the time spent in a unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once the STP change is converged, the Topology Change count will be reset to 0. The figures showing in the screen may not be the exact time it spent but very close to, because the time is eclipsing.

Time Since Last Topology Change:

Time Since Last Topology Change is the accumulated time in unit of seconds the STP has been since the last STP Topology Change was made. When Topology Change is initiated again, the counter will be reset to 0 and resume counting once the STP topology change is completed.

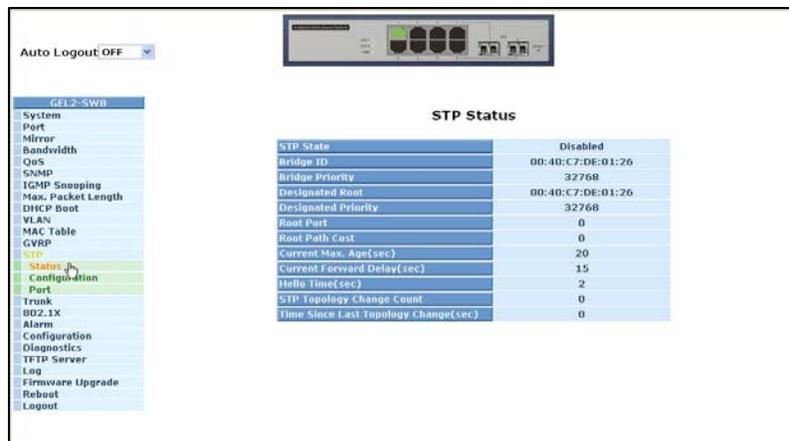


Figure 5.45 – STP Status

5.19.2 STP Configuration

STP includes Rapid Spanning Tree Protocol (RSTP). STP has six parameters to be configured. These parameters are described below.

Function name:

STP Configuration

Function description:

Set the following Spanning Tree parameters to control STP function (enable/disable). Select mode RSTP/STP and affect STP state machine behavior to send BPDU in the switch. The default setting of STP is **Disable**.

Parameter description:

Spanning Tree Protocol:

Set 802.1W Rapid STP function Enable / Disable. Default is "Disable"

Bridge Priority:

The lower the number for bridge priority, the higher the priority it will have. Usually, the bridge with the highest bridge priority is the root. If you want this switch to be the root bridge, set the value lower than that of the bridge in the LAN. The valid value is 0 ~ 61440. The default is 32768.

Hello Time:

Hello Time is used to determine the periodic time to send normal BPDU from designated ports among bridges. It decides how long a bridge should notify other bridges to say that it is up and connected. If the GSM switch is the root bridge of the LAN, for example, all other bridges will use the hello time assigned by this switch to communicate with each other. The valid value is 1 ~ 10 in unit of second. The default is 2 seconds.

Max. Age:

When the GSM switch is the root bridge, the whole LAN will apply the number set by the switch as their maximum age time. When a bridge received a BPDU originating from the root bridge and if the message age conveyed in the BPDU exceeds the Max. Age of the root bridge, the bridge will treat the root bridge as malfunctioning and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges in the LAN will re-calculate to determine who the root bridge is. The valid value of Max. Age is 6 ~ 40 seconds. Default is 20 seconds.

Forward Delay:

You can set the root bridge forward delay time. This figure is set by the root bridge only. The forward delay time is defined as the time spent from Listening state moved to Learning state and also from Learning state moved to Forwarding state of a port in bridge. The forward delay time contains two states, Listening state to Learning state and Learning state to Forwarding state. It assumes that forward delay time is 15 seconds, then total forward delay time will be 30 seconds.

The valid value is 4 ~ 30 seconds, default is 15 seconds.

Force Version:

Two options are offered for the STP algorithm. One is RSTP and the other is STP. If STP is chosen, RSTP will run as a legacy STP. The switch supports RSTP (802.1w) which is backward compatible with STP (802.1d).

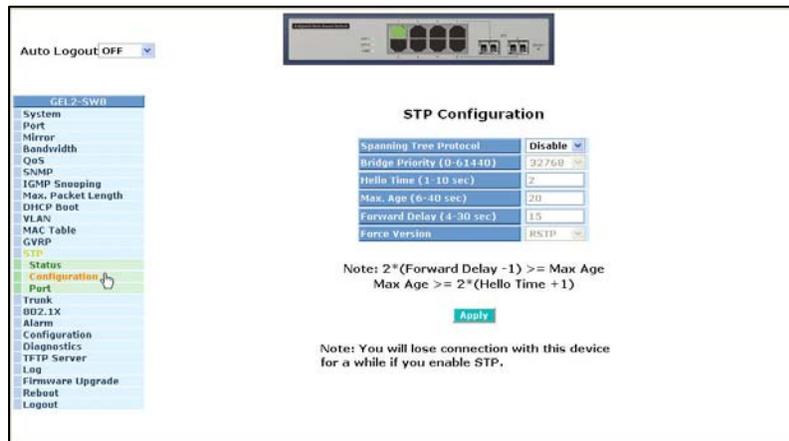


Figure 5.46 – STP Configuration

5.19.3 STP Port Configuration

Function name:

STP Port Setting

Function description:

In the STP Port Setting, one item selection and five parameters are available for setup. You can disable and enable each port. You can set “Path Cost” and “Priority” for each port and set “Admin Edge Port” and “Admin Point To Point”.

Parameter description:

Port Status:

Displays the current state of a port for viewing only. There are three possible states. (according to 802.1w specification)

- DISCARDING state indicates that this port can neither forward packets nor contribute learning knowledge.
- LEARNING state indicates this port can now contribute its learning knowledge but cannot forward packets.
- FORWARDING state indicates this port can both contribute its learning knowledge and forward packets normally.

Note: Three other states (Disable state, BLOCKING state and LISTENING state) defined in the 802.1d specification are now represented as DISCARDING state.

Path Cost Status:

The contribution value of the path through this port to Root Bridge. STP algorithm determines a best path to Root Bridge by calculating the sum of path cost contributed by all ports on this path. A port with a smaller path cost value would become the Root Port.

Configured Path Cost:

The range is 0 – 200,000,000. If the path cost is set to zero, the STP will get the recommended value resulted from auto-negotiation of the link accordingly and display this value in the field of Path Cost Status. Otherwise, the value set by the administrator set up will be displayed.

802.1w RSTP recommended value: (Valid range: 1 – 200,000,000)

10 Mbps : 2,000,000

100 Mbps : 200,000

1 Gbps : 20,000

Default: 0

Priority:

Port Priority and Port Number are combined to form the Port ID. Port IDs are often compared in order to determine which port of a bridge would become the Root Port. The range is 0 – 240.

Default is 128.

Admin Edge Port:

If you select **Yes**, this port will be an edge port. An Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology keeps unchanged. Unlike the designate port or root port though, an edge port will transit to a normal spanning-tree port immediately if it receives a BPDU.

Default: No

Admin Point To Point:

A port is a point-to-point link, from RSTP's view, if it is in full-duplex mode. It is a shared link if it is in half-duplex mode. RSTP fast convergence can only happen on point-to-point links and on edge ports. This can expedite the convergence because this will have the port fast transitioned to forwarding state.

There are three parameters, Auto, True and False, used to configure the type of the point-to-point link. If the parameter is configured to Auto, RSTP will use the duplex mode resulting from the auto-negotiation. If it goes into half-duplex, the port will not transit to Forwarding state. If it is set as True, the port is treated as point-to-point link by RSTP and unconditionally transitioned to Forwarding state. If it is set to False, fast transition to Forwarding state will not occur on this port.

Default: Auto

M Check:

Migration Check. Forces the port sending out an RSTP BPDU instead of a legacy STP BPDU at the next transmission. The only benefit of this operation is to make the port quickly get back to act as an RSTP port. Select **M Check** to send a RSTP BPDU from the port you specified.

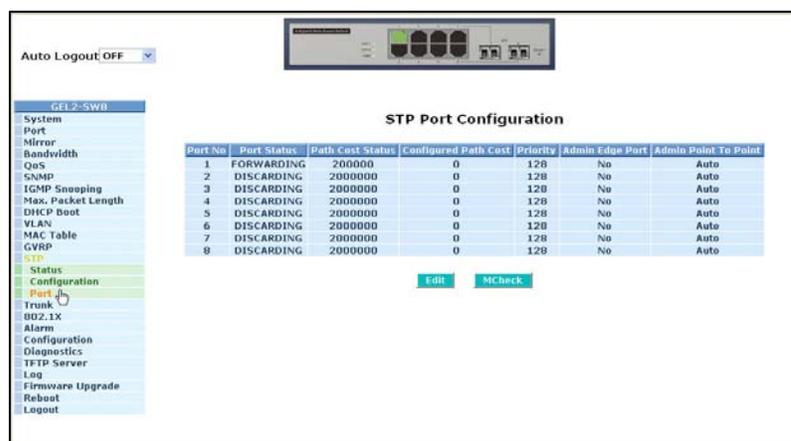


Figure 5.47 – STP Port Configuration

5.20 Trunking Configuration

The Port Trunking Configuration is used to configure the settings of Link Aggregation. More than one port can be bundled with the same speed, full duplex and the same MAC to be a single logical port. The logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port.

The switch supports two types of port trunking methods:

LACP:

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID (1~8) to form a logic “trunked port”. The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a “trunk group” (also called aggregator). LACP is safer than the other trunking method - static trunk.

The switch LACP does not support the followings:

- Link Aggregation across switches
- Aggregation with non-IEEE 802.3 MAC link
- Operating in half-duplex mode
- Aggregate the ports with different data rates

Static Trunk:

Ports using Static Trunk as their trunk method can choose their unique Static Group ID (also 1~8, this Static group ID can be the same with another LACP group ID) to form a logic “trunked port”. The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without handshaking with its peer port. This is a disadvantage because the peer ports of the static trunk group may not know that they should be aggregate together to form a “logic trunked port”. Using Static Trunk on both end of a link is strongly recommended. Low speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

The switch supports a maximum of eight trunk groups for LACP and additional eight trunk groups for Static Trunk. In the system capability view, only eight “real trunked” groups are supported. An LACP trunk group with more than one ready member-ports is a “real trunked” group. An LACP trunk group with only one or less than one ready member-ports is not a “real trunked” group. Any Static trunk group is a “real trunked” group.

Per Trunking Group supports a maximum of 12 ready member-ports. Please note that some decisions will automatically be made by the system while you are configuring your trunking ports. Some configuration examples are listed below:

- 12 ports have already used Static Trunk Group ID 1, the 13th port willing to use the same Static Trunk Group ID will be automatically set to use the “None” trunking method and its Group ID will turn to 0. This means the port won’t aggregate with other ports.
- 14 ports use LACP Trunk Group ID 1. At most 12 ports can aggregate together and transit into the ready state.
- A port using the “None” trunking method or Group ID 0 will be automatically set to use the “None” trunking method with Group ID 0.

Function name:

Port Setting/Status

Function description:

Port setting/status is used to configure the trunk setting for the ports.

Parameter description:

Method:

This determines the method a port uses to aggregate with other ports.

None:

A port does not aggregate with other ports.

LACP:

A port uses LACP as its trunk method to aggregate with other ports also using LACP.

Static:

A port uses Static Trunk as its trunk method to aggregate with other ports also using Static Trunk.

Group:

Ports choosing the same trunking method other than “None” must be assigned a unique Group number (i.e. Group ID, valid value is from 1 to eight) so they can aggregate with each other.

Active LACP:

This field is only available when a port’s trunking method is LACP.

Active:

An Active LACP port begins to send LACPDU to its link partner as soon as the LACP protocol entity takes control of this port.

Passive:

A Passive LACP port will not actively send LACPDU out until it receives an LACPDU from its link partner.

Aggr:

Aggr is an abbreviation of “aggregator”. Every port is also an aggregator, and its own aggregator ID is the same as its own port number. An aggregator is a representative of a trunking group. Ports with same Group ID and using same trunking method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest port number within the trunking group.

Status:

This field represents the trunking status of a port which uses a trunking method other than “None”. It also represents the management link status of a port which uses the “None” trunking method. “---” means “not ready”

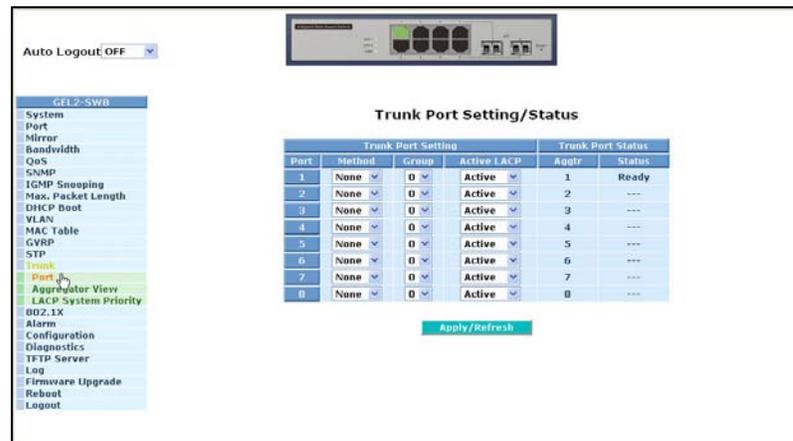


Figure 5.48 – Trunk Port Setting/Status

Function name:

Aggregator View

Function description:

To display the current port trunking information from the aggregator point of view.

Parameter description:

Aggregator:

Displays the aggregator ID (from 1 to 8) of every port. Every port is also an aggregator, and its own aggregator ID is the same as its own port number.

Method:

Displays the method a port uses to aggregate with other ports.

Member Ports:

Displays all member ports of an aggregator (port).

Ready Ports:

Displays only the ready member ports within an aggregator (port).

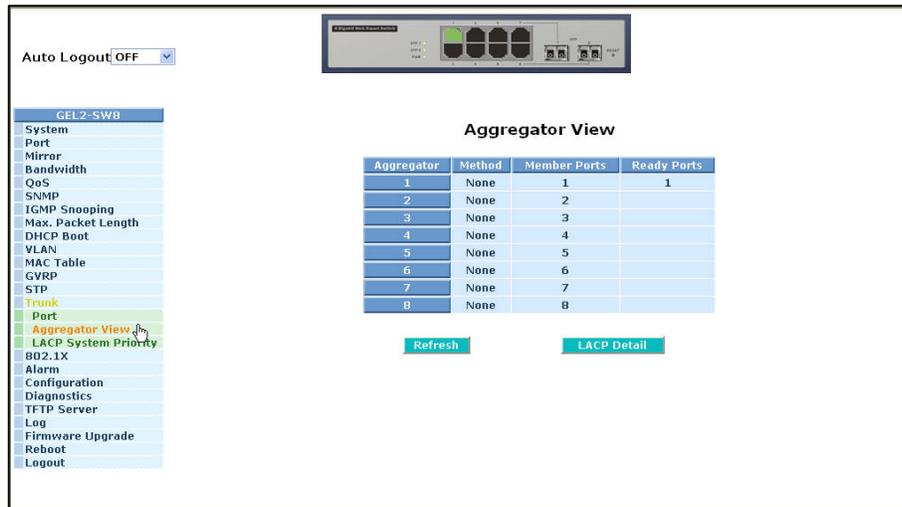


Figure 5.49 – Aggregator View

Function name:

LACP Detail (LACP Aggregator Detailed Information)

Function description:

Displays the detailed information of the LACP trunking group.

Parameter description:

Actor:

The switch you are using to view LACP.

Partner:

The peer system from the aggregator's view.

System Priority:

Displays the System Priority of a system ID.

MAC Address:

Displays the MAC Address of a system ID.

Port:

Displays the port number of an LACP port ID.

Key:

Displays the key value of the aggregator. The key value is determined by the LACP protocol entity and can't be set through management.

Trunk Status:

Displays the trunk status of a single member port.”---“ means “not ready”

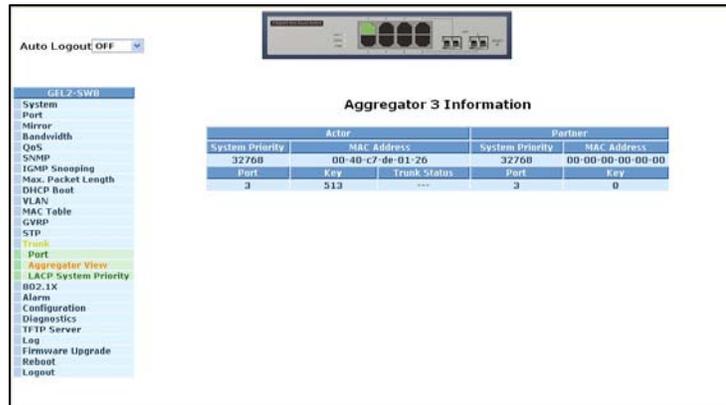


Figure 5.50 – Aggregator Information

Function name:

LACP System Priority

Function description:

Used to set the priority of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system supports LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value. The System Priority can be set by the user. Its range is from 1 to 65535. Default: 32768



Figure 5.51 – LACP System Priority

5.21 802.1X Configuration

802.1X port-based network access control provides a method to restrict users to access network resources via authenticating user's information. This restricts users from gaining access to the network resources through a 802.1X-enabled port without authentication. To access the network through a port under 802.1X control, you must first input your account name for authentication and wait to gain authorization before sending or receiving any packets from a 802.1X-enabled port.

Before the devices or workstations can access the network resources through the ports under 802.1X control, the devices or workstations must send an authentication request to the authenticator. The authenticator passes the request to the authentication server to authenticate and verify, and the server informs the authenticator to grant the request for authorization for the ports.

According to IEEE 802.1X, there are three components are implemented:

- Supplicant
- Authenticator
- Authentication server shown in Figure 5.52.

Supplicant:

- An entity authenticated by an authenticator. Used to communicate with the Authenticator PAE (Port Access Entity) by exchanging the authentication message when the Authenticator PAE performs a request.

Authenticator:

- An entity facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate itself at a configured time period. Once re-authenticating has begun, the controlled port remains in the authorized state until re-authentication fails.
- A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass packets when the authenticator PAE is authorized. Otherwise, an uncontrolled port will unconditionally pass the packets with PAE group MAC address, which has the value of 01-80-c2-00-00-03 and will not be forwarded by MAC bridge, at any time.

Authentication server:

- A device provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.
- The overview of operation flow for the Figure 5.52 is quite simple. When Supplicant PAE issues a request to Authenticator PAE, Authenticator and Supplicant exchanges authentication message. Then, Authenticator passes the request to RADIUS server to verify. Finally, RADIUS server replies if the request is granted or denied.
- During the authentication process, the message packets, encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the message to authentication server using EAP encapsulation. Before successfully authenticating, the supplicant can only touch

the authenticator to perform authentication message exchange or access the network from the uncontrolled port.

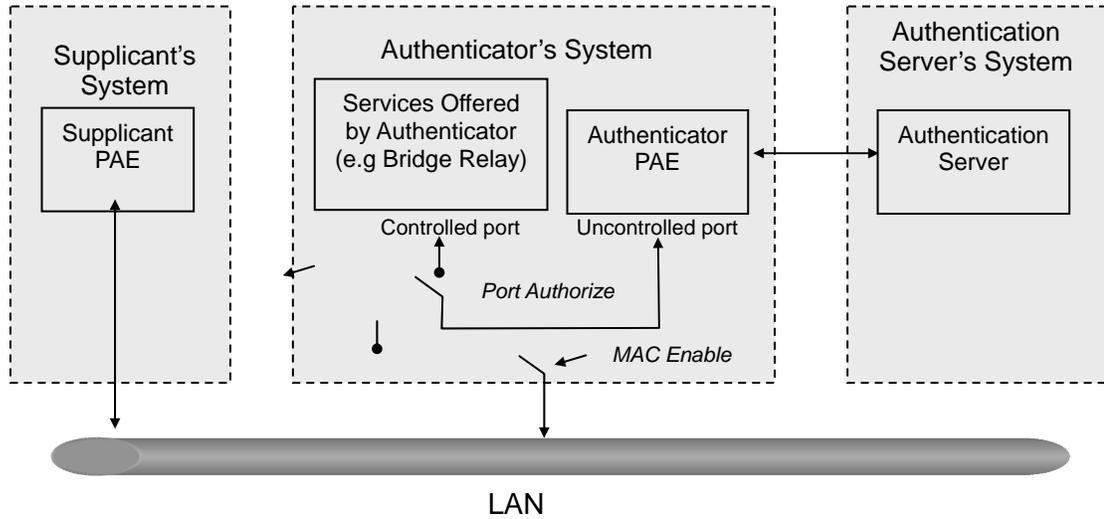


Figure 5.52

Figure 5.53 represents a typical configuration; a single supplicant, an authenticator and an authentication server. B and C are in the internal network, D is the Authentication server running RADIUS, switch at the central location which acts as Authenticator connecting to PC A. A is a PC outside the controlled port, running Supplicant PAE. In this case, PC A wants to access the services on device B and C. It first must exchange the authentication message with the authenticator on the port it connected via EAPOL packet. The authenticator transfers the supplicant's credentials to Authentication server for verification. If successful, the authentication server will notify the authenticator. PC A is then allowed to access B and C via the switch. If there are two switches directly connected together instead of a single one, the link ports connecting the two switches may have to perform two port roles: authenticator and supplicant, because the traffic is bi-directional.

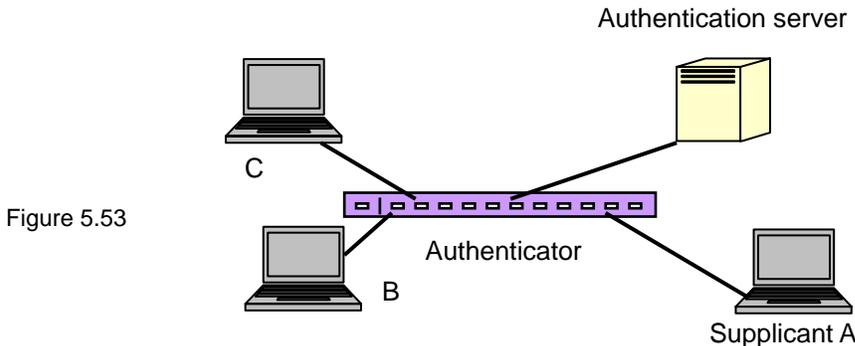


Figure 5.53

Figure 5.54 illustrates the procedure of 802.1X authentication. There are steps for the login based on 802.1X port access control management. The protocol used in the right side is EAPOL and the left side is EAP.

1. At the initial stage, supplicant A is unauthenticated so the port acting as an authenticator is in unauthorized state. Access is blocked in this stage.
2. Either authenticator or supplicant can initiate the message exchange. If supplicant initiates the process, it sends EAPOL-start packet to the authenticator PAE and authenticator will immediately respond EAP-Request/Identity packet.
3. The authenticator periodically sends EAP-Request/Identity to the supplicant to request the identity it wants to be authenticated.
4. If the authenticator doesn't send EAP-Request/Identity, the supplicant will initiate EAPOL-beginning the process by sending it to the authenticator.
5. The Supplicant replies an EAP-Response/Identity to the authenticator. The authenticator will embed the user ID into Radius-Access-Request command and send it to the authentication server for identity confirmation.
6. After receiving the Radius-Access-Request, the authentication server sends Radius-Access-Challenge to the supplicant asking for inputting user password via the authenticator PAE.
7. The supplicant will convert the user password into the credential information, perhaps, in MD5 format and replies an EAP-Response with this credential information as well as the specified authentication algorithm (MD5 or OTP) to Authentication server via the authenticator PAE. As per the value of the type field in message PDU, the authentication server knows which algorithm should be applied to authenticate the credential information, EAP-MD5 (Message Digest 5) or EAP-OTP (One Time Password) or other algorithm.
8. If user ID and password is correct, the authentication server will send a Radius-Access-Accept to the authenticator. If not correct, the authentication server will send a Radius-Access-Reject.
9. When the authenticator PAE receives a Radius-Access-Accept, it will send an EAP-Success to the supplicant. At this time, the supplicant is authorized and the port is connected to the supplicant and is under 802.1X control in the authorized state. The supplicant and other devices connected to this port can access the network. If the authenticator receives a Radius-Access-Reject, it will send an EAP-Failure to the supplicant. This means the supplicant has failed to authenticate. The port connected is in the unauthorized state, the supplicant and the devices connected to this port won't be allowed to access the network.
10. When the supplicant issues an EAP-Logoff message to Authentication server, the active port being used is set to unauthorized.

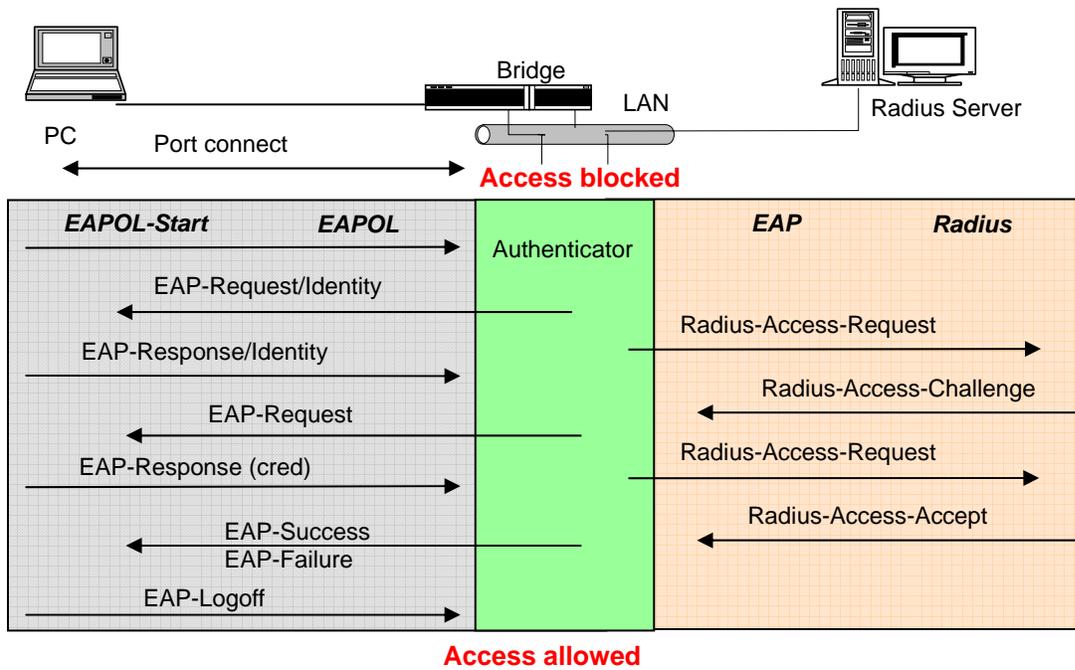


Figure 5.54

The type of authentication supported in the switch is multihost 802.1x. In this mode, once a supplicant is authorized, the devices connected to this port can access the network resources.

802.1X Port-based Network Access Control function supported by the switch is complex. Support, by basic multihost mode, can distinguish the device's MAC address and its VID. The following table summarizes the combination of the authentication status and the port status versus the status of port mode, set in 802.1X Port mode, port control state, set in 802.1X port setting. Entry Authorized means MAC entry is authorized.

Port Mode	Port Control	Authentication	Port Status
Disable	Don't Care	Don't Care	Port Uncontrolled
Multihost	Auto	Successful	Port Authorized
Multihost	Auto	Failure	Port Unauthorized
Multihost	ForceUnauthorized	Don't Care	Port Unauthorized
Multihost	ForceAuthorized	Don't Care	Port Authorized

Table 5-3

Function name:

802.1X State Setting

Function description:

This function is used to configure the global parameters for RADIUS authentication in 802.1X port security application.

Parameter description:

Radius Server:

RADIUS server IP address for authentication.

Default: 192.168.1.1

Port Number:

The port number to communicate with RADIUS server for the authentication service. The valid value ranges 1-65535.

Default port number is 1812.

Secret Key:

The secret key between authentication server and authenticator. It is a string with the length 1 – 31 characters. The character string may contain upper case, lower case and 0-9 without spaces.

Default: Radius



Figure 5.55 – 802.1X State Setting

Function name:

802.1X Mode Setting

Function description:

Set the operation mode of 802.1X for each port. In this device, multihost operation mode is supported.

Parameter description:

Port Number:

Indicate which port is selected to configure the 802.1X operation mode.

802.1X Mode:

802.1X operation mode. There are two options, including Disable and Multihost mode. Default is Disable.

- Disable

The chosen port acts as a plain port, which means 802.1X port access control does not work on the port.

- 802.1X with multihost

In multihost mode, the devices connected to this port can access the network, once a supplicant is authorized.



Figure 5.56 – 802.1X Mode Setting

Function name:

Port Security Management

Function description:

Displays each port status. In multihost mode, the port number and its status, authorized or unauthorized are displayed.

Parameter description:

Disable Mode:

If Disable mode is selected for a port, in the function 802.1X Port Mode Configuration, the port is in the uncontrolled port state and does not apply the 802.1X authenticator. Any node attached to this port can access the network without the admittance of 802.1X authenticator. The Port Status will display the following screen.

Port Number:

The port number to be chosen to show its 802.1X Port Status. The valid number is Port 1 – 8.

Port Status:

The current 802.1X status of the port. In Disable mode, this field is Disabled.

802.1X with Multihost mode:

Select 802.1X with Multihost mode for a port. With the function 802.1X Port Mode Configuration, devices can access the network through this port once the authenticator is authorized. The Port Status will display the following screen. If the port is granted to access the network, the port status is authorized, otherwise, unauthorized.



Figure 5.57 – Port Security Management

Function name:

Parameter Setting

Function description:

This function is used to configure the parameters for each port in 802.1X port security application. Refer to the following parameters description for details.

Parameter description:

Port:

The port number to be selected for configuring its associated 802.1X parameters which are Port control, reAuthMax, txPeriod, Quiet Period, reAuthEnabled, reAuthPeriod, max. Request, suppTimeout, serverTimeout and Controlled direction.

Port Control:

This is used to set the operation mode for authorization. There are three types of operation mode supported, ForceUnauthorized, ForceAuthorized, Auto.

- ForceUnauthorized:

The controlled port remains in the unauthorized state.

- ForceAuthorized:

The controlled port remains in the authorized state.

- Auto:

The controlled port is set to be in authorized state or unauthorized state depends on the result of the authentication exchange between the authentication server and the supplicant.

Default: Auto

reAuthMax (1-10):

The number of authentication attempts that is permitted before the port becomes unauthorized.

Default: 2

txPeriod (1-65535 s):

A time period to transmitted EAPOL PDU between the authenticator and the supplicant.

Default: 30

Quiet Period (0-65535 s):

A period of time during in which access the supplicant will not be attempted.

Default: 60 seconds

reAuthEnabled:

Choose whether regular authentication will take place in this port.

Default: ON

reAuthPeriod (1-65535 s):

A non-zero number seconds between the periodic re-authentication of the supplicant.

Default: 3600

max. Request (1-10):

The maximum of number times that the authenticator will retransmit an EAP Request to the supplicant before it times out the authentication session. The valid range: 1 – 10.

Default: 2 times

suppTimeout (1-65535 s):

A timeout condition in the exchange between the authenticator and the supplicant. The valid range: 1 –65535.

Default: 30 seconds.

serverTimeout (1-65535):

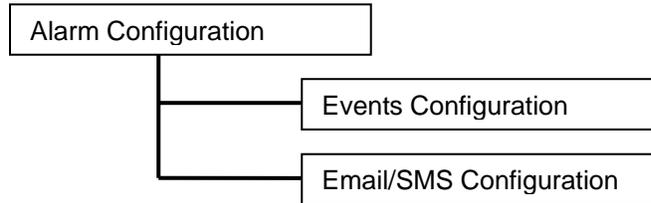
A timeout condition in the exchange between the authenticator and the authentication server. The valid range: 1 –65535.

Default: 30 seconds



Figure 5.58 – Port Parameter Setting

5.22 Alarm Configuration



Function name:

Events Configuration

Function description:

The Trap Events Configuration function is used to enable the switch to send out trap information while pre-defined trap events occur. The switch provides 24 different trap events. The trap information can be sent out in three ways, including email, mobile phone SMS (short message system) and trap. The message will be sent if you check (☑) the trap event individually on the web page shown below.

Parameter description:

Trap: Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, User login, User logout

STP: STP Topology Changed, STP Disabled, STP Enabled

LACP: LACP Disabled, LACP Enabled, LACP Member Added, LACP Port Failure

GVRP: GVRP Disabled, GVRP Enabled

VLAN: VLAN Disabled, Port-based VLAN Enabled, Tag-based VLAN, Enabled, Metro-mode VLAN Enabled, Double-tag VLAN Enabled

Module Swap: Module Inserted, Module Removed, Dual Media Swapped

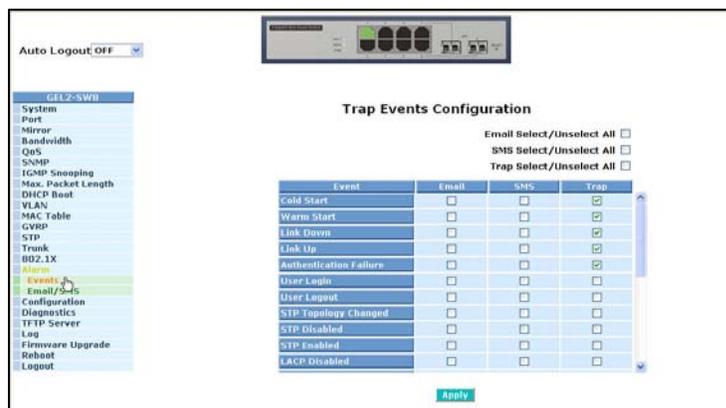


Figure 5.59 – Trap Events Configuration

Function name:

Email/SMS Configuration

Function description:

Alarm configuration is used to configure the recipients of the alarm message via email or SMS, or both. The method is dependent on the settings. An email address or a mobile phone number has to be set in the alarm configuration (See Figure 5.60). If set properly, you can read the trap information from your email or mobile phone. This function provides up to six email addresses and up to six mobile phone numbers. The 24 trap events will be sent out to SNMP Manager when trap event occurs. Once trap events have been selected, enter your desired email addresses and mobile phone numbers. Select **Apply** to complete the alarm configuration. The alarm settings will take effect in a few seconds.

Note: SMS may not work in your mobile phone system. It is customized for different systems.

Parameter description:

Email:

Mail Server: IP address of the server transferring your email.

Username: Username on the mail server.

Password: Password on the mail server.

Email Address 1 – 6: Additional email addresses that would like to receive the alarm message.

SMS:

SMS Server: IP address of the server transferring your SMS.

Username: Username in ISP.

Password: Password in ISP.

Mobile Phone 1-6: Additional mobile phone numbers that would like to receive the alarm message.

The screenshot displays the 'Alarm Configuration' page in a web browser. On the left, a navigation menu lists various system settings, with 'Email/SMS' highlighted. The main area is titled 'Alarm Configuration' and is divided into two main sections: 'Email' and 'SMS'. The 'Email' section contains input fields for 'Mail Server', 'Username', 'Password', and six 'Email Address' fields (labeled 1 through 6). The 'SMS' section contains input fields for 'SMS Server', 'Username', 'Password', and four 'Mobile Phone' fields (labeled 1 through 4). At the top of the interface, there is an 'Auto Logout OFF' dropdown menu and a small image of a network switch.

Figure 5.60 – Alarm Configuration

5.23 Configuration

The switch supports three copies of configurations, including the default configuration, working configuration and user configuration for your configuration management. The three copies are described below:

Note: If you make changes to the configuration, you must **save** the configuration before rebooting the switch.

Default Configuration:

- The factory setting and cannot be altered.

Working Configuration:

- The working configuration is the current configuration and can be changed any time. The configurations you are using are saved into this configuration file. This is updated each time you click on **Apply**.

User Configuration:

- User configuration is the specified file for backup purposes and can be updated while confirming the configuration. You can retrieve this configuration by performing Restore User Configuration.

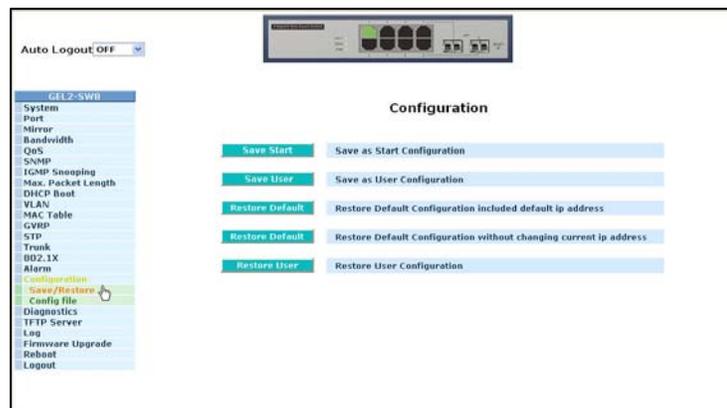


Figure 5.61 - Configuration

5.23.1 Save/Restore

Function name:

Save As Start Configuration

Function description:

Save the current configuration as a start configuration file in flash memory.



Figure 5.62 - Configuration

Function name:

Save As User Configuration

Function description:

Save the current configuration as a user configuration file in flash memory.



Figure 5.63 - Configuration

5.23.2 Restore Default

Function name:

Restore Default Configuration (includes default IP address)

Function description:

Restore Default Configuration function can retrieve the factory setting to replace the start configuration. If the factory settings are restored, the IP address of the switch will be restored to 192.168.1.1.



Figure 5.64 – Restore Configuration

Function name:

Restore Default Configuration (excludes current IP address)



Figure 5.65 - Restore Configuration

Function description:

Restore Default Configuration function can retrieve the factory setting to replace the start configuration. However, by using this restore, the switch's current IP address will not be changed and will NOT be restored to 192.168.1.1.

Function name:

Restore User Configuration

Function description:

Restore User Configuration function retrieves the previous confirmed working configuration stored in the flash memory to update start configuration. When restoring the configuration, the system's start configuration is updated and will be changed its system settings after rebooting the system.



Figure 5.66 – Restore Configuration

5.23.3 Configuration File

Function name:

Config File

Function description:

Use this function to back up or reload the configuration files of Save As Start or Save As User via TFTP.

Parameter description:

Export File Path:

Export Start:

Export Save As Start's configuration file stored in flash.

Export User-Conf:

Export Save As User's configuration file stored in flash.

Import File Path:

Import Start:

Import Save As Start's configuration file stored in flash.

Import User-Conf:

Import Save As User's configuration file stored in flash.

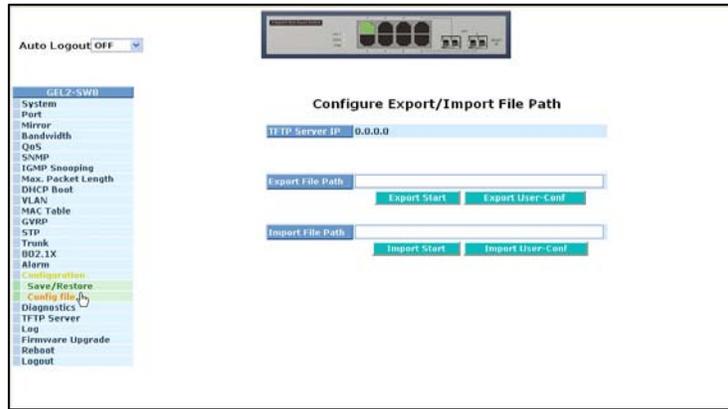
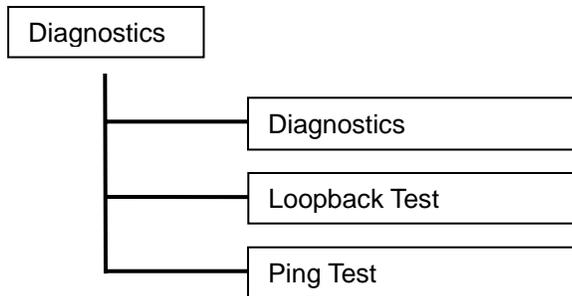


Figure 5.67 – Configuration Import/Export

5.24 Diagnostics

Three functions, including Diagnostics, Loopback Test and Ping Test are available for device self-diagnostics. Each of them will be described in detail in the following sections.



Function name:

Diagnostics

Function description:

Diagnostics provides a set of basic system diagnosis. Diagnostics provides tests to see if the system in working order. The basic system check includes EEPROM test, UART test, DRAM test and Flash test.

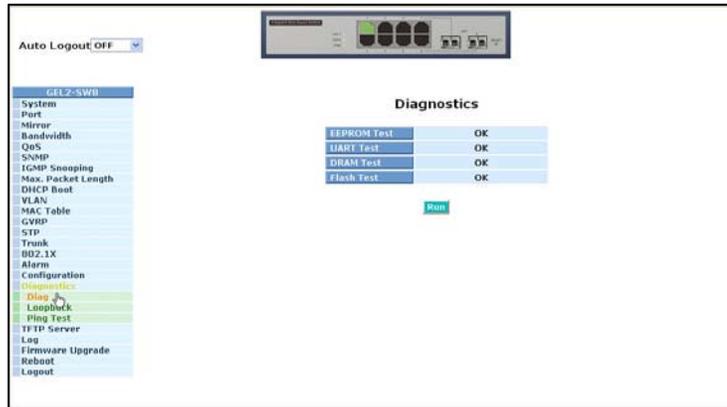


Figure 5.68 - Diagnostics

Function name:

Loopback Test

Function description:

In the Loopback Test function, there are two loopback tests -- Internal Loopback Test and External Loopback Test. The former test function will not send the test signal outside the switch box. The test signal only wraps around in the switch. The second function will send the test signal to its link partner. If the switch is not connected to active network devices, i.e. the ports are link down, the switch will report the port numbers failed. If they all are okay, OK is displayed.

Note: When you choose either of these tests, there will be interference with the normal system. Packets that are being sent and received will stop temporarily.

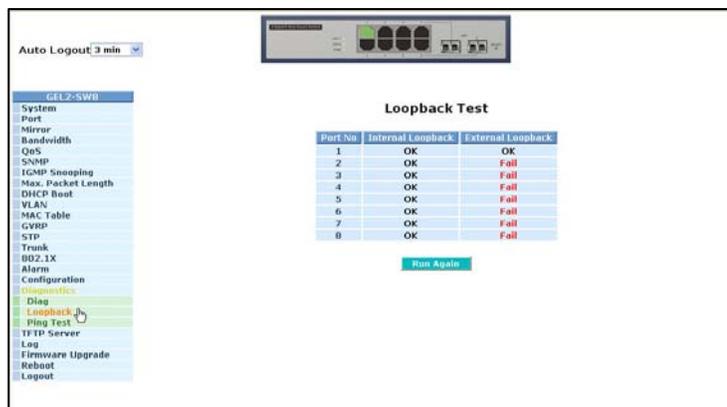


Figure 5.69 – Loopback Test

Function name:

Ping Test

Function description:

Ping Test function is a tool for detecting whether or not the target device is making a connection through the ICMP protocol which submits report messages. The switch provides Ping Test function to let you know whether the target device is available or not. You can simply fill in a known IP address and then click **Ping**. After a few seconds, the switch will report to the pinged device the result of the Ping.

Parameter description:

IP Address:

An IP address with the version of v4, e.g. 192.168.1.1.

Default Gateway:

IP address of the default gateway.

For more details, please see the section of IP address in Section 4.4.

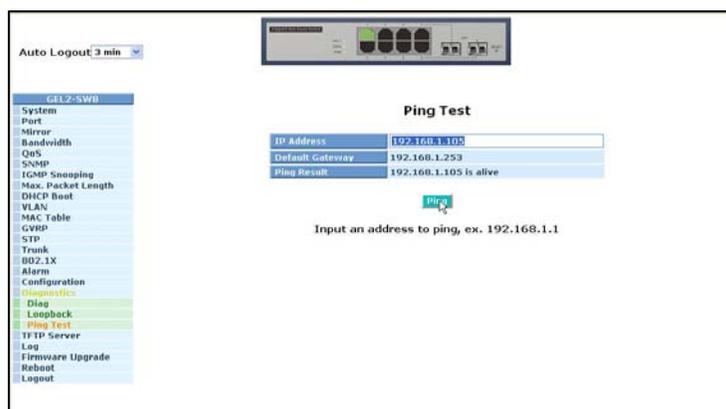


Figure 5.70 – Ping Test

5.25 TFTP Server

Function name:

Trivial File Transfer Protocol (TFTP) Server

Function description:

Set up IP address of TFTP server.

Parameter description:

Specify the IP address of the TFTP server. Once you have entered the IP of the TFTP server, click on **Apply** so the setting will take effect.



Figure 5.71 – TFTP Server

5.26 Log Data

This function displays the log data. The switch provides system log data for users. There are nineteen private trap logs and five public trap logs. The switch supports a total 120 log entries. For more details on log items, please refer to Section 5.22 for Trap/Alarm Configuration and SNMP Configuration.

Function name:

Log Data

Function description:

The Trap Log Data displays the log items including all SNMP Private Trap events, SNMP Public traps and user logs occurred in the system. In the report table, No., Time and Events are three fields contained in each trap record.

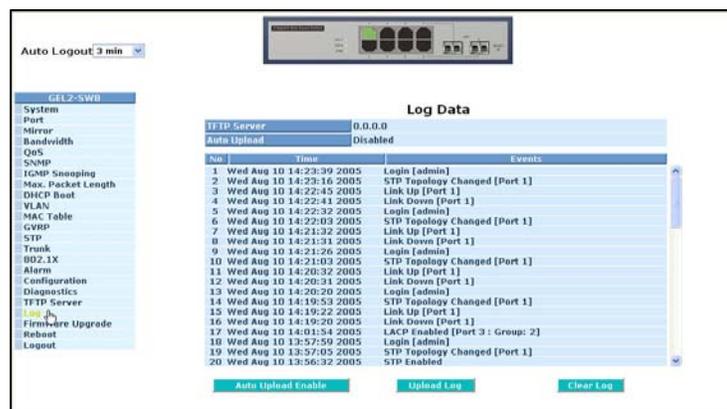


Figure 5.72 – Log Data

Parameter description:

No.:

Displays the order number of the traps.

Time:

Displays the time of the trap.

Events:

Displays the trap event name.

Auto Upload Enable:

Switch the enabled or disabled status of the auto upload function.

Upload Log:

Upload log data through tftp.

Clear Log:

Clear log data.

5.27 Firmware Upgrade

A software upgrade tool is used to upgrade the software functions and to fix or improve the functionality of the switch. The switch provides a TFTP client for software upgrade which is done through the network connection.

Function name:

Firmware Upgrade

Function description:

The switch supports software upgrade through a TFTP server. To apply a firmware upgrade, follow this procedures:

1. Specify the IP address TFTP server.
2. Specify the filename and the full path for the location of the file.
3. Select **Upgrade**.
4. When the download is complete, the switch begins upgrading the software. You will be prompted to reboot the switch after completing the upgrade. The switch must be rebooted so the new software will be applied.

Note: If the download is not successful, the switch will return to "Software Upgrade." Software upgrade is hazardous if power is off.

Parameter description:

TFTP Server: A TFTP server stores the image file you want to upgrade.

Path and Filename: File path and filename stored the image file you want to upgrade.



Figure 5.73 – Firmware Upgrade

5.28 Reboot

There are a few ways to reboot the switch, including power up, hardware reset and software reset. You can press the RESET button in the front panel to reset the switch. After upgrading software, changing IP configuration or modifying VLAN configurations, you must reboot in order for the new configuration to take effect.

Function name:

Reboot

Function description:

Reboot the switch. Reboot takes the same effect as the RESET button on the front panel of the switch. It will take around thirty (30) seconds to complete the system boot.

Parameter description:

Save and Reboot:

Save the current settings as start configuration before rebooting the switch.

Reboot:

Reboot the system directly.

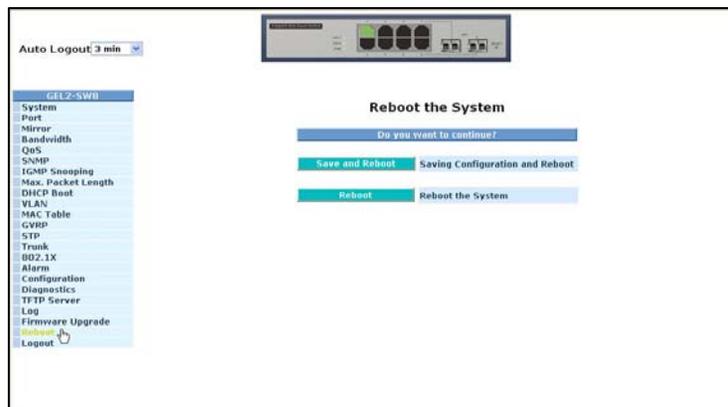


Figure 5.74 - Reboot

5.29 Logout

You can manually logout by using Logout function. You can also configure the switch to logout automatically.

Function name:

Logout

Function description:

The switch provides and automatic logout to prevent unauthorized users from using the system. If you do not logout and exit the browser, the switch will automatically logout. You can use **Auto Logout**.

Parameter description:

Auto Logout:

Default is ON (three minutes). If no action is taken within three minutes, the switch will logout automatically.



Figure 5.75 - Logout

6.0 Operation of CLI Management

Section 4 of this manual provides detailed information for console connection to the switch. This section provides detailed syntax and examples for CLI management.

6.1 Login

The command-line interface (CLI) is a text-based interface. You can access the CLI through either a direct serial connection to the device or a Telnet session. The default login identification is:

```
Username: admin
Password: admin
```

After you login successfully, the prompt will be shown as “#” if you are the first login person and your authorization is administrator; otherwise it may show “\$”. The “#” symbol allows you to perform administrator functions and have full access to the system. The “\$” symbol allows you to perform guest functions. Guest functions only permit the system to be viewed. You will not be able to modify settings on the switch with the guest login.

```
L2 Managed Switch - GEL2-SW8
Login: admin
Password:
GEL2-SW8#
```

Figure 6-1 – Login screen

6.2 Commands of CLI

To see the commands of the mode, please input “?” after the prompt, then all commands will be listed in the screen. All commands can be divided into two categories, including global commands and local commands. The following **global commands** can be used in any mode:

- Exit
- End
- Help
- History
- Logout
- Save start
- Save user
- Restore default
- Restore user

Command instructions residing in the corresponding modes are **local commands**. The same commands can be used in different modes and will perform a different function resulting in totally different information. For example, **show** in IP mode displays the IP information; however, in system mode, it will display the system information.

```
L2 Managed Switch - GEL2-SW8
Login: admin
Password:
GEL2-SW8# ?
 802.1x          Enter into 802.1x mode
 account        Enter into account mode
 alarm          Enter into alarm mode
 autologout     Change autologout time
 bandwidth      Enter into bandwidth mode
 config-file    Enter into config file mode
 dhcp-boot     Enter into dhcp-boot mode
 diag          Enter into diag mode
 firmware      Enter into firmware mode
 gvrp          Enter into gvrp mode
 hostname      Change hostname
 igmp          Enter into igmp mode
 ip            Enter into ip mode
 log           Enter into log mode
 mac-table     Enter into mac table mode
 management    Enter into management mode
 max-pkt-len   Enter into max packet length mode
 mirror        Enter into mirror mode
```

Figure 6-2

The following table lists the CLI commands and descriptions.

Command	Syntax	Description	Argument	Possible Value
Global Commands				
End	end	Return to top mode	None	None
Exit	exit	Returns to previous mode	None	None
Help	help	Displays available commands.	None	None

Command	Syntax	Description	Argument	Possible Value
		When you use <i>help</i> , all commands are displayed. This command will help you distinguish between local and global commands.		
History	history	Displays the list of commands you have been using during the session. CLI supports up to 256 records. If no argument is entered, CLI will list total records up to 256. If an argument is provided, CLI would display the number of records equal to the argument.	Optional (Show last number of history records)	1, 2, 3....256
Logout	logout	If you use this command via Telnet connection, you will logout and disconnect. If you used this command through direct console connection, you will be logged out of the system and return to the login prompt.	None	None
Restore Default	restore default	Use this command to restore the startup configuration provided by factory default. If the restore is successful, you will be prompted to reboot. Once rebooted, startup configuration will be reset to factory default.	None	None
Restore user	restore user	Restores startup configuration as defined by user configuration. If restoring is successful, you will be prompted to reboot. After restoring the user defined configuration, all changes in the startup configuration would be lost. After rebooting, the entire startup configuration will replace the user defined configuration.	None	None
Save Start	save start	Use this command to save the current configuration as the startup configuration. This command must be used in order to use the current configuration if the switch is rebooted.	None	None
Save User	save user	Use this command to save the current configuration as the user-defined configuration. This command saves your	None	None

Command	Syntax	Description	Argument	Possible Value
		current configuration into the non-volatile FLASH as the user-defined configuration.		
Local Commands				
802.1x				
Set max-request	set max-request <port-range> <times>	This command sets the number of times the state machine will retransmit an EAP request packet to the Supplicant before it times out the authentication session.	<port range>: syntax 1, 5-7, available from 1 to 8 <times>: max-times, range 1-10	<port range> 1 to 8 <times>: 1-10, default is 2
Set mode	set mode <port-range> <mode>	This command is used to set up the 802.1x authentication mode of each port	<port range>: syntax, 1, 5-7, available from 1 to 8 <mode>: set up 802.1x mode 0:disable the 802.1x function 1:set 802.1x to multihost mode	<port range>: 1 to 8 <mode>: 0 or 1
Set port-control	set port-control <port-range>	Use this command to set up the 802.1x status of each port	<port range>: syntax 1, 5-7, available from 1 to 8 <authorized>: set up the status of each port 0:ForceUnauthorized 1:ForceAuthorized 2:Auto	<port range>: 1 to 8 <authorized>: 0, 1 or 2
Set quiet period	set quiet-period <port-range> >sec>	This command is used to define periods of time when the authenticator state machine will not attempt to acquire a supplicant.	<port range>: syntax 1, 5-7, available from 1 to 8 <sec>: timer, range 0-65535	<port range>: 1 to 8 <sec>: 0~65535, default is 60
Set reAuthEnabled	set reauthenabed >port range> <ebl>	Use to define whether regular reauthentication will take place on a particular port	<port range>: syntax 1, 5-7, available 1 to 8 <ebl> : 0 :OFF Disable reauthentication 1 :ON Enable reauthentication	<port range>: 1 to 8 <ebl>: 0 or 1, default is 1
Set reAuthMax	set reauthmax	Use to set the number of reauthentication attempts that are permitted before the port becomes unauthorized.	<port range>: syntax 1, 5-7, available 1 to 8 <max> : max. value, range 1-10	<port range> : 1 to 8 <max> : 1-10, default is 2
Set ReAuthPeriod	Set reauthperiod <port-range> <sec>	This command sets a constant that defines a non zero number of seconds between periodic reauthentication of the supplicant.	<port range>: syntax 1, 5-7, available 1 to 8 <sec> : timer, range 1-65535	<port range>: 1 to 8 <sec> : 1~65535, default is 3600

Command	Syntax	Description	Argument	Possible Value
Set serverTimeout	set servertimeout <port-range> <sec>	This command sets a timer used by the Backend Authentication state machine to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this time is either suppTimeout or serverTimeout.	<port-range>: syntax 1, 5-7, available 1 to 8 <sec> :timer, range 1~65535	<port-range> : 1 to 8 <sec> :1~65535, default is 30
Set state	set state <ip> <port number> <secret-key>	Used to configure the settings related to the 802.1x radius server.	<ip>: the IP address of the radius server. <port-number> the service port of radius server (authorization port) <secret-key>: set up the value of secret-key and the length of secret-key is from 1 to 31	<port-number> :1~65535, default is 1812
Set suppTimeout	set supptimeout <port range> <sec>	A timer is provided by the Backend Authentication state machine to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value is either suppTimeout or serverTimeout as determined by the operation of the Backend Authentication state machine.	<port-range>: syntax 1, 5-7, available 1 to 8 <sec> :timer, range 1-65535	<port-range>: 1 to 8 <sec> :1~65535, default is 30
Set txPeriod	set txperiod <port-range> <sec>	A time used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted.	<port-range>: syntax 1, 5-7, available 1 to 8 <sec> :timer, range 1-65535	<port-range>: 1 to 8 <sec> :1~65535, default is 30
Show mode	show mode	Displays the mode of each port	None	None
Show parameter	show parameter	Displays the parameters of each port	None	None
Show security	show security	Displays the authentication status of each port	None	None
Show state	Show state	Displays the Radius server configuration	None	None
Account Commands				
Add	add	Used to create a new guest user. When a new guest user is created, the new password must be entered and confirmed.	<name> : new account name	At least 5 characters

Command	Syntax	Description	Argument	Possible Value
Del	del <name>	Used to delete an existing account	<name>: existing user account	None
Modify	modify <name>	Used to modify the username and password of an existing account	<name>: existing user account	None
Show	show	Used to display the system account, including account name and identity	None	None
Alarm <<email>>				
Del mail-address	del mail-address <#>	Used to remove the configuration of an email address	<#>: email address number, range 1 to 6	<#> 1 to 6
Del server-user	del server-user	Used to remove the configuration of the server user account and password	None	None
Set mail-address	set mail-address <#> <mail address>	Used to set up an email address	<#>:email address number, range 1 to 6	<#> 1 to 6
Set server	set server <ip>	Used to set up the IP address of the email server	<ip>:email server ip address or domain name	None
Set user	set user <username>	Used to set up the account for the email server	<username>: email server account and password	None
Show	Show	Used to display email configuration	None	None
<<email>>				
Del all	del all <range>	Used to disable email, sms and trap of events	<range>: del the range of events, syntax 1, 5-7	<range> 1~24
Del email	del email <range>	Used to disable email of events	<range>: del the range of email, syntax 1, 5-7	<range> 1~24
Del sms	del sms <range>	Used to disable sms of events	<range>: del the range of sms, syntax 1, 5-7	<range> 1~24
Del trap	del trap <range>	Used to disable trap of events	<range>: del the range of trap, syntax 1, 5-7	<range> 1~24
Set all	set all <range>	Used to enable email, sms and trap of events	<range>: set the range of events, syntax 1, 5-7	<range> 1~24
Set email	set email <range>	Used to enable email of the events	<range>: set the range of email, syntax 1, 5-7	<range> 1~24
Set sms	set sms <range>	Used to enable the SMS of the events	<range>: set the range of sms, syntax 1, 5-7	<range> 1~24
Set trap	set trap <range>	Used to enable the trap of events	<range>: set the range of sms, syntax 1, 5-7	<range> 1~24

Command	Syntax	Description	Argument	Possible Value
Show	show	Used to display the configuration of an alarm event	None	None
Show (alarm)	show	Alarm is used to display the configuration of Trap, SMS or email	None	None
<<sms>>				
Del phone-number	del phone-number <#>	Used to delete SMS phone number	<#> : mobile phone number, range 1 to 6	<#>: 1 to 6
Del server-user	del server-user	Used to delete SMS server, user account and password	None	None
Set phone-number	set phone-number <#> <phone-number>	Used to add SMS phone number	<#>: mobile phone number, range 1 to 6 <phone-number>; phone number	<#>: 1 to 6
Set server	set server <ip>	Used to set up the IP address of SMS sever	<ip>; SMS server ip address or domain name	None
Set user	set user <username>	Used to set up user account and password of SMS server	<username>: SMS server account	None
Show	show	Used to display the configuration os SMS trap event	None	None
Autologout				
Autologout	autologout <time>	Used to set time for autologout	<time>: range 1 to 3600 seconds, 0 for autologout OFF; default setting is 180 seconds	<time>: 1, 1-3600
Bandwidth				
Disable egress-rate	disable egress-rate <range>	Used to cancel the egress-rate of the port.	<range> : syntax 1, 5-7, available from 1 to 8	<range>; 1 to 8
Disable ingress-rate	disable ingress-rate <range>	Used to cancel the ingress-rate of the port.	<range> : syntax 1, 5-7, available from 1 to 8	<range>; 1 to 8
Disable storm-rate	disable store-rate <range>	Used to cancel the storm-rate of the port	<range> : syntax 1, 5-7, available from 1 to 8	<range>; 1 to 8
Enable egress-rate	enable egress-rate <range> <data_rate>	Used to set the egress-rate of the port.	<range> : syntax 1, 5-7, available from 1 to 8 <data rate>: 0-1000	<range>; 1 to 8 <data rate>: 0-1000
Enable ingress-rate	enable ingress-rate <range> <data_rate>	Used to set up the Ingress-rate of the port	<range> : syntax 1, 5-7, available from 1 to 8 <data rate>: 0-1000	<range>; 1 to 8 <data rate>: 0-1000
Enable storm-rate	enable storm-rate <range> <data_rate>	Used to set the storm-rate of the port	<range> : syntax 1, 5-7, available from 1 to 8 <data rate>: 0-1000	<range>; 1 to 8 <data rate>: 0-1000
Show	Show	Used to display all current	None	None

Command	Syntax	Description	Argument	Possible Value
		settings for bandwidth		
Config-file				
Export start	export start	Used to run the export start function	None	None
Export user-conf	export-user-conf	Used to export user-conf function	None	None
Import start	import start	Used to run the import start function	None	None
Import user-conf	import user-conf	Used to run the import user-conf function	None	None
Set export-path	set export-path <filepath>	Used to set the filepath and filename that will be exported	<filepath>:filepath and filename	<filepath>:filepath and filename
Set import-path	set import-path <filepath>	Used to set the filepath and filename that will be imported	<filepath>:filepath and filename	<filepath>:filepath and filename
Show	show	Used to display the config-file information	None	None
DHCP-boot				
Set dhcp-boot	set dhcp-boot <sec>	Used to set the delay time for DHCP boot	<sec>:range syntax: 0, 1-30; the value "o" is used to disable DHCP boot delay	<sec>: 0-30
Show	show	Used to display the status of DHCP boot	None	None
Diag				
Diag	diag	Used to determine whether UART, DRAM, Flash and EEPROM is normal or not normal.	None	None
Loopback	loopback	Used for internal/external loopback test	None	None
Ping	ping <ip>	Used to confirm the remote end-station or switch itself is making a connection	<ip>:ip address or domain name	IP address, e.g. 192.168.2.65 or domain name, e.g. yahoo.com
Firmware				
Set upgrade-path	set upgrade-path <filepath>	Used to download the image for firmware upgrade	<filepath>:upgrade file path	<filepath>: upgrade file path
Show	show	Used to display information for ftp server	None	None
Upgrade	upgrade	Used to run the upgrade function	None	None
GVRP				
Disable	disable	Used to disable the GVRP function	None	None
Enable	enable	Used to enable the GVRP function	None	None
Group	group <group number>	Used to modify a GVRP group's setting. The applicant or	<group number>: enter the GVRP	<group number>:

Command	Syntax	Description	Argument	Possible Value
		registrar mode of an existing GVRP group per port can be changed.	group you have created using the VID. Available range 1 to 4094	1~4094
Set applicant	set applicant <range> <normal non-participant>	Used to set default applicant mode for each port	<range>:port range, syntax 1, 5-7, available from 1 to 8 <normal>: set applicant as normal mode <non-participant>: set applicant as non-participant mode	<range> : 1 to 8
Set registrar	set registrar <range> <normal fixed forbidden>	Used to set default registrar mode for each port	<range>:port range, syntax 1, 5-7, available from 1 to 8 <normal>: set registrar as normal mode <fixed>: set registrar as fixed mode <forbidden>: set registrar as forbidden mode	<range>: 1 to 8 <normal fixed forbidden>:normal or fixed or forbidden
Set restricted	set restricted <range> <enable disable>	Used to set the restricted mode for each port	<range>: port range, syntax 1, 5-7, available from 1 to 8 <enable>: set restricted enabled <disabled>: set restricted disabled	<range>: 1 to 8 <enable disable>: enable or disable
Set timer	set timer <range> <join> <leaveall>	Used to set GVRP join time, leave time and leaveall time for each port.	<range>:port range, syntax 1, 5-7, available from 1 to 8 <join>: join timer, available from 20 to 100 <leave>: leave timer, available from 60 to 300 <leaveall>: 1000 to 5000 Leave time must be equal to or greater to the join time	<range> 1 to 8 <join>: 20 to 100 <leave>: 60 to 300 <leaveall>: 1000 to 5000
Show config	show config	To display the GVRP configuration	None	None
Show counter	show counter	Used to display the counter number of the port	<port>: port number	<port>: available from 1 to 8
Show group	show group	Used to display the GVRP groups	None	None

Command	Syntax	Description	Argument	Possible Value
Hostname				
Hostname	hostname <name>	Used to set the hostname of the switch	<name>:hostname, max 40 characters	<name>:hostna me, max 40 characters
IGMP				
Set igmp_snooping	set igmp_snooping <status>	Use to set the most for IGMP snooping	<status>:0:disable 1:active 2:passive	<status>: 0, 1 or 2
Show	show	Used to display IGMP snooping mode and IP multicast table	None	None
IP				
Disable DHCP	disable dhcp	Used to disable the DHCP function	None	None
Enable DHCP	enable dhcp	Used to enable the DHCP function and set DNS server for manual or auto mode	<manual auto>:set DHCP with either manual or auto mode	<manual auto>: manual or auto
Set DNS	set dns	Used to set the IP address of the DNS server	<ip>:dns ip address	168.95.1.1
Set IP	set <ip> <mask> <gateway>	Used to set the system IP address, subnet mask and gateway	<ip>:ip address <mask>:subnet mask <gateway>:default gateway	<ip>:192.168.1. 2 or others <mask>:255.25 5.255.0 or others <gateway>:192 .168.1.253 or others
Show	show	Used to display the system's DHCP state, IP address, subnet mask, default gateway, DNS mode, DNS server IP address and current IP address	None	None
Log				
Clear	clear	Used to clear the log data	None	None
Disable auto-upload	disable auto-upload	Used to disable the auto-upload function	None	None
Enable auto-upload	enable auto-upload	Used to enable the auto-upload function	None	None
Show	show	Used to display a list of the trap log events. When a log event occurs, it is recorded. Show is used to query the log functions. Up to 120 records are supported.	None	None
Upload	upload	Used to upload log data through tftp.	None	None
Mac-Table <<alias>>				
Del	del <mac>	Used to delete the MAC alias entry	<mac>; mac address, format: 00-02-03-04- 05-06	<mac>:mac address
Set	set <mac> <alias>	Used to set the MAC alias entry.	<mac>; mac address, format: 00-02-03-04-	None

Command	Syntax	Description	Argument	Possible Value
			05-06 <alias> mac alias name, max 15 characters	
Show	show	Used to display the MAC alias entry	None	None
<<information>>				
Search	search <port> <mac> <vid>	Used to find the relative MAC information in the MAC table	<port>: set up the range of the ports to search for Syntax 1, 5-7, available from 1 to 8 <mac>: mac address, format: 01-02-03-04-05-06 '?' can be used <vid>: vlan id from 1 to 4094; '?' as don't care, 0 as untagged	<port>; 1 to 8 <vid>:0, 1~4094
show	show	Used to display all MAC table information	None	None
<<maintain>>				
Set aging	set aging	Used to set up the age out time of dynamic learning MAC	<#>; age-timer in seconds 0, 10 to 65535. The value "0" means to disable aging	<#>; 0, 10 to 65535
Set flush	set flush	Used to delete all MACs learned dynamically	None	None
Show	show	Used to display the age timer settings	None	None
<<static mac>>				
Add	add <mac> <port> <vid> [alias]	Used to add the static MAC entry	<mac>: mac address, format: 00-02-03-04-05-06 <port>: 0-8. The value "0" means this entry is a filtering entry <vid>: vlan id 0, 1-4094. VID must be zero if vlan mode is not tag-based [alias]: mac alias name, max 15 characters	<mac>: mac address <port>:0-8 <vid>:0, 1-4094 [alias]: mac alias name
Del	del <mac> <vid>	Used to remove the static MAC entry	<mac>: mac address, format 00-02-03-04-05-06 <vid>:vlan id. 0, 1-4094. VID must be zero if VLAN mode is	<mac>: mac address <vid>: 0, 1-4094

Command	Syntax	Description	Argument	Possible Value
			not tag-based	
Show filter	show filter	Used to display the static filter table	None	None
Show forward	show forward	Used to display the static forward table	None	None
Management				
Add	set [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>] [<type> <value>] [<action> <value>]	Used to set management policy records	[<name> <value>] ACL entry name [<vid> <value>] VLAN ID [<ip> <value>] Incoming port [<type> <value>] Access type [<action> <value>] a(ccept) or d (eny)	[<name> <value>] No default, must be set [<vid> <value>] Range is 1-4095 and can be set to any [<ip> <value>] Any valid IP address [<port> <value>] 1 or 1-9 [<type> <value>] h(ttp), s(nmp) or t(elnet) or any [<action> <value>] No default and must be set
Delete	delete #	Used to delete a specific record or range	<#>: a specific or range management security entry	None
Edit [#] the specific management policy entry	edit # [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>] [<type> <value>] [<action> <value>]	Used to edit a management policy record	[<name> <value>] ACL entry name [<vid> <value>] VLAN ID [<ip> <value>] Incoming port [<type> <value>] Access type [<action> <value>] a(ccept) or d (eny)	[<name> <value>] No default, must be set [<vid> <value>] Range is 1-4095 and can be set to any [<ip> <value>] Any valid IP address [<port> <value>] 1 or 1-9 [<type> <value>] h(ttp), s(nmp) or t(elnet) or any [<action> <value>] No default and

Command	Syntax	Description	Argument	Possible Value
				must be set
Show	show	Used to show the specific management policy record	None	None
Max-pkt-len				
Set len	set len <range> <lenth>	Used to set the maximum length of the packet that each port of the switch can accept	<range>: port range, syntax 1, 5-7, available from 1 to 8 <length (bytes)>: maximum packet length	<range>: 1 to 8 <length (bytes)>: 1518/1343/9216
Show	show	Used to display current setting for maximum packet length	None	None
Mirror				
Set mirror-mode	set mirror-mode <rx disable>	Used to set the mirror mode (rx mode or disable)	<rx disable>: rx:enable the mode of mirror (only mirror packets that are received) Disable: end of the function of mirroring	<rx diable>: rx or disable
Set monitored port	set monitored-port <range>	Used to set the port that will be monitored. The packets received by this port will be copied to the monitoring port.	<range>: the port that is chosen for monitored port for the mirror function, syntax 1, 5-7, available from 1 to 8	<range>: 1 to 8
Set monitoring-port	set monitoring-port	Used to set the monitoring port for the mirror function. User can observe the packets of the monitored port received by this port.	<#>: the monitoring port that is chosen for the mirror function. Only one port is allowed to configure, available from 1 to 8	<#>: 1 to 8
Show	show	Used to display the setting status of the Mirror function	None	None
Port				
Clear counter	clear counter	Used to clear all ports' counter information (including simple and detailed port counter)	None	None
Disable flow-control	disable flow-control <range>	Used to disable the flow control function of the port	<range>: syntax 1, 5-7, available from 1 to 8	<range>: 1~8
Disable state	disable state <range>	Used to disable the communication capability of the port	<range>: syntax 1, 5-7, available from 1 to 8	<range> :1~8
Enable flow-control	enable flow-control <range>	Used to enable the flow control function of the port	<range>:syntax 1, 5-7, available from 1 to 8	<range>: 1~8
Enable state	enable state <range>	Used to enable the communication capability of the port	<range>:syntax 1, 5-7, available from 1 to 8	<range>: 1~8
Set speed-	set speed-	Used to set the speed and	<range>:syntax 1, 5-	<range>: 1 to 8

Command	Syntax	Description	Argument	Possible Value
duplex	duplex <range> <auto 10half 10full 100half 100full 1gfull>	duplex mode of all ports	7, available from 1 to 8 <port-speed>: auto: set auto-negotiation mode 10half: set speed/duplex 10M Half 10full: set speed/duplex 10M Full 100half:set speed/duplex 100M half 100full: set speed/duplex 100M full 1Gfull: set speed/duplex 1G full	<port-speed>: auto, 10half, 10full, 100half, 100full, 1Gfull
Show conf	show conf	Used to display each port's configuration regarding state, speed-duplex and flow control	None	None
Show detail-counter	show detail-counter <#>	Used to display the detailed counter number for port traffic	<#>: port, available from 1 to 8	<#>: 1-8
Show sfp	show sfp <port>	Used to display the SFP module information	<port>: SFP port, available 7-8	<port>: 7, 8
Show simple-counter	show simple-counter	Used to display the summary counter for each port's traffic	None	None
Show status	show status	Used to display the port's current status	None	None
QoS				
Set advance-layer4	set advance-layer4 <port-range> <#> <tcp/udp port> <default> <match>	Used to set class of ports on advanced mode for Layer 4 QoS	<port-range>:port range, syntax 1, 5-7, available from 1 to 8 <#>: special UDP/TCP port selection, range: 1-10 <tcp/udp port range>: 0-65535 <default>: default class (all other TCP/UDP ports) 1:high, 0:low <match>:special TCP/UDP class. 1:high, 0:low	<port -range>: 1 to 8 <#>: 1-10 <tcp/udp port range>:0-65535 <default>: 1 or 0 <match>: 1 or 0
Set default	set default <class>	Used to set priority class of the packets that QoS doesn't affect	<class>: class of service setting 1:high, 0:low	<class>: 1 or 0
Set diffserv	set diffserve <ds-range>	Used to set class of ports on IP DiffServe QoS	<ds-range>: dscp field, syntax 1, 5-7,	<ds-range>: 0 to 63

Command	Syntax	Description	Argument	Possible Value
	<class>		available from 0 to 63 <class>: class of service setting. 1:high, 0:low	<class>: 1 or 0
Set mode	set mode <port/pri_tax/tos/layer4/diffserv>	Used to set QoS priority mode of the switch	<port>: per port priority <pri_tag>:vlan tag priority <tos>: ip tos classification <diffserv>:ip diffserv classification	Port/pri_tag/tos / layer4/diffserv
Set port <range> <class>	set port <range> <class>	Used to set class of ports on port-based QoS	<range>: port range, syntax 1, 5-7, available from 1 to 8 <class>: class of service setting. 1: high, 0:low	<range>: 1 to 8 <class> 1 or 0
Set pri-tag	set pri_tax <port-range><tag-range> <class>	Used to set class of ports on VLAN tag-based QoS	<range>: port range, syntax 1, 5-7, available from 1 to 8 <tag-range>: tag priority level, syntax: 1, 5-7, available 0 to 7 <class>: class of service setting. 1: high, 0:low	<port-range>: 1 to 8 <tag-range>: 0 to 7 <class> 1 or 0
Set simple layer4	set simple-layer4 <#>	Used to set class of ports on simple mode of Layer 4 QoS	<#>: layer4-configuration mode, valid values are as follows: 0:disable ip tcp/udp port classification 1 :down prioritize web browsing, e-mail, FTP and news 2:prioritize IP telephony (VoIP) 3: prioritize iSCSI 4: prioritize web browsing, email, FTP transfers and news 5: prioritize streaming audio/video 6: prioritize databases (Oracle, IBM DB2, SQL, Microsoft)	<#>: 0~6
Set tos	set tos <port-range> <tos-range> <class>	Used to set class of ports on IP TOS QoS	<port-range>:, syntax: 1, 5-7, available from 1 to 8	<port-range> 1 to 8 <tos-range>: 0

Command	Syntax	Description	Argument	Possible Value
			<tos-range>: tos precedence field, syntax 1, 5-7, available from 0 to 7 <class>: class of service setting. 1:high, 0:low	to 7 <class> : 1 or 0
Show	show	Used to display the information of the mode you have chosen	None	None
Reboot				
Reboot	reboot	Used to reboot the switch	None	None
SNMP				
Disable	disable set-ability disable snmp	Disable used in this mode will deactivate SNMP or set-community	None	None
Enable	enable set-ability enable snmp	Enable used in this mode will activate SNMP or set-community	None	None
Set	set get-community <community> set set-community <community> set trap <#> <ip> [port] [community]	Set used in this mode is used to set up get-community, set-community, trap host IP, host port and trap-community.	<#>: trap number <ip>: IP address or domain name <port>: trap port <community>:trap community name	<#>: 1 to 6 <port>:1~65535
show	show	Used to display the configuration of SNMP	None	None
STP				
Mcheck	mcheck <range>	Used to force the port to transmit RST BPDUs	<range>: syntax 1, 5-7, available form 1 to 8	<range>: 1 to 8
Disable	disable	Used to disable the STP function	None	None
Enable	enable	Used to enable the STP function	None	None
Set config	set config <bridge priority> <hello time> <max.age> <forward delay>	Used to set the parameters of STP	<bridge priority>: priority must be a multiple of 4096, available from 0 to 61440 <hello time>: available from 1 to 10 <max.age> : available from 6 to 40 <forward delay>: available from 4 to 30. Note: 2*(Forward delay -1)>=MaxAge Max Age> =2*(Hello	bridge priority>: 0 to 61440 <hello time>: 1 to 10 <max.age> : 6 to 40 <forward delay>: 4 to 30

Command	Syntax	Description	Argument	Possible Value
			Time +1)	
Set port	set port <range> <path cost> <priority> <edge_port> <admin p2p>	Used to set up the port information of STP	<range>: syntax 1, 5-7, available from 1 to 8 <path cost>: 0, 1-200000000. The value zero means auto status <priority>: priority must be a multiple of 16, available from 0 to 240 <edge_port>: Admin Edge Port, <yes/no> <admin p2p>: Admin point to point, <auto/true/false>	<range>: 1 to 8 <path cost>: 0, 1-200000000 <priority>: 0 to 240 <edge_port>: Admin Edge Port, <yes/no> <admin p2p>: <auto/true/false>
Set version	set version <stp rstp>	Used to set up the version of STP	<stp rstp>: stp/rstp	<stp rstp>: stp/tstp
Show config	show config	Used to display the configuration of STP	None	None
Show port	show port	Used to display the port information of STP	None	None
Show status	show status	Used to display the status of STP	None	None
System				
Set contact	set contact <contact string>	Used to set the contact description of the switch	<contact>: string length up to 40 characters	<contact>: a, b, c, d, ...z and 1, 2, 3, ... etc.
Set device-name	set device-name <device-name string>	Used to set the description of the device name of the switch	<device-name>: string length up to 40 characters	<device-name>: a, b, c, d, ...z and 1, 2, 3, ... etc.
Set location	set location <location string>	Used to set the description of the location of the switch	<location>: string length up to 40 characters	<location>: a, b, c, d, ...z and 1, 2, 3, ... etc.
Show	show	Used to display the basic information of the switch	None	None
TFFP				
Set server	set server <IP>	Used to set the IP address of the TFFP server	<IP>: the IP address of the TFFP server	<IP>: TFFP server IP
Show	show	Used to display information of the TFFP server	None	None
Time				
Set daylightsaving	Set daylightsaving <hr> <MM/DD/HH> <mm/dd/hh>	Used to set daylight savings time	hr:daylight saving hour, range -5 to +5 MM: daylight saving start month (01-12) DD: daylight saving start Day (01-31) HH: daylight saving	hr:daylight: -5 to +5 MM: (01-12) DD: (01-31) HH: (01-23) mm: (01-12) dd: (01-31)

Command	Syntax	Description	Argument	Possible Value
			start hour (01-23) mm: daylight saving end month (01-12) dd: daylight saving end day (01-31) hh: daylight saving end hour (00-23)	hh: (00-23)
Set manual	set manual <YYYY/MM/DD > <hh:mm:ss>	Used to set the current time manually	YYYY: Year (2000-2036) MM: Month (01-12) DD: Day (01-31) hh: Hour (00-23) mm: minute (00-59) ss: second (00-59)	YYYY: (2000-2036) MM: (01-12) DD: (01-31) hh: (00-23) mm: (00-59) ss: (00-59)
Set ntp	set ntp <ip> <timezone>	Used to set the current time via the NTP server	<IP>: ntp server IP address or domain name <timezone>: time zone (GMT), range: -12 to +13	<timezone>: -12, -11..., 0, 1..., 13
Show	show	Used to show the time configuration, including <i>current time, NTP server, timezone, daylight saving, daylight saving start and daylight saving end!</i>	None	None
Trunk				
Del trunk	del trunk <port-range>	Used to delete the trunking port	<port-range>: port range, syntax 1, 5-7, available from 1 to 8	<port-range>: 1 to 8
Set priority	set priority <range>	Used to set up the LACP system priority	<range>: available from 1 to 65535	<range>: 1 to 65535, default: 32768
Set trunk	set trunk <port-range> <method> <group> <active LACP>	Used to set up the status of trunk, including the group number and mode of the trunk as well as LACP mode	<port-range>: port range, syntax 1, 5-7, available from 1 to 8 <method>: static: adopt the static link aggregation; lacp: adopt the dynamic link aggregation-link aggregation control protocol <group>: 1-8 <active LACP>: active: set the LACP to active mode; passive: set the LACP to passive mode	<port-range>: 1 to 8 <method>: static / lacp <group>: 1 to 8 <active LACP>: active / passive
Show aggtr-view	show aggtr-view	Used to display the aggregator list	None	None
Show lacp-	show lacp-	Used to display the detailed	<aggtr>: aggregator,	<aggtr>: 1 to 8

Command	Syntax	Description	Argument	Possible Value
detail	detail <aggr>	information of the LACP trunk group	available from 1 to 8	
Show lacp-priority	show lacp-priority	Used to display the value of LACP priority	None	None
Show status	show status	Used to display the aggregator status and the settings of each port	None	None
VLAN				
Del port-group	del port-group <name>	Used to delete the port-based VLAN group	<name>: VLAN group to be deleted	<name>: port-VLAN name
Del tag-group	del tag-group	Used to delete the tag-based VLAN group	<vid>: VLAN group to be deleted	<vid>: 1 to 4094
Disable drop-untag	disable drop-untag <range>	Used to set untagged frames to not be dropped	<range>: ports to be set, syntax 1, 5-7, available 1 to 8	<range>: 1 to 8
Disable sym-vlan	disable sym-vlan	Used to drop frames from the non-member port	<range>: ports to be set, syntax 1, 5-7, available 1 to 8	<range>: 1 to 8
Enable drop-untag	enable drop-untag <range>	Used to drop the untagged frames	<range>: ports to be set, syntax 1, 5-7, available 1 to 8	<range>: 1 to 8
Enable sym-vlan	enable sym-vlan <range>	Used to drop frames from the non-member port	<range>: ports to be set, syntax 1, 5-7, available 1 to 8	<range>: 1 to 8
Set mode	set mode <disable port tag metro double-tag> [up-link]	Used to switch LVAN mode, including disable, port-based, tag-based, metro and double-tag modes	<disable>: vlan disable <tag>: set tag-based vlan <port>: set port-based vlan <metro>: set metro mode vlan <double-tag>: enable Q-in-Q function <up-link>: syntax 1, 5-7, available from 7 to 8, only for metro mode vlan	<disable port tag metro double-tag>: disable, port, tag, metro, double-tag [up-link] 7 or 8 or 7. 8
Set port-group	set port-group <name> <range>	Used to add or edit a port-based VLAN group	<name>: port-vlan name <range>: syntax 1, 5-7, available from 1 to 8	<range>: 1 to 8
Set port-role	set port-role <range> <access trunk hybrid> [vid]	Used to set the egress rule. Configure the port roles.	<range>: ports to be set, syntax 1, 5-7, available from 1 to 8 <access>: do not tag frames <trunk>: tag all frames <hybrid>: tag all	<range>: 1 to 8 <vid>: 1 to 4094

Command	Syntax	Description	Argument	Possible Value
			frames except a specific VID <vid>: untag-vid for hybrid port	
Set pvid	set pvid <range> <pvid>	Used to set the PVID of the VLAN	<range> ports to be set PVID(s), 1, 5-7, available from 1 to 8 <pvid>; PVIDs to be set, available 1 to 4094	<range>: 1 to 8 <pvid>: 1 to 4094
Set tag-group	set tag-group <vid> <name> <range> <#>	Used to add or edit the tag-based vlan group	<vid>: vlan ID, range from 1 to 4094 <name>: tag-vlan name <range>: vlan group members, syntax 1, 5-7, available from 1 to 8 <#>: sym/asym vlan setting. 1:symmetric vlan, 0: asymmetric vlan	<vid>: 1 to 4094 <range>: 1 to 8 <#>: 0 or 1
Show group	show group	Used to display the VLAN mode and VLAN group	None	None
Show pvid	show pvid	Used to display pvid, ingress/egress rule	None	None
VS				
Disable	disable	Used to disable the virtual stack	None	None
Enable	enable	Used to enable the virtual stack	None	None
Set gid	set gid <gid>	Used to set the group ID	<gid>: group ID	<gid>: a-z, A-Z, 0-9
Set role	set role <master slave>	Used to set role	<master slave>: master: act as master, slave: act as slave	<master slave> ; master or slave
Show	show	Used to display the configuration of the virtual stack.	None	None

7.0 Maintenance

- The possible causes for a no link LED status are as follows:
- The attached device is not powered on
- The cable may not be the correct type or is faulty
- The installed building premise cable is faulty
- The port may be faulty

7.1 Examples

1. Computer A connects to Computer B but cannot connect to Computer C.
 - a. The network cable from Computer C may be faulty. Check the link/act status of Computer C on the LED indicator. Try another network device with this connection.
 - b. The network configuration of Computer C may be faulty. Verify the network configuration on Computer C.
2. The uplink connection function fails to work.
 - a. Please check the uplink setup of the Managed Switch to verify the uplink function is enabled.
3. The console interface does not appear on the console port connection.
 - a. The COM port default parameters are: Baud Rate: 57600, Data Bits: 8, Parity Bits: None, Stop Bit: A, Flow Control: None. Check the COM port to confirm that it is working properly in the terminal program and that you are using the correct COM port.
 - b. Check the RS-232 cable is to make sure it is connected to console port on the switch and the COM port of PC.
 - c. Check to make sure the COM port of the PC is enabled.

8.0 Troubleshooting

All Waters' switching products are designed to provide reliability and consistently high performance in all network environments. The installation of Waters' ProSwitch GSM switch is a straightforward procedure. Should problems develop during installation or operation, this section is intended to help locate, identify and correct these types of problems. Please follow the suggestions listed below prior to contacting your supplier. However, if you are unsure of the procedures described in this section or if the Waters' GSM switch is not performing as expected, do not attempt to repair the unit; instead contact your supplier for assistance or contact Waters Network Systems' Customer Support Center at **800.328.2275** or email carolynl@watersnet.com.

8.1 Before Calling for Assistance

1. If difficulty is encountered when installing or operating the unit, refer back to the Installation Section of this manual. Also check to make sure that the various components of the network are operational and compatible.
2. Check the cables and connectors to ensure that they have been properly connected and the cables/wires have not been crimped or in some way impaired during installation. (About 90% of network downtime can be attributed to wiring and connector problems.)
3. Make sure that an AC power cord is properly attached to the GSM.
4. Be certain that each AC power cord is plugged into a functioning electrical outlet. Use the PWR LEDs to verify each unit is receiving power.
5. If the problem is isolated to a network device other than the Waters' GSM switch, it is recommended that the problem device be replaced with a known good device. Verify whether or not the problem is corrected. If not, go to next step. If the problem is corrected, the Waters' GSM switch and its associated cables are functioning properly.
6. If the problem continues, contact Waters Network Systems Customer Service at 800.328.2275 or email carolynl@watersnet.com for assistance.

When Calling for Assistance

Please be prepared to provide the following information.

1. A complete description of the problem, including the following:
 - a. The nature and duration of the problem
 - b. Situations when the problem occurs
 - c. The components involved in the problem
 - d. Any particular application that, when used, appears to create the problem
2. An accurate list of Waters Network Systems product model(s) involved. Include the date(s)

that you purchased the products from your supplier.

3. It is useful to include other network equipment models and related hardware, including personal computers, workstations, terminals and printers; plus, the various network media types being used.
4. A record of changes that have been made to your network configuration prior to the occurrence of the problem. Any changes to system administration procedures should all be noted in this record.

8.2 Return Material Authorization (RMA) Procedure

All returns for repair must be accompanied by a Return Material Authorization (RMA) number. To obtain an RMA number, call Waters Network Systems Customer Service at 800.328.2275 during business hours of 8:00 am to 5:00 pm (CT) or email carolynl@watersnet.com. When calling, please have the following information readily available:

- Name and phone number of your contact person
- Name of your company/institution
- Your shipping address
- Product name
- Failure symptoms, including a full description of the problem
- Waters Network Systems will carefully test and evaluate all returned products, will repair products that are under warranty at no charge, and will return the warranty-repaired units to the sender with shipping charges prepaid (see Warranty Information at the end of this manual for complete details). However, if Waters cannot duplicate the problem or condition causing the return, the unit will be returned as: **No Problem Found**.

Waters Network Systems reserves the right to charge for the testing of non-defective units under warranty. Testing and repair of product that is not under warranty will result in a customer (user) charge.

8.3 Shipping and Packaging Information

Should you need to ship the unit back to Waters Network Systems, please follow these instructions: Package the unit carefully. It is recommended that you use the original container if available. Units should be wrapped in a "bubble-wrap" plastic sheet or bag for shipping protection. (You may retain all connectors and this Installation Guide.) CAUTION: Do not pack the unit in Styrofoam "popcorn" type packing material. This material may cause electro-static shock damage to the unit.

Clearly mark the Return Material Authorization (RMA) number on the outside of the shipping container. Waters Network Systems is not responsible for your return shipping charges.

Ship the package to:

Waters Network Systems
Attention: Customer Service
945 37th Avenue, NW
Rochester, MN 55901

9.0 Warranty

Waters Network Systems' Warranty Statement

Waters Network Systems' products are warranted against defects in materials and workmanship. The warranty period for each product will be provided upon request at the time of purchase. Unless otherwise stated, the warranty period is for the useable life of the product.

In the event of a malfunction or other indication of product failure attributable directly to faulty materials and/or workmanship, Waters Network Systems will, at its option, repair or replace the defective products or components at no additional charge as set for herein. This limited warranty does not include service to repair damage resulting from accident, disaster, misuse, neglect, lightning, acts of God, tampering or product modification.

Service under the warranty may be obtained by contacting Waters Network Systems and receiving a Return Material Authorization (RMA) number from Waters Network Systems. Returned product accompanied with the issued RMA number and prepaid shipping will be repaired or replaced by Waters Network Systems. Repaired or replaced products will be returned at no cost to the original Buyer and shipped via the carrier and method of delivery chosen by Waters Network Systems.

Specific warranty by product family is as follows:

ProSwitch-Secure:	Limited Lifetime (see note)
ProSwitch-SecureAir+:	Limited Lifetime
ProSwitch-Lite:	3 Years from date of manufacture (see note)
ProSwitch-Xpress:	Limited Lifetime
ProSwitch-PSX	Limited Lifetime
ProSwitch-Xtreme:	Limited Lifetime (see note)
ProSwitch-FlexPort:	Limited Lifetime
ProSwitch-FixPort:	Limited Lifetime
ProSwitch-CS and CSX:	3 Years from date of manufacture (see note)
ProMedia Converters	3 Years from date of manufacture (see note)

Note: Warranty period for any and all external power supplies is one (1) year from date of purchase.

EXCEPT FOR THE EXPRESS WARRANTY SET FORTH ABOVE, *WATERS NETWORK SYSTEMS* GRANTS NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, BY STATUTE OR OTHERWISE, REGARDING THE PRODUCTS, THEIR FITNESS FOR ANY PURPOSE, THEIR QUALITY, THEIR MERCHANTABILITY, OR OTHERWISE.

WATERS NETWORK SYSTEMS' LIABILITY UNDER THE WARRANTY SHALL BE LIMITED TO PRODUCT REPAIR, OR REPLACEMENT OF THE BUYER'S PURCHASE PRICE. IN NO EVENT SHALL *WATERS NETWORK SYSTEMS* BE LIABLE FOR THE COST OF PROCUREMENT OF SUBSTITUTE GOODS BY THE CUSTOMER OR FOR ANY CONSEQUENTIAL OR INCIDENTAL DAMAGES FOR BREACH OR WARRANTY.