



**LevelOne**

**GSW-1290**

4-port 1000T/mini GBIC + 2 expandable slots  
L2 SNMP Gigabit Switch

**User`s Manual**

## **Copyright**

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

## **Trademarks**

All product, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

## **FCC Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

## **CE Declaration of Conformity**

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B, and EN 50082-1. This meets the essential protection requirements of the European Council Directive 89/336/EEC on the approximation of the laws of the member states relation to electromagnetic compatibility.

## Table of Contents

---

About This Manual .....	vii
<i>Intended Readers</i> .....	vii
<i>Typographical Conventions</i> .....	vii
<i>Notes, Notices, and Cautions</i> .....	viii
<b>Safety Instructions .....</b>	<b>viii</b>
<b>Introduction .....</b>	<b>11</b>
Switch Description .....	11
Features .....	11
Front Panel Components .....	13
<i>LED Indicators</i> .....	13
<i>Stacking LED Indicators</i> .....	14
Rear Panel Description .....	14
Plug-in Modules .....	15
<i>MDU-1290T 1000BASE-T Module</i> .....	15
<i>MDU-1290M SFP (Mini GBIC) Module</i> .....	15
<i>MDU-1290S IEEE 1394 Stacking Module</i> .....	16
Switch Stacking .....	16
Management Options .....	17
<b>Installation .....</b>	<b>19</b>
Package Contents .....	19
Before You Connect to the Network .....	19
<i>Installing the Switch without the Rack</i> .....	20
<i>Installing the Switch in a Rack</i> .....	20
<i>Connecting Stacked Switch Groups</i> .....	23
<i>Configuring a Switch Group for Stacking</i> .....	25
<i>Connecting the Console Port</i> .....	28
<i>Password Protection</i> .....	28
<i>SNMP Settings</i> .....	29
<i>IP Address Assignment</i> .....	30
<i>Connecting Devices to the Switch</i> .....	32
<b>Basic Switch Management .....</b>	<b>33</b>
Before You Start .....	33
Web-based User Interface .....	34
<i>Areas of the User Interface</i> .....	34
<i>Login to Web Manager</i> .....	35
<i>Web Pages and Folders</i> .....	35
<i>Switch Information</i> .....	36
Switch IP Settings .....	36
<i>Security IP Management Stations Configuration</i> .....	38
User Account Management .....	40
<i>Admin and User Privileges</i> .....	41
Save Changes .....	41
Factory Reset .....	42
<i>Restart System</i> .....	43
<i>Advanced Settings</i> .....	44

Stack Information .....	46
<b>System Configuration .....</b>	<b>49</b>
Port Configuration .....	50
Port Mirroring .....	51
Traffic Control.....	52
Link Aggregation .....	53
LACP Port Settings.....	55
IGMP .....	56
IGMP Snooping.....	56
Static Router Ports Entry.....	58
Spanning Tree.....	59
Switch Spanning Tree Settings.....	60
STP Port Settings.....	63
Forwarding & Filtering .....	65
Unicast Forwarding .....	65
Multicast Forwarding.....	66
Multicast Port Filtering Mode.....	67
VLANs .....	68
802.1Q Static VLANs.....	71
GVRP Setting.....	74
QoS .....	76
802.1p Default Priority.....	76
802.1p User Priority.....	77
QoS Output Scheduling Configuration .....	77
Traffic Segmentation.....	78
Bandwidth Control .....	80
MAC Notification .....	81
Global Settings .....	81
Port Settings .....	82
System Log Server.....	83
Port Security.....	85
SNTP Settings.....	86
Current Time and SNTP Settings.....	86
Time Zone and DST.....	87
Access Profile Table .....	89
<b>Security Management .....</b>	<b>97</b>
Trusted Host.....	97
Port Access Entity .....	98
802.1X Authenticator Settings .....	100
PAE System Control .....	103
Radius Server.....	106
<b>SNMP Management .....</b>	<b>108</b>
SNMPV3 .....	108
SNMP User Table.....	108
SNMP View Table.....	111
SNMP Group Table .....	112
SNMP Community Table .....	114
SNMP Host Table .....	116
SNMP Engine ID.....	117

<b>Network and System Monitoring</b> .....	<b>118</b>
Port Utilization .....	120
Packets .....	121
<i>Received Packets</i> .....	121
<i>Received Unicast/Multicast/Broadcast Packets</i> .....	122
<i>Transmitted Packets</i> .....	124
Errors .....	125
<i>Received Errors</i> .....	126
<i>Transmitted Errors</i> .....	128
<i>Packet Size</i> .....	130
MAC Address .....	131
Switch History .....	133
IGMP Snooping .....	134
Browser Router Port.....	135
VLAN Status.....	136
Session Table .....	136
Authenticator State.....	137
<b>System Maintenance</b> .....	<b>138</b>
TFTP Services .....	138
<i>Download Firmware</i> .....	138
<i>Download Configuration File</i> .....	139
<i>Save Settings</i> .....	139
<i>Save History Log</i> .....	139
Ping Test .....	140
Save Changes.....	140
Factory Reset.....	141
Restart System.....	141
<i>Logout</i> .....	142
<b>Technical Specifications</b> .....	<b>143</b>



## About This Manual

This manual is divided into two general sections:

Chapters 1-3 provide **Basic Setup** information. This is where you will find a general introduction to the Switch, its hardware and management features, as well as a guide to setting up the Switch hardware and initial configuration.

Chapters 4-8 discuss **Advanced Configuration** topics. These chapters describe management and configuration of Switch features, following the layout of the Switch's Web Manager. Each of the Switch's six main folders—Configuration, Security, Management, Monitoring, Maintenance, and Single IP Management—has a separate chapter devoted to it.

## Intended Readers

The GSW-1290 User Manual contains information useful for setup and management and of the LevelOne GSW-1290 Switch. This manual is intended for network managers familiar with network management concepts and terminology.

## Typographical Conventions

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry. For example: [ <b>copy filename</b> ] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
<b>Bold font</b>	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the <b>File</b> menu and choose <b>Cancel</b> . Used for emphasis. May also indicate system messages or prompts appearing on your screen. For example: You have mail. Bold font is also used to represent filenames, program names and commands. For example: use the <b>copy</b> command.
<b>Boldface Typewriter Font</b>	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
<b>Initial capital letter</b>	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click <b>Enter</b> .
<i>Italics</i>	Indicates a window name or a field. Also can indicate a variables or parameter that is replaced with an appropriate word or string. For example: type <i>filename</i> means that you should type the actual filename instead of the word shown in italic.
<b>Menu Name &gt; Menu Option</b>	Indicates the menu structure. <b>Device &gt; Port &gt; Port Properties</b> means the Port Properties menu option under the Port menu option that is located under the Device menu.

## Notes, Notices, and Cautions



**NOTE:** A NOTE indicates important information that helps you make better use of your device.



**NOTICE:** A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



**CAUTION:** A CAUTION indicates a potential for property damage, personal injury, or death.

## Safety Instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage. Throughout this safety section, the caution icon (  ) is used to indicate cautions and precautions that you need to review and follow.



### Safety Cautions

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the following precautions.

Observe and follow service markings. Do not service any product except as explained in your system documentation. Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock. Components inside these compartments should be serviced only by a trained service technician.

If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:

- The power cable, extension cable, or plug is damaged.
- An object has fallen into the product.
- The product has been exposed to water.
- The product has been dropped or damaged.
- The product does not operate correctly when you follow the operating instructions.

Keep your system away from radiators and heat sources. Also, do not block cooling vents.

Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.

Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.

Use the product only with approved equipment.

Allow the product to cool before removing covers or touching internal components.

Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.

To help avoid damaging your system, be sure the voltage selection Switch (if provided) on the power supply is set to match the power available at your location:

- 115 volts (V)/60 hertz (Hz) in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
- 100 V/50 Hz in eastern Japan and 100 V/60 Hz in western Japan
- 230 V/50 Hz in most of Europe, the Middle East, and the Far East

Also be sure that attached devices are electrically rated to operate with the power available in your location.

Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.



**NOTE:** A qualified electrician must perform all connections to DC power and to safety grounds. All electrical wiring must comply with applicable local or national codes and practices.

To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.

Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.

To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).

Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.

Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.

When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:

- Install the power supply before connecting the power cable to the power supply.
- Unplug the power cable before removing the power supply.
- If the system has multiple sources of power, disconnect power from the system by unplugging ALL power cables from the power supplies.

Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.



## General Precautions for Rack-Mountable Products

Observe the following precautions for rack stability and safety. Also refer to the rack installation documentation accompanying the system and the rack for specific caution statements and procedures.

Systems are considered to be components in a rack. Thus, "component" refers to any system as well as to various peripherals or supporting hardware.



**CAUTION:** Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack.

After installing system/components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a component from the rack.
- Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.
- After a component is inserted into the rack, carefully extend the rail into a locking position, and then slide the component into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step on or stand on any component when servicing other components in a rack.



**CAUTION:** The system chassis must be positively grounded to the rack cabinet frame. Do not attempt to connect power to the system until grounding cables are connected. A qualified electrical inspector must inspect completed power and safety ground wiring. An electrical shock hazard will exist if the safety ground cable is omitted or disconnected.



**CAUTION:** Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

## Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your system. To prevent static damage, discharge static electricity from your body before you touch any of the electronic components, such as the microprocessor. You can do so by periodically touching an unpainted metal surface on the chassis.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.

When transporting a sensitive component, first place it in an antistatic container or packaging.

Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads and an antistatic grounding strap.

# Chapter 1

## Introduction

**Switch Description**

**Features**

**Front Panel Components**

**LED Indicators**

**Stacking LED Indicators**

**Rear Panel Description**

**Plug-in Modules**

**Switch Stacking**

**Management Options**

## Switch Description

The GSW-1290 is a modular Gigabit Ethernet backbone Switch designed for adaptability and scalability. The Switch provides a management platform and uplink to backbone for a stacked group of up to twelve GSW-2492 Switches in a star topology arrangement. Alternatively, the Switch can utilize up to twelve Gigabit Ethernet ports to function as a central distribution hub for other Switches or Switch groups, or routers. The four built-in combination Gigabit ports have the option of being used as either 1000BASE-T or SFP Gigabit connections

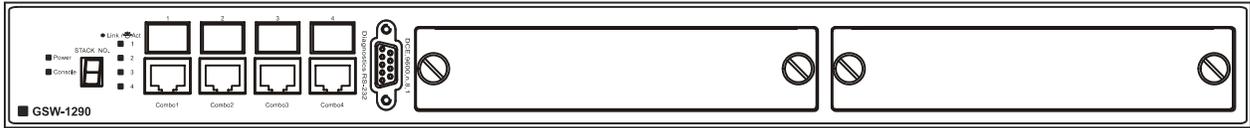
## Features

- Four built-in combination 10/100/1000BASE-T/SFP ports
- Two additional 4-port modules can be added to stack up to eight additional Switches (IEEE 1394) or up to eight additional Gigabit Ethernet ports (1000BASE-T or SFP) or use combination of stacking and Gigabit Ethernet ports.
- Four built-in 1000Base-T ports allow four GSW-2492 to stack.
- Star topology Switch stacking configuration for up to 12 additional GSW-2492 Switches.
- 24 Gbps Switching fabric capacity
- Supports 802.1D STP and 802.1w Rapid Spanning Tree for redundant back up bridge paths
- Supports 802.1Q VLAN
- Supports IGMP snooping
- Supports 802.1p Priority Queues and 802.3ad LACP Link Aggregation.
- Access Control Profile (ACL)
- Multi-layer Access Control (based on MAC address, IP address, VLAN, Protocol, 802.1p, DSCP)
- Quality of Service (QoS) customized control
- Port Security (MAC address table lock) and administrator-definable port security
- 802.1x (port-based and MAC-based) access control and RADIUS Client support
- Per-port bandwidth control
- Broadcast, Multicast and DLF storm control
- IEEE 802.3z and IEEE 802.3x compliant Flow Control for all Gigabit ports
- SNMP v.1, v.2, v.3 network management, RMON support
- Supports optional external Redundant Power Supply
- Flexible management platforms include web-based GUI manager, CLI commands via console or Telnet
- Supports BOOTP/DHCP/DNS Relay
- Supports TFTP upgrade
- Supports System Log
- Simple Network Time Protocol

- MAC address update notification
- Web GUI Traffic Monitoring
- Supports Single IP Management v.1.0
- Supports Traffic Segmentation

## Front Panel Components

The front panel of the Switch consists of LED indicators, an RS-232 communication port, two slide-in module slots, and four 1000BASE-T/SFP combination “Combo” ports.



**Figure 1-1. Front Panel View of the Switch as shipped (no modules are installed)**

Comprehensive LED indicators display the status of the Switch and the network.

An RS-232 DCE console port for setting up and managing the Switch via a connection to a console terminal or PC using a terminal emulation program.

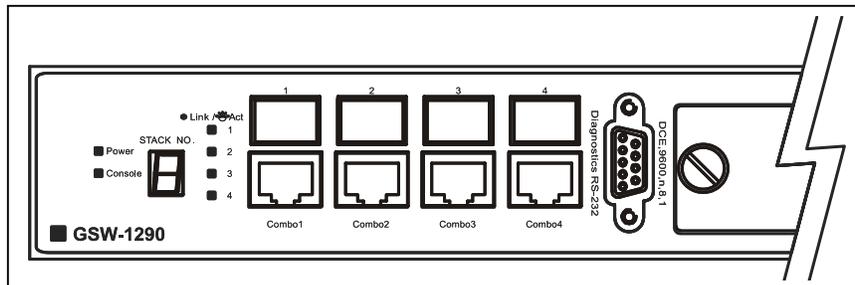
A front-panel slide-in module slot for Gigabit Ethernet ports can accommodate a 4-port 1000BASE-T Gigabit Ethernet module, a 4-port Gigabit Ethernet SFP module, or a stacking module to connect to four GSW-2492 Switches.



**NOTICE:** The **Stack ID** LED on the Switch’s front panel will display an **F**, regardless of the Switch’s stacking mode (Master Switch in a Switch stack, or Standalone mode).

## LED Indicators

The LED indicators of the Switch include Power, Console, and Link/Act. The following shows the LED indicators for the Switch along with an explanation of each indicator.



**Figure 1-2. LED Indicators**

LED	Description
<b>Power</b>	This indicator on the front panel should be lit during the Power-On Self Test (POST). It will light green approximately two seconds after the Switch is powered on to indicate the ready state of the device.
<b>Console</b>	This indicator is lit green when the Switch is being managed via out-of-band/local console management through the RS-232 console port using a straight-through serial cable.
<b>Link/Act</b>	Each on-board Gigabit Ethernet port has a corresponding indicator. This will light steady green for a valid link and blink whenever there is reception or transmission (i.e. Activity--Act) of data occurring at a port.

See below for description of Stack ID LED indicator.

### Stacking LED Indicators

Stacking LED indicators include the Stack ID indicator on the front panel and the Link/Act indicators on the front of the MDU-1290S stacking module.



**NOTICE:** The four build-in combination ports on the front panel of the GSW-1290 can be configured as stacking ports using the CLI.

Each stacking module has a single **Link/Act** LED indicator on its front panel for each IEEE 1394 IN/OUT pair

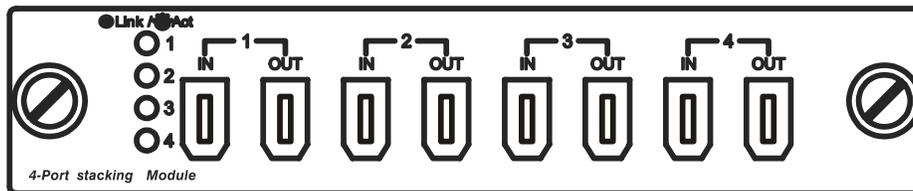


Figure 1-3. Front panel of MDU-1290S IEEE 1394 stacking module

<b>Link/Act</b>	The Link/Act LEDs have the same function as the corresponding LEDs for the Switch's built-in Gigabit Ethernet ports. The Link LED lights to confirm a valid link, while the Act LED blinks to indicate activity on the link.
<b>Stack ID</b>	The Switch includes a digital indicator to indicate the Switch status in a stacked Switch group. An "F" indicates the Switch is acting in the capacity of a master Switch of a stacked group of GSW-1290/GSW-2492 Switches. The remaining slave Switches in the group will display a corresponding stack number (1-C) to indicate the logical position of the slave Switch in the stacked group. See the discussion of Switch Stacking below for more information on stacking GSW-1290/GSW-2492 Switches.



**NOTICE:** Do not connect the stacked Switch group to the network until you have properly configured all Switches for stacking. An improperly configured Switch stack can cause a broadcast storm.

### Rear Panel Description

The rear panel of the Switch contains an AC power connector.



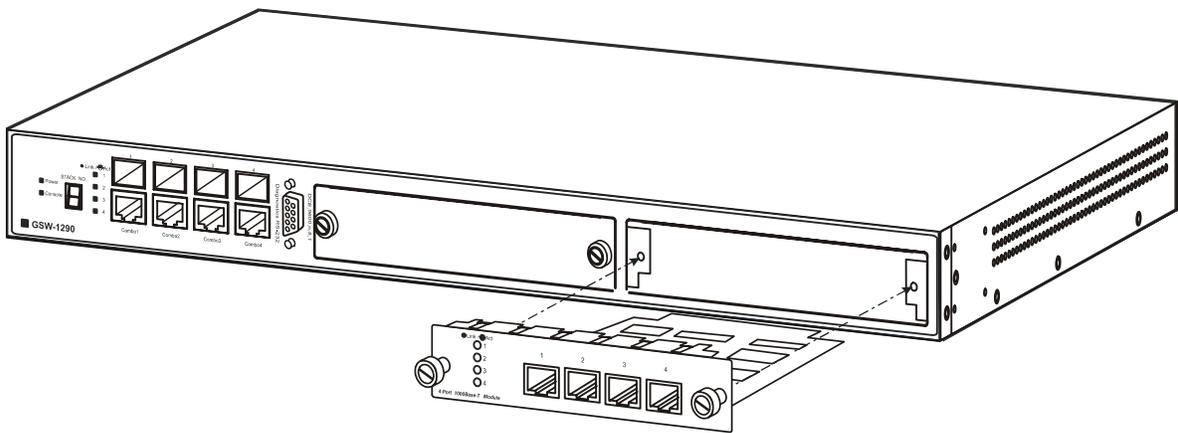
**Figure 1-4. Rear panel view of the Switch**

The AC power connector is a standard three-pronged connector that supports the power cord. Plug-in the female connector of the provided power cord into this socket, and the male side of the cord into a power outlet. The Switch automatically adjusts its power setting to any supply voltage in the range from 100 ~ 240 VAC at 50 ~ 60 Hz.

## Plug-in Modules

The GSW-1290 Switch is able to accommodate optional plug-in modules in order to increase functionality and performance. Two modules may be installed and used in combination with any of the three available modules. Plug-in modules must be purchased separately.

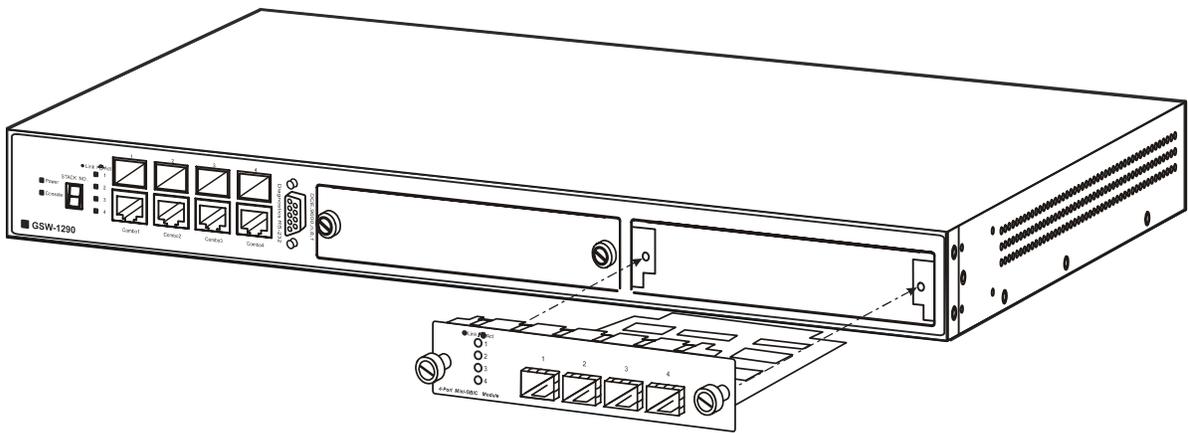
### MDU-1290T 1000BASE-T Module



**Figure 1-5. 1000BASE-T Four-port module**

- Front-panel module
- Connects to 1000BASE-T devices
- LED indicators for Link/Activity

### MDU-1290M SFP (Mini GBIC) Module



**Figure 1-6. Four-port Gigabit SFP module**

- Front-panel module
- Connects to Gigabit Ethernet devices
- LED indicators for Link/Activity and Status

### MDU-1290S IEEE 1394 Stacking Module

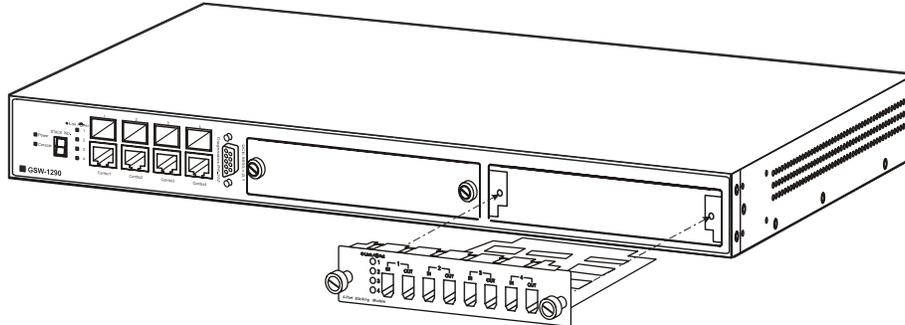


Figure 1-7. MDU-1290S IEEE 1394 Stacking module

- Front-panel module
- Connect to four GSW-2492 Switches (up to eight additional slave units may be stacked)
- Four transmitting ports and Four receiving port
- Use the connector of IEEE 1394b
- Data rate up to 1000 Mbps
- 8-segment LED display to indicate Switch ID number within the Switch stack

### Switch Stacking

The GSW-1290 can be stacked with a GSW-2492, functioning as a Master of the stack. There are two connection options available to for stacking. One option is to use the built-in combination ports (1000BASE-T/SFP). The other possibility is to install one or two MDU-1290S stacking modules and complete the stacking connection through the IEEE 1394 stacking ports. With two stacking modules installed, the GSW-1290 can be stacked with as many as twelve slave units.

Each optional stacking module allows up to four GSW-2492 Switches to be interconnected in a stack with the GSW-1290. Two stacking modules may be used to form a nine-Switch stack consisting of one Master and eight Slaves, managed through the GSW-1290 Master Switch. The stacked group has a single IP address and is managed as a single device. The entire Switch stack is managed and monitored through the network or alternatively, through the serial port on the GSW-1290. The stacking modules connect to the slaves using IEEE 1394 serial cable (Firewire) in a star topology for GSW-2492 groups (see illustration on page 19).

The stacking ports are marked **IN** and **OUT**. The IEEE 1394 compliant cable must be connected from an **IN** port on one Switch to an **OUT** port on the next Switch in the stack.

### Restrictions and Cautions for Stacking

The GSW-1290 may serve as the Master of up to twelve additional Switches. The slave Switch units must meet the following criteria:

All additional slave Switches must be the same model - that is, the slaves must be all GSW-2492 Switches. The slave unit types cannot be mixed within a single stacked group. Make sure that all Switches in the group have the latest firmware installed.

The GSW-1290 is automatically started as the Master Switch when it is connected in a Switch stack. It is necessary however to enable stacking for each slave Switch in a stacked group before interconnecting them and before connecting the group to the network. Stacking can be enabled by connecting to each slave through the console port and using the CLI stacking configuration command. Before stacking has been enabled on the slaves, the IEEE 1394 port is treated logically as an individual 1000BASE port in full-duplex mode. Since the Spanning Tree Protocol is disabled by default, a broadcast storm will result if the stacking link is completed between Switches that have not been properly configured.



**NOTE:** The CLI stacking command set for the GSW-1290 is slightly different from the CLI stacking command set for the GSW-2492. Please refer to the CLI Reference Manual for details.

## Management Options

The system may be managed out-of-band through the console port on the front panel or in-band using Telnet, a web browser or SNMP-based management.

### Web-based Management Interface

After you have successfully installed the Switch, you can configure the Switch, monitor the LED panel, and display statistics graphically using a web browser, such as Opera, Netscape Navigator (version 6.2 and higher) or Microsoft® Internet Explorer (version 5.0).



**NOTE:** To access the Switch through a web browser, the computer running the web browser must have IP-based network access to the Switch.

### Command Line Console Interface through the Serial Port or Telnet

You can also connect a computer or terminal to the serial console port or use Telnet to access the Switch. The command-line-driven interface provides complete access to all Switch management features. For a full list of commands, see the Command Line Reference Manual, which is included on the documentation CD.

### SNMP-Based Management

You can manage the Switch with an SNMP-compatible console program. The Switch supports SNMP version 1.0, version 2.0 and version 3.0. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

The Switch supports a comprehensive set of MIB extensions:

- RFC 1643 Ether-like MIB
- RFC 1724 RIPv2 MIB
- RFC 1757 RMON
- RFC 1850 OSPF MIB
- RFC 1907 SNMPv2 MIB
- RFC 2021 RMON II MIB
- RFC 2096 IP-FORWARD MIB
- RFC 2233 IF-MIB
- RFC 2358 Ethernet-Link MIB
- RFC 2573 SNMP Notification and Target MIB
- RFC 2574 SNMP User-based SM MIB
- RFC 2575 SNMP View-based ACM MIB

- RFC 2674 802.1p and 802.1q Bridge MIB
- RFC 2737 Entity MIB
- RFC 2932 IPMROUTE STD MIB
- RFC 2933 IGMP MIB
- RFC 2934 PIM MIB
- IEEE8021-PAE 802.1x PAE MIB

## Chapter 2

### Installation

#### *Package Contents*

#### *Before You Connect to the Network*

#### *Installing the Switch without a Rack*

#### *Installing the Switch in a Rack*

#### *Connecting Stacked Switch Groups*

#### *Configuring a Switch Group for Stacking*

#### *External Redundant Power System*

#### *Connecting the Console Port*

#### *Password Protection*

#### *SNMP Settings*

#### *IP Address Assignment*

#### *Connecting Devices to the Switch*

### **Package Contents**

Before you begin installing the Switch, confirm that your package contains the following items:

1. One GSW-1290 Layer 2 Switch
2. Mounting kit: 2 mounting brackets and screws
3. Four rubber feet with adhesive backing
4. One AC power cord
5. This User Manual
6. CLI Reference Manual

### **Before You Connect to the Network**

Before you connect to the network, you must install the Switch on a flat surface or in a rack, set up a terminal emulation program, plug in the power cord, and then set up a password and IP address.



**NOTICE:** Do not connect the Switch to the network until you have established the correct IP settings, user accounts and proper stacking configuration (if the Switch is stacked).

## Installing the Switch without the Rack

The Switch is supplied with rubber feet for stationing it on a flat surface and mounting brackets and screws for mounting the Switch in a rack.

Install the Switch on a level surface that can safely support the weight of the Switch and its attached cables. The Switch must have adequate space for ventilation and for accessing cable connectors.

Set the Switch on a flat surface and check for proper ventilation. Allow at least 5 cm (2 inches) on each side of the Switch and 15 cm (6 inches) at the back for the power cable.

Attach the rubber feet on the marked locations on the bottom of the chassis.

The rubber feet, although optional, are recommended to keep the unit from slipping.

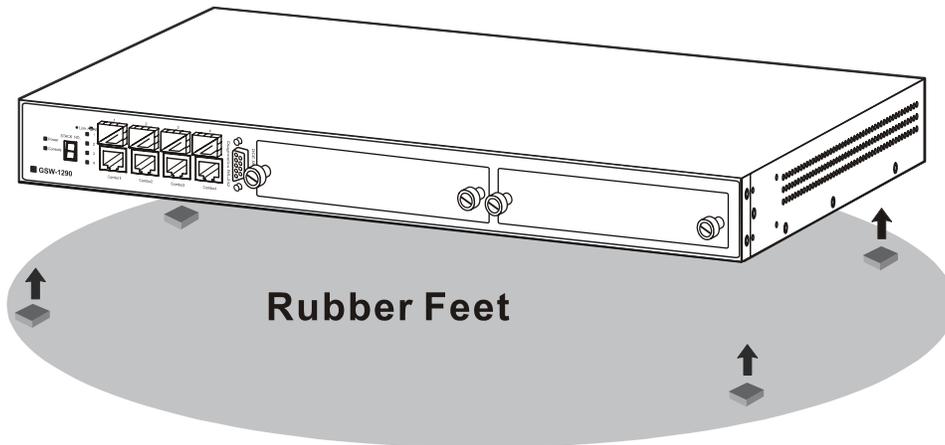


Figure 2-1. Install rubber feet for installations with or without a rack

## Installing the Switch in a Rack

You can install the Switch in most standard 19-inch (48.3-cm) racks. Refer to the illustrations below.

Use the supplied screws to attach a mounting bracket to each side of the Switch.

Align the holes in the mounting bracket with the holes in the rack.

Insert and tighten two screws through each of the mounting brackets.

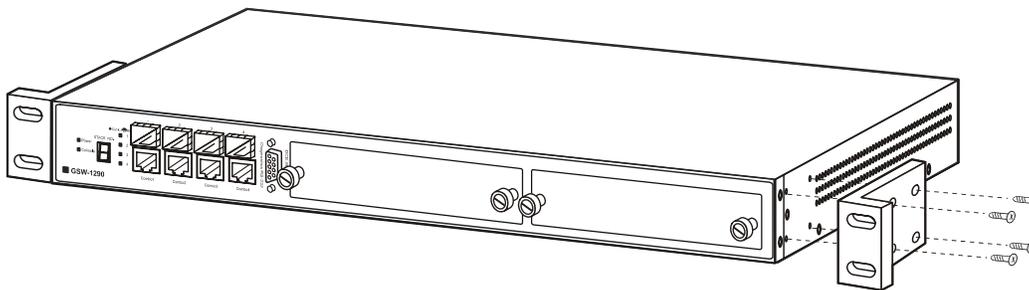
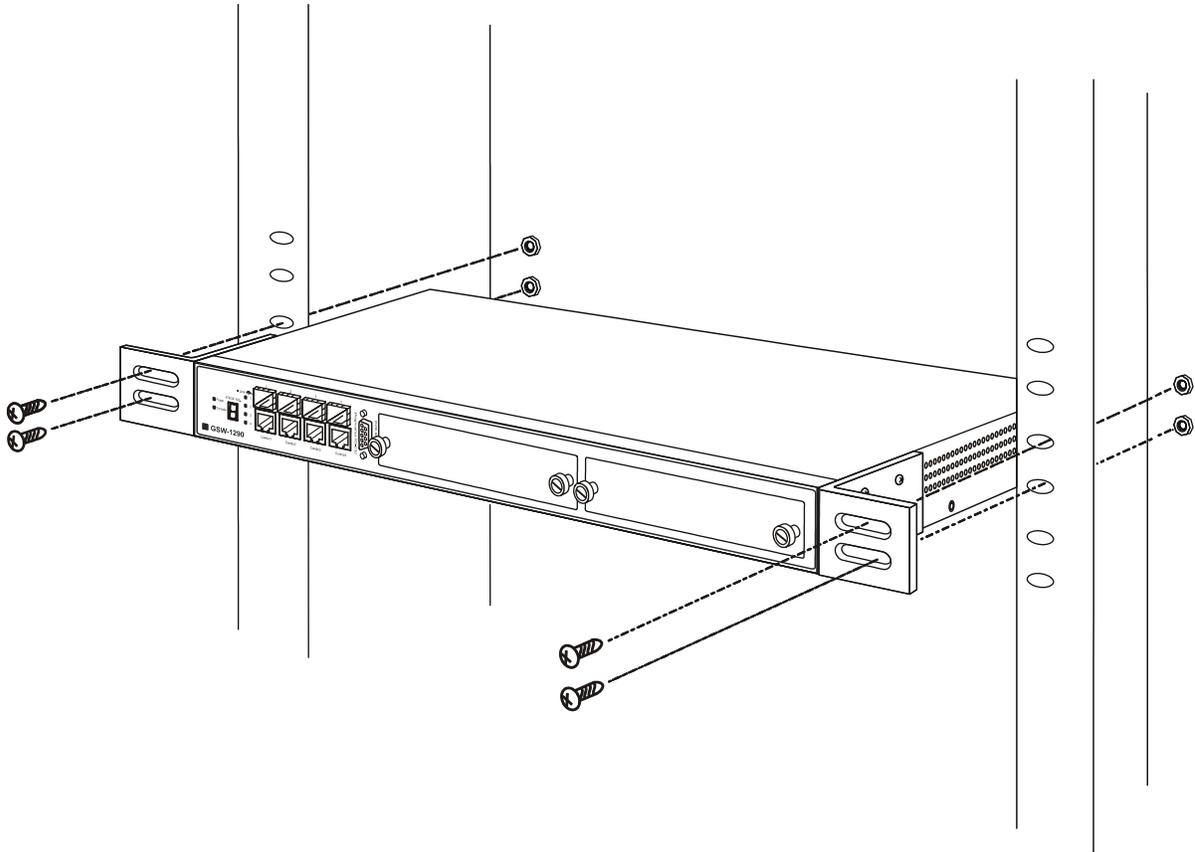


Figure 2-2. Attach mounting brackets



**Figure 2-3. Install Switch in equipment rack**



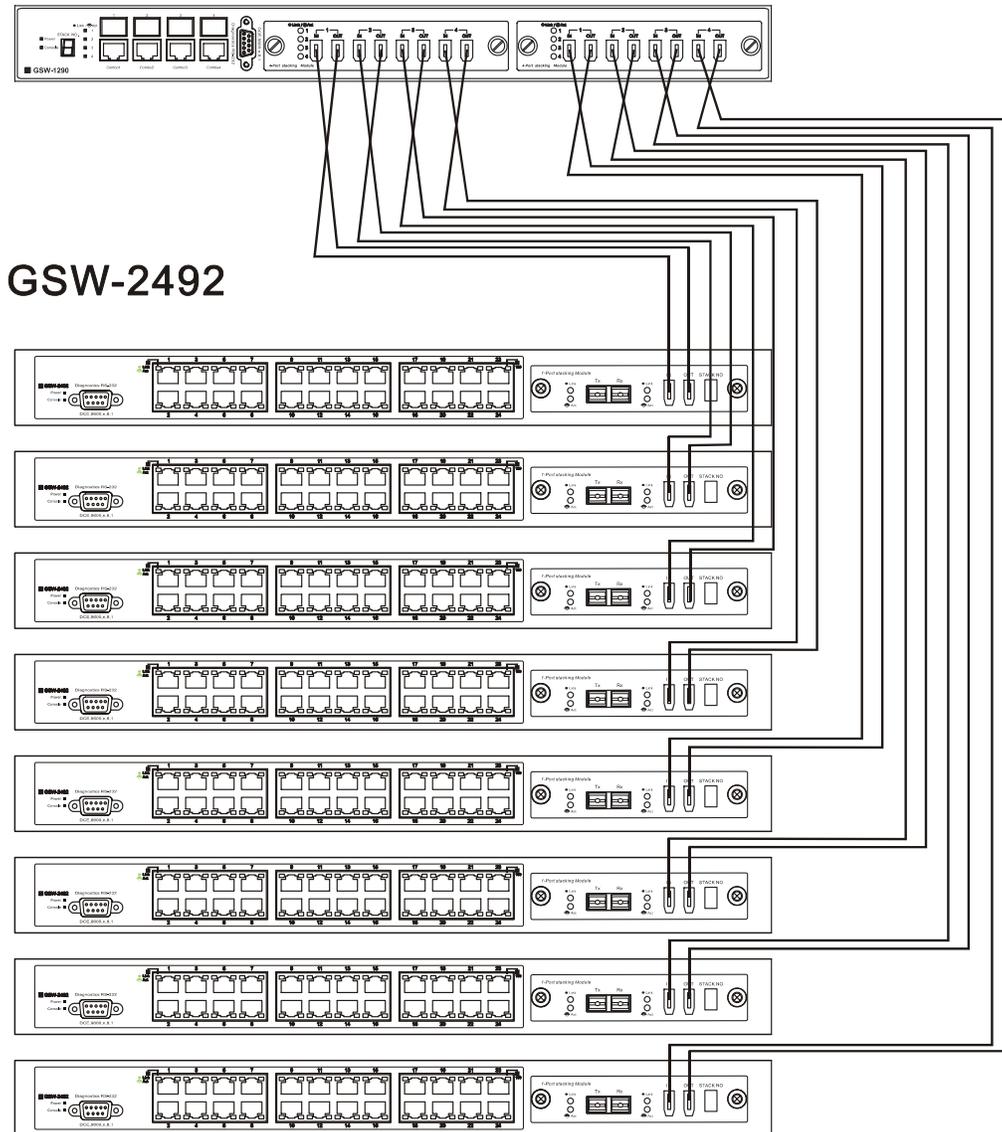
## Connecting Stacked Switch Groups

The GSW-1290 may be configured to function as the Master of a stacked group of GSW-2492 Switches (see Restrictions for Stacking on page 16). A stacked group of GSW-2492 Switches connects to the GSW-1290 in a star topology. The instructions below, tell you how to configure the GSW-1290 to function as a Master, as well as how to configure the GSW-2492 to function as a slave Switch units using the CLI interface.



**NOTICE:** Do not connect the stacked Switch group to the network until you have properly configured all Switches for stacking. An improperly configured Switch stack can cause a broadcast storm.

### GSW-1290



**Figure 2-4. Star topology stacked Switch group connected via IEEE 1394 cabling**

The stacking ports are marked **IN** and **OUT**. The IEEE 1394 compliant cable must be connected from an **IN** port on one Switch to an **OUT** port on the next Switch in the stack.

## Configuring a Switch Group for Stacking

Follow the instructions below to first configure the slave units, and then to configure the GSW-1290 as the designated Master.



**NOTICE:** The GSW-1290 can be used to manage a Switch stack consisting of only GSW-2492 Switches.

For the GSW-2492 the stacking configuration as a Master or Slave Switch is no longer necessary. The GSW-1290 can communicate with a GSW-2492 regardless of its stacking configuration. It is recommended that you configure all GSW-2492 Switches in a Switch stack in the auto stacking mode to reduce the potential for problems. The default stacking mode configuration for the GSW-2492 is auto.

To configure the GSW-2492 to function in a stacked group as a slave, do the following:

At the CLI login prompt, enter **config stacking mode enable auto** and press the **Enter** key.

You will be prompted to save the stacking mode configuration. Press the Y key (yes) to save the stacking mode configuration.

Successful configuration will be verified by a **Success** message. It takes a few seconds for the change to take effect and be saved. See the example below for the GSW-2492.

```
GSW-2492:4#config stacking mode enable auto
Command: config stacking mode enable auto

Do you want to save the new system configuration to NV-RAM now?(y/n)
Saving all configurations to NV-RAM... Done.
Success.

GSW-2492:4#.....
```

The default settings for the GSW-1290 has the stacking mode enabled. However if the stacking mode has been disabled it will be necessary to enable it. Follow the instructions below to change the stacking mode to enable. If you do not know what the stacking mode setting currently is, use the command **show stacking mode**.

To enable stacking in the GSW-1290, do the following:

At the CLI login prompt, enter **config stacking mode enable** and press the **Enter** key.

You will be prompted to save the stacking mode configuration. If you save the new stacking mode by pressing the Y key, the settings will be saved and the Switch will restart.

Press the Y key (yes) to save the stacking mode configuration and restart the switch.

**GSW-1290:4#config stacking mode enable**

**Command: config stacking mode enable**

**The new stacking mode configuration must be saved and the system restarted to put the new settings into effect.**

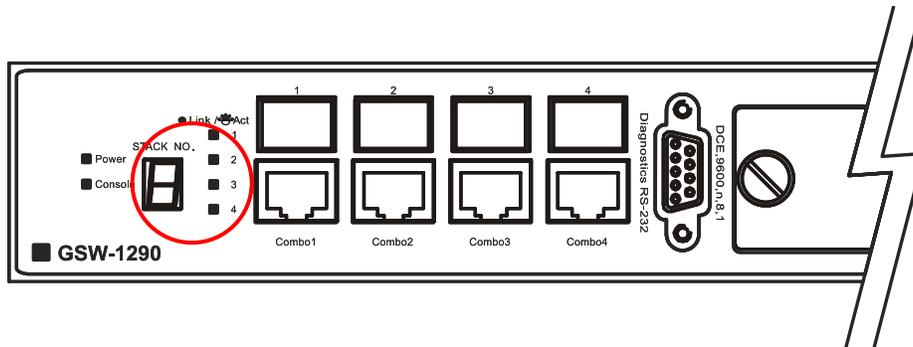
**If you do not save the changes now, they will be lost.**

**Saving all configurations to NV-RAM... 15%**

Changing the stacking mode in the GSW-1290 will automatically save the settings and restart the system. It will take a few minutes to complete the process.

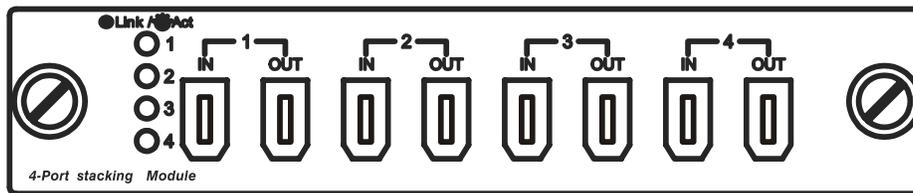
**Unit ID Display for Switches in a Switch Stack**

The Stack ID 7-segment LED (as shown below) on the front panel of the GSW-1290 will always display F (15 in hex). An F will also be displayed in the Stack ID LED even if the GSW-1290 is in standalone mode.



**Figure 2-5. GSW-1290 Front Panel (left side)**

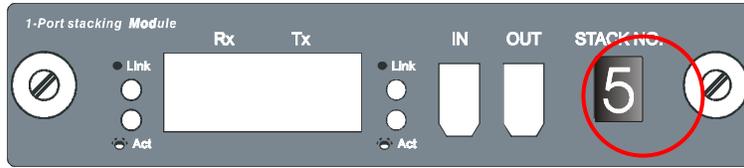
The Unit ID of individual GSW-2492 Switches in a Switch stack is determined by the port number of the port on the GSW-1290 that the Switch is connected to. The ports on the GSW-1290 are numbered starting with port 1 from left to right along the front panel of the Switch. For example, the four combination ports next to the Stack NO. LED are numbered 1 through 4, so if a four port stacking module is installed in the first module slot, the stacking ports will be numbered 5 through 8. If two stacking modules are installed in the GSW-1290, then the stacking ports on the second module will be numbered 9 through 12.



**Figure 2-6. MDU-1290S Stacking Module Front Panel**

If a stacking module is installed in the GSW-1290's first module slot, then the first IN/OUT pair in the figure above will be port 5. If a GSW-2492 in a Switch stack is connected to the first stacking port (port number 5 on the GSW-1290), then the Unit ID of the GSW-2492 will be 5.

The Unit ID of the GSW-2492 will be displayed in the STACK NO. LED on the front panel of the GSW-2492's stacking module, as shown below.



**Figure 2-7. MDU-2492S Stacking Module Front Panel**

## Connecting the Console Port

The Switch provides an RS-232 serial port that enables a connection to a computer or terminal for monitoring and configuring the Switch. This port is a male DB-9 connector, implemented as a data terminal equipment (DTE) connection.

To use the console port, you need the following equipment:

- A terminal or a computer with both a serial port and the ability to emulate a terminal
- A null modem or crossover RS-232 cable with a female DB-9 connector for the console port on the Switch
- To connect a terminal to the console port:
- Connect the female connector of the RS-232 cable directly to the console port on the Switch, and tighten the captive retaining screws.
- Connect the other end of the cable to a terminal or to the serial connector of a computer running terminal emulation software. Set the terminal emulation software as follows:
- Select the appropriate serial port (COM port 1 or COM port 2).
- Set the data rate to 9600 baud.
- Set the data format to 8 data bits, 1 stop bit, and no parity.
- Set flow control to `none`.
- Under Properties, select VT100 for Emulation mode.
- Select Terminal keys for Function, Arrow, and Ctrl keys. Ensure that you select Terminal keys (*not* Windows keys).



**NOTICE:** When you use HyperTerminal with the Microsoft® Windows® 2000 operating system, ensure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 allows you to use arrow keys in HyperTerminal's VT100 emulation. See [www.microsoft.com](http://www.microsoft.com) for information on Windows 2000 service packs.

After you have correctly set up the terminal, plug the power cable into the power receptacle on the back of the Switch. The boot sequence appears in the terminal.

After the boot sequence completes, the console login screen displays.

If you have not logged into the command line interface (CLI) program, press the Enter key at the User name and password prompts. There is no default user name and password for the Switch, user names and passwords must first be created by the administrator. If you have previously set up user accounts, log in and continue to configure the Switch.

Enter the commands to complete your desired tasks. Many commands require administrator-level access privileges. Read the next section for more information on setting up user accounts. See the *Command Line Reference* on the documentation CD for a list of all commands and additional information on using the CLI.

When you have completed your tasks, exit the session with the `logout` command or close the emulator program.

## Password Protection

The GSW-1290 does not have a default user name and password. One of the first tasks when settings up the Switch is to create user accounts. If you log in using a predefined administrator-level user name you have privileged access to the Switch's management software.

After your initial login, define new passwords for both default user names to prevent unauthorized access to the Switch, and record the passwords for future reference.

To create an administrator-level account for the Switch, do the following:

At the CLI login prompt, enter **create account admin** followed by the <user name> and press the **Enter** key.

You will be asked to provide a password. Type the <password> used for the administrator account being created and press the **Enter** key.



**NOTE:** Passwords are case sensitive.

You will be prompted to enter the same password again to verify it. Type the same password and press the **Enter** key.

Successful creation of the new administrator account will be verified by a **Success** message.

User names and passwords can be up to 15 characters in length.

The sample below illustrates a successful creation of a new administrator-level account with the user name “newmanager”.

```
GSW-1290:4#create account admin newmanager
Command: create account admin newmanager

Enter a case-sensitive new password:*****
Enter the new password again for confirmation:*****
Success.

GSW-1290:4#
```



**NOTICE:** CLI configuration commands only modify the running configuration file and are not saved when the Switch is rebooted. To save all your configuration changes in nonvolatile storage, you must use the **save** command to copy the running configuration file to the startup configuration.

## SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, Switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, Switch group or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The GSW-1290 supports the SNMP versions 1, 2c, and 3. You can specify which version of the SNMP you want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v.1 and v.2, user authentication is accomplished using ‘community strings’, which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

The default community strings for the Switch used for SNMP v.1 and v.2 management access are:

**public** - Allows authorized management stations to retrieve MIB objects.

**private** - Allows authorized management stations to retrieve and modify MIB objects.

SNMP v.3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMP v.1 while assigning a higher level of security to another group, granting read/write privileges using SNMP v.3.

Using SNMP v.3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMP v.3 in that SNMP messages may be encrypted. To read more about how to configure SNMP v.3 settings for the Switch read the next section, Management.

## Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast\Multicast Storm.

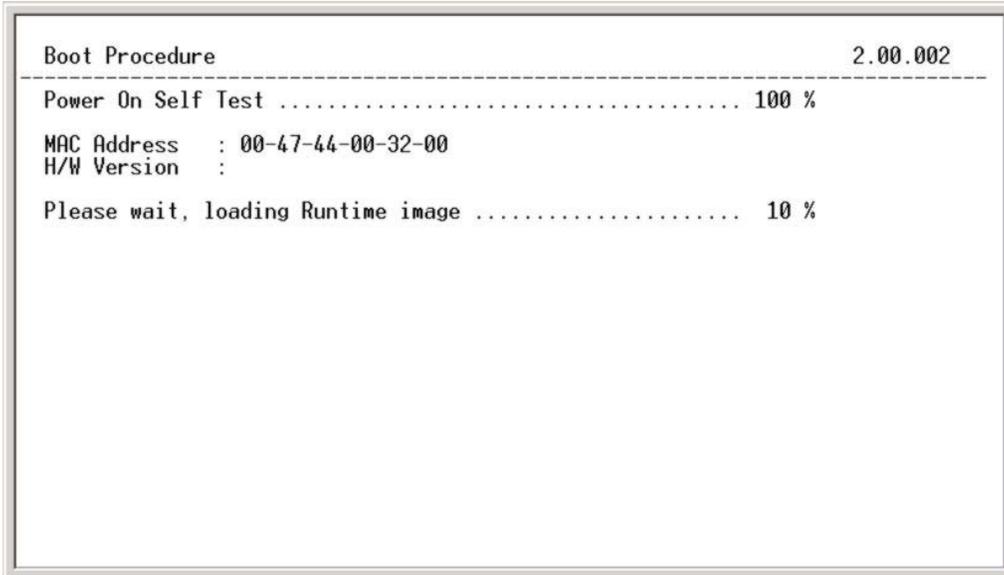
## MIBs

Management and counter information are stored by the Switch in the Management Information Base (MIB). The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. The proprietary MIB may also be retrieved by specifying the MIB Object Identifier. MIB values can be either read-only or read-write.

## IP Address Assignment

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch’s default IP address is 10.90.90.90. You can change the default Switch IP address to meet the specification of your networking address scheme.

The Switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found from the initial boot console screen – shown below.



**Figure 2-8. Boot screen**

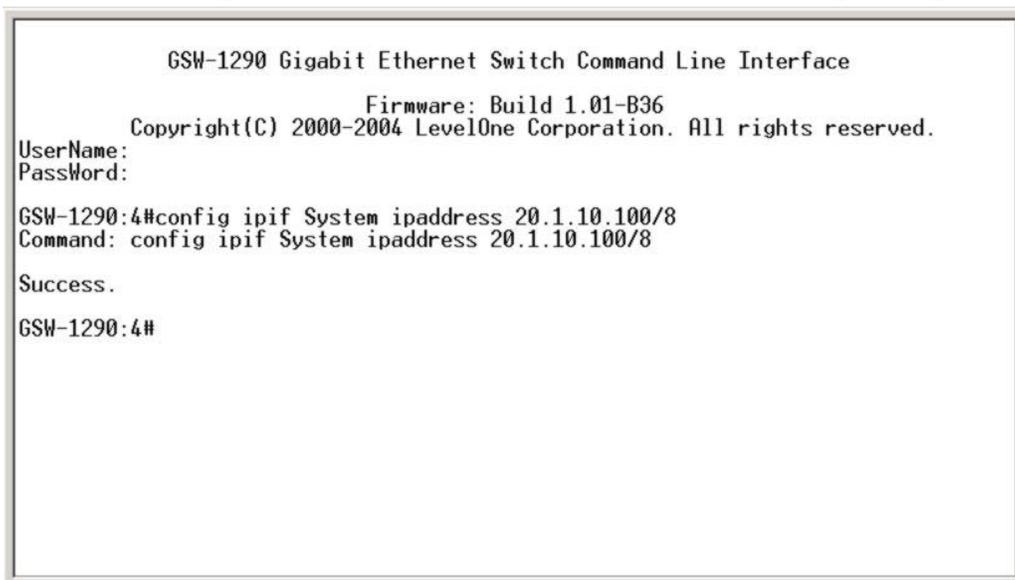
The Switch’s MAC address can also be found from the Web management program on the Switch Information (Basic Settings) window on the Configuration menu.

The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known.

The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows: Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**’s represent the IP address to be assigned to the IP interface named **System** and the **y**’s represent the corresponding subnet mask.

Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the **x**’s represent the IP address to be assigned to the IP interface named **System** and the **z** represents the corresponding number of subnets in CIDR notation.

The IP interface named System on the Switch can be assigned an IP address and subnet mask that can then be used to connect a management station to the Switch’s Telnet or Web-based management agent.



### **Figure 2-9. Assigning the Switch an IP Address**

In the above example, the Switch was assigned an IP address of 20.1.10.100 with a subnet mask of 255.0.0.0. The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management.

## **Connecting Devices to the Switch**

After you assign IP addresses to the Switch, you can connect devices to the Switch.

To connect a device to an SFP transceiver port:

Use your cabling requirements to select an appropriate SFP transceiver type.

Insert the SFP transceiver (sold separately) into the SFP transceiver slot.

Use the appropriate network cabling to connect a device to the connectors on the SFP transceiver.



**NOTICE:** When the SFP transceiver acquires a link, the associated integrated 10/100/1000BASE-T port is disabled.

## Chapter 3

### Basic Switch Management

*Before You Start*

*Web-based User Interface*

*Basic Setup*

*Switch Information*

*Switch IP Settings*

*Security IP Management Stations*

*User Accounts Management*

*Saving Changes*

*Factory Reset*

*Restart System*

*Advanced Settings*

*Switch Stack Management*

All software function of the GSW-1290 can managed, configured and monitored via the embedded web-based (HTML) interface. The Switch can be managed from remote stations anywhere on the network through a standard browser such as Opera, Netscape Navigator/Communicator or Microsoft Internet Explorer. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

The web-based management module and the Console program (and Telnet) are different ways to access the same internal Switching software and configure it. Thus, all settings encountered in web-based management are the same as those found in the console program.

#### ***Before You Start***

The GSW-1290 Layer 2 Switch supports a wide array of functions and gives great flexibility and increased network performance.

This flexibility and rich feature set requires a bit of thought to create a deployment strategy that will maximize the potential of the GSW-1290 Layer 2 Switch. Please read the portions of this manual pertaining to the functions you wish to perform with the Switch.

## Web-based User Interface

The user interface provides access to various Switch configuration and management windows, allows you to view performance statistics, and permits you to graphically monitor the system status.

### Areas of the User Interface

The figure below shows the user interface. The user interface is divided into three distinct areas as described in the table below.

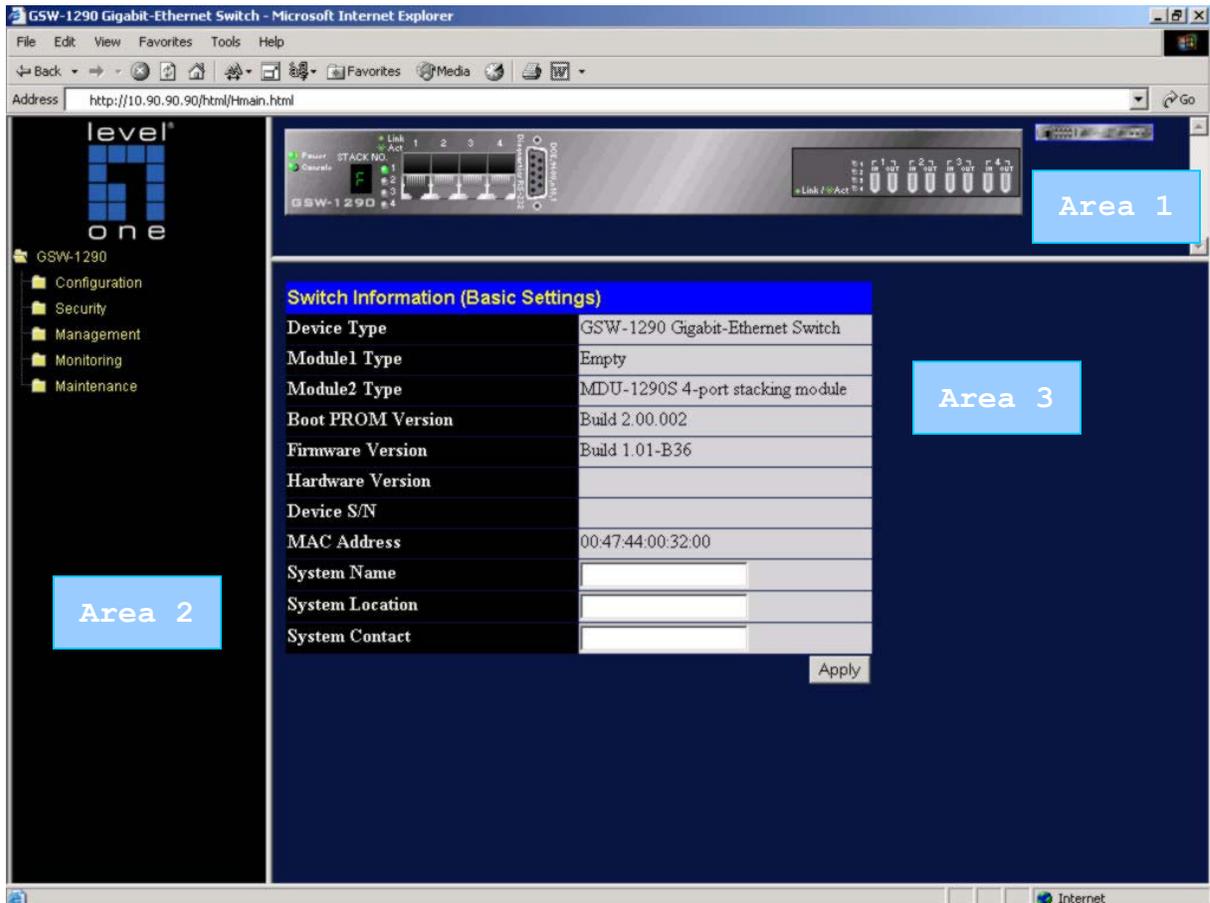
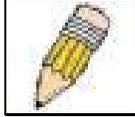


Figure 3-1. Main Web-Manager window

Area	Function
1	<p>Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports and expansion modules. When the Switch is stacked a virtual representation of the Switch stack appears in the right hand portion.</p> <p>Click on the ports in the front panel to manage the port's configuration or view data for the port.</p>
2	<p>Select the window to be displayed. The folder icons can be opened to display the hyperlinked window buttons and sub-folders contained within them.</p>
3	<p>Presents the information selected for configuration or display.</p>

## Login to Web Manager

To begin managing the Switch simply run the browser you have installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: `http://123.123.123.123`, where the numbers 123 represent the IP address of the Switch.



**NOTE:** The Factory default IP address for the Switch is 10.90.90.90.

In the Welcome page, click on the Login hyperlink; this opens a login dialog box. Enter a user name and password to access the Switch's management main page (pictured above). There is no user name or password configured for the Switch in the default settings, so if this is the first time logging in it is not necessary to enter these.



**NOTICE:** Any changes made to the Switch configuration during the current session must be saved in the **Save Configuration** window (explained below) or use the command line interface (CLI) command **save**.

## Web Pages and Folders

Below is a list and description of the main folders and windows available in the web interface:

**Configuration:** This folder includes all the sub-folders and windows used to configure various performance functions of the Switch.

**Security:** This folder contains the Port Access Entity (PAE) sub-folder used to configure 802.1x and RADIUS server settings. The Trusted Host window link is located here as well.

**Management:** The windows used to configure SNMP settings, management IP stations, and user accounts are located here.

**Monitoring:** Data tables for performance statistics, application and protocol status are contained in the links and subfolders of this folder.

**Maintenance:** Contains windows for upgrading firmware and saving configuration files (TFTP Services), saving configuration changes, resetting and rebooting the Switch, PING test, and logging out of the web manager.

**Single IP Management:** SIM settings, Topology, Firmware Update, and Configuration Backup/Restore windows are located here.



**NOTE:** Be sure to configure the user name and password in the User Accounts window before connecting the Switch to the greater network.

## Switch Information

The first page displayed upon logging in is the **System Information (Basic Settings)** window. This window can be accessed at any time by clicking the **Switch Information** button in the **Configuration** folder.

Switch Information (Basic Settings)	
Device Type	GSW-1290 Gigabit-Ethernet Switch
Module1 Type	Empty
Module2 Type	MDU-1290S 4-port stacking module
Boot PROM Version	Build 2.00.002
Firmware Version	Build 1.01-B36
Hardware Version	
Device S/N	
MAC Address	00:47:44:00:32:00
System Name	LevelOne Core Switch
System Location	BR-549
System Contact	Junior Samples
Apply	

Figure 3-2. Switch Information (Basic Settings) menu

This window displays general information about the Switch including its MAC Address, Hardware Boot PROM version and Firmware version, as well as installed module information.

## Switch IP Settings

Switch IP settings may initially be set using the console interface prior to connecting to it through the Ethernet. If the Switch IP address has not yet been changed, read the Introduction of the CLI Reference or skip ahead to the end of this section for a quick description of how to use the console port and CLI IP settings commands to establish IP settings for the Switch.

To change IP settings using the web manager you must access the **Switch IP Settings** window located in the **Configuration** folder.

To configure the Switch's IP address:

Open the **Configuration** folder and click the IP Address button. The web manager will display the **Switch IP Settings** window below.

Switch IP Settings	
Get IP From	Manual
IP Address	10.10.1.100
Subnet Mask	255.0.0.0
Default Gateway	10.20.1.100
VID	1
Apply	

Figure 3-3. Switch IP Settings menu



**NOTE:** The Switch's factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

**To manually assign the Switch’s IP address, subnet mask, and default gateway address:**

1. Select *Manual* from the Get IP From drop-down menu.
2. Enter the appropriate IP address and subnet mask.

If you want to access the Switch from a different subnet from the one it is installed on, enter the IP address of the gateway. If you will manage the Switch from the subnet on which it is installed, you can leave the default address (0.0.0.0) in this field.

If no VLANs have been previously configured on the Switch, you can use the default VLAN ID (VID) 1. The default VLAN contains all of the Switch ports as members. If VLANs have been previously configured on the Switch, you will need to enter the VLAN ID of the VLAN that contains the port connected to the management station that will access the Switch. The Switch will allow management access from stations with the same VID listed here.

**To use the BOOTP or DHCP protocols to assign the Switch an IP address, subnet mask, and default gateway address:**

Use the Get IP From pull-down menu to choose from *BOOTP* or *DHCP*. This selects how the Switch will be assigned an IP address on the next reboot.

The Switch IP Settings options are:

Parameter	Description
<b>BOOTP</b>	The Switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.
<b>DHCP</b>	The Switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the Switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.
<b>Manual</b>	Allows the entry of an IP address, Subnet Mask, and a Default Gateway for the Switch. These fields should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the network administrator. The fields which require entries under this option are as follows:
<b>Subnet Mask</b>	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
<b>Default Gateway</b>	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.
<b>VID</b>	This allows the entry of a VLAN ID from which a management station will be allowed to manage the Switch using TCP/IP (in-band via web manager or Telnet). Management stations that are on VLANs other than the one

entered in the VID field will not be able to manage the Switch in-band unless their IP addresses are entered in the Security IP Management menu. If VLANs have not yet been configured for the Switch, the default VID (1) contains all of the Switch's ports. There are no entries in the Security IP Management table, by default – so any management station that can connect to the Switch can access the Switch until either Management Station IP Addresses (see page 38) are assigned or SNMP settings are configured to control management.

### Setting the Switch's IP Address using the Console Interface

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 10.90.90.90. You can change the default Switch IP address to meet the specification of your networking address scheme.

The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known.

The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows: Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.

Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **z** represents the corresponding number of subnets in CIDR notation.

The IP interface named **System** on the Switch can be assigned an IP address and subnet mask that can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

### Security IP Management Stations Configuration

Use the **Security IP Management** window to define up to four community strings. Community strings are used to verify who can receive SNMP information from the Switch.

To access the **Security IP Management** window, click **Trusted Host** in the **Security** folder.



Figure 3-4. Security IP Management menu

Use the Management Station IP Settings to select up to three management stations used to manage the Switch. If you choose to define one or more designated management stations, only the chosen stations, as defined by IP address, will be allowed management privilege through the web manager or Telnet session.

To define a management station IP setting, type in the IP address in the area provided and then click the **Apply** button.

## User Account Management

Use the **User Account Management** to control user privileges. To view existing User Accounts, open the **Management** folder and click on the **User Accounts** link. This will open the **User Account Management** window.

User Account Management		
User Name	Access Right	Add
Bootsy	User	Modify
Clyde	User	Modify
FredWes	User	Modify
FunkyPres	Admin	Modify
JamesBrown	Admin	Modify
Maceo	User	Modify
PeeWee	User	Modify

Figure 3-5. User Account Management table

To add a new user, click on the **Add** button in the User Account Management Table. To modify or delete an existing user, click on the **Modify** button for that user.

User Account Modify Table	
User Name	BigMaceo
New Password	*****
Confirm New Password	*****
Access Right	Admin
	<div style="border: 1px solid black; padding: 2px;">                     Admin                      User                 </div>
<input type="button" value="Apply"/>	

Figure 3- 6. User Account Add menu

Add a new user by typing in a User Name, and New Password and retype the same password in the Confirm New Password. Choose the level of privilege (*Admin* or *User*) from the Access Right drop-down menu.

User Account Modify Table	
User Name	Bootsy
Old Password	*****
New Password	*****
Confirm New Password	*****
Access Right	User
<input type="button" value="Apply"/> <input type="button" value="Delete"/>	

Figure 3- 7. User Account Modify menu

Modify or delete an existing user account in the **User Account Modify Table** window. To delete the user account, click on the **Delete** button. To change the password, type in the New Password and retype it in the Confirm New Password entry field. Choose the level of privilege (*Admin* or *User*) from the Access Right drop-down menu.

### Admin and User Privileges

There are two levels of user privileges: *Admin* and *User*. Some menu selections available to users with *Admin* privileges may not be available to those with *User* privileges.

The following table summarizes the *Admin* and *User* privileges:

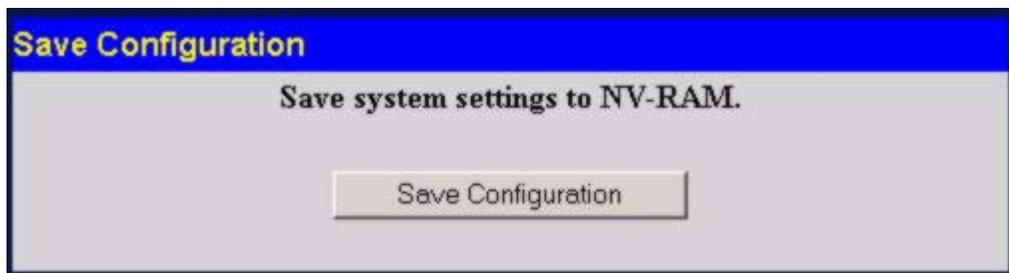
Management	Admin	User
<b>Configuration</b>	Yes	Read Only
<b>Network Monitoring</b>	Yes	Read Only
<b>Community Strings and Trap Stations</b>	Yes	Read Only
<b>Update Firmware and Configuration Files</b>	Yes	No
<b>System Utilities</b>	Yes	PING Only
<b>Factory Reset</b>	Yes	No
<b>User Account Management</b>		
<b>Add/Update/Delete User Accounts</b>	Yes	No
<b>View User Accounts</b>	Yes	No

**Table 3- 1. Admin and User Privileges**

After establishing a User Account with *Admin*-level privileges, be sure to save the changes (see below).

### Save Changes

Changes made to the Switch’s configuration must be saved in order to retain them. Access the **Save Configuration** window by clicking the **Save Changes** button located in the **Maintenance** folder.



**Figure 3- 8. Save Configuration menu**

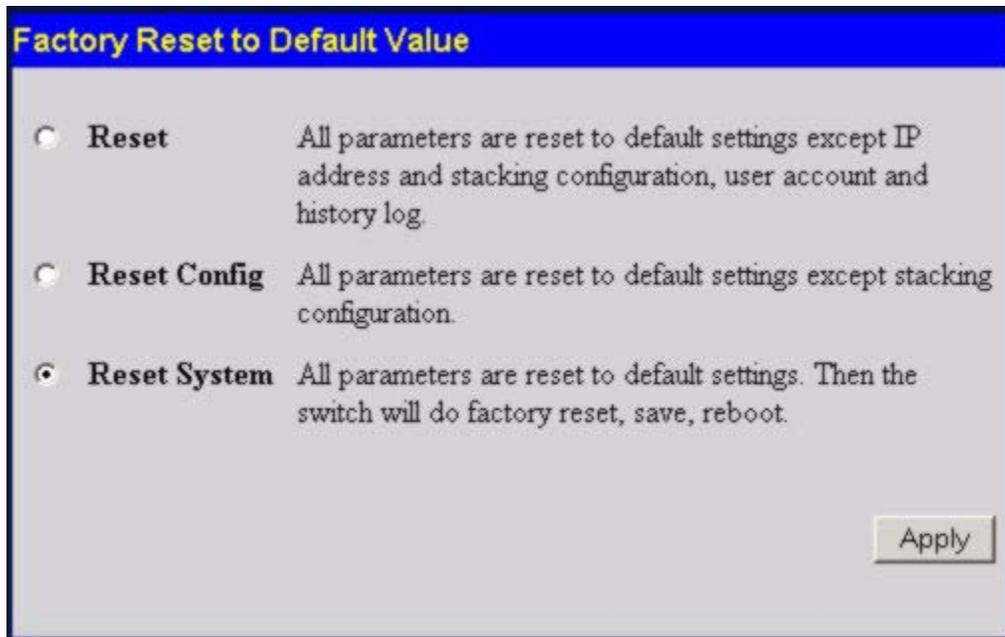
The Switch has two levels of memory, normal RAM and non-volatile or NV-RAM. To save all the changes made in the current session to the Switch’s flash memory, click the **Save Configuration** button. Click the **OK** button in the new dialog box that appears to continue. When this is done, the settings will be immediately applied to the Switching software in RAM, and will immediately take effect. Once the Switch

configuration settings have been saved to NV-RAM, they become the default settings for the Switch. These settings will be used every time the Switch is rebooted.

Some settings, though, require you to restart the Switch before they will take effect. Restarting the Switch erases all settings in RAM and reloads the stored settings from the NV-RAM. Thus, it is necessary to save all setting changes to NV-RAM before rebooting the Switch.

## Factory Reset

Click the **Factory Reset** link in the **Maintenance** folder to bring up the following window.



**Figure 3- 9. Factory Reset to Default Value menu**

The following options are available to perform a factory reset:

**Reset** – Returns all configuration settings to the factory default settings except the Switch’s stacking mode, IP address, subnet mask, and default gateway settings.

**Reset Config** – Returns all configuration settings to the factory default settings except the stacking mode configuration, but does not save the settings or reboot the Switch. If you select this option the Switch configuration will be returned to the factory default settings for the current session only. When the Switch is rebooted, it will return to the last configuration saved to the Switch’s NV-RAM using the Save Changes option.

- **Reset System** – Returns all configuration settings to the factory default settings, but does not save the settings or reboot the Switch. If you select this option the Switch configuration will be returned to the factory default settings and then saves the factory default configuration to the Switch’s NV-RAM. The Switch will then reboot. When the Switch has rebooted, it will have the same configuration as when it was delivered from the factory.

Select the reset option you want to perform and click on the **Apply** button.

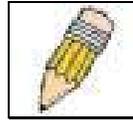
## Restart System

The following window is used to restart the Switch. Access this window by clicking on the **Restart System** link in the **Maintenance** folder.

Click the Yes after “Do you want to save the settings?” to instruct the Switch to save the current configuration to non-volatile RAM before restarting the Switch.

Clicking the No option instructs the Switch not to save the current configuration before restarting the Switch. All of the configuration information entered from the last time **Save Changes** was executed will be lost.

Click the **Restart** button to restart the Switch.



**NOTE:** Clicking Yes is equivalent to executing Save Changes and then restarting the Switch.

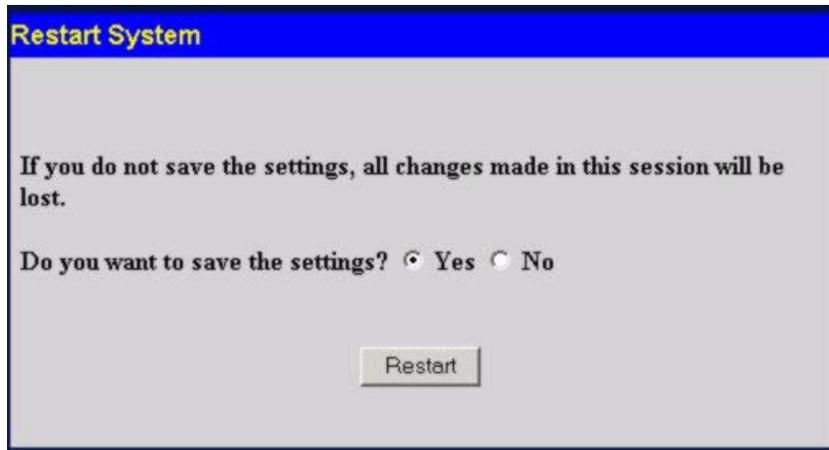


Figure 3- 10. Restart System menu

## Advanced Settings

Switch Information (Advanced Settings)	
Serial Port Auto Logout	10 Minutes ▾
Serial Port Baud Rate	9600 ▾
MAC Address Aging Time (10-1000000)	300
IGMP Snooping	Disabled ▾
Multicast router Only	Disabled ▾
Telnet Status	Enabled ▾
Web Status	Enabled ▾
RMON Status	Disabled ▾
GVRP	Disabled ▾
Link Aggregation Algorithm	MAC Source ▾
Switch 802.1x	Port Base ▾
<input type="button" value="Apply"/>	

Figure 3- 11. Switch Information (Advanced Settings) menu

The Advanced Settings options are summarized in the table below:

Parameter	Description
<b>Serial Port Auto Logout</b>	Select the logout time used for the console interface. This automatically logs the user out after an idle period of time as defined. Choose from the following options: <i>2 Minutes, 5 Minutes, 10 Minutes, 15 Minutes</i> or <i>Never</i> .
<b>Serial Port Baud Rate</b>	Select the baud rate used for the console interface. This automatically logs the user out after an idle period of time as defined. Choose from the following options: <i>9600, 19200, 38400</i> or <i>115200</i> .
<b>MAC Address Aging Time (10-1000000)</b>	This field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The default age-out time for the Switch is 300 seconds. To change this, type in a different value representing the MAC address age-out time in seconds. The Aging Time can be set to any value between <i>10</i> and <i>1,000,000</i> seconds.
<b>IGMP Snooping</b>	To enable system-wide IGMP Snooping capability select <i>Enabled</i> . IGMP snooping is <i>Disabled</i> by default. Enabling IGMP snooping allows you to specify use of a multicast router only (see below). To configure IGMP Snooping for individual VLANs, use the <b>IGMP Snooping</b> window in the <b>IGMP</b> folder.
<b>Multicast router Only</b>	If this option is enabled and IGMP Snooping is also enabled, the Switch forwards all multicast traffic to a multicast-enabled router only. Otherwise, the Switch will forward all multicast traffic to any IP router.
<b>Telnet Status</b>	Telnet configuration is <i>Enabled</i> by default. If you do not want to allow configuration of the system through Telnet choose <i>Disabled</i> .
<b>Telnet TCP Port Number(1-65535)</b>	The Telnet TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the Telnet protocol is 23.
<b>Web Status</b>	Web-based management is <i>Enabled</i> by default. If you choose to disable this by selecting <i>Disabled</i> , you will lose the ability to configure the system through the web interface as soon as these settings are applied.
<b>Web TCP Port Number(1-65535)</b>	The TCP port number currently being utilized by the Switch to connect to the web interface. The "well-known" TCP port for the Web interface is 80.
<b>RMON Status</b>	Remote monitoring (RMON) of the Switch is <i>Enabled</i> or <i>Disabled</i> here.
<b>GVRP</b>	Use this pull-down menu to enable or disable GVRP on the Switch.
<b>Link Aggregation Algorithm</b>	The algorithm that the Switch uses to balance the load across the ports that make up the port trunk group is defined by this definition. Choose <i>MAC Source, MAC Destination, MAC Src &amp; Dest, IP Source, IP Destination, and IP Src &amp; Dest</i> . (See Link Aggregation)
<b>Switch 802.1x</b>	Use this pull-down menu to enable or disable 802.1x functions on the Switch.
<b>Syslog state</b>	Use this pull-down menu to enable or disable Syslog.

### Stack Information

The GSW-1290 Switch can be used as a standalone high-capacity Switch or be used in a stacked arrangement. There are two hardware requirements to use the Switch in a stacked group:

1. The proper module(s) must be installed. One or two MDU-1290S Stacking modules must be installed in order to use the GSW-1290 Switch in a stacked configuration.
2. The Slave Switch units must be the GSW-2492 equipped with a Stacking module.
3. Two MDU-1290S Stacking modules can be installed on the GSW-1290 to allow up to eight GSW-2492 Switches to be stacked. The four built-in combination ports may also be used as stacking ports. Therefore it is possible to stack twelve GSW-2492 Switches with a GSW-1290.

The web manager can be used to enable or disable the stacking mode and to enable stacking for any of the built-in combination ports.

The Switch stack displayed in the upper right-hand corner of your web-browser is a virtual representation of the actual stack (see example below). The icons appear in the same order as their respective Switches.

When the Switches are properly interconnected, information about the resulting Switch stack is displayed in the **Stack Mode Setup** window. To view stacking information or to enable/disable the stacking mode, click the **Stack Information** link in the **Configuration** folder.



**Figure 3- 12. Stack Mode Setup (stacking disabled) window**

To enable the stacking mode, follow the steps listed below.

1. Select *Enabled* from the Stack Mode State drop-down menu.
2. Click on the **Apply** button.

To enable stacking for one or more built-in combination ports, do the following:

1. Select *Enabled* from the Stack Mode State drop-down menu.
2. Select the Stack Port by clicking to check a corresponding selection box.

The Stack Information Table displays the read-only information listed in the table on the next page.

The current order in the Switch stack is also displayed on the front panel of each slave Switch, under the STACK NO. heading. The Stack ID LED display on the front panel of the GSW-1290 will always display an F (15 in hex), regardless of whether the GSW-1290 is the master Switch in a Switch stack or in standalone mode.

Below is an example of the **Stack Mode Setup** window with stacking mode enabled on Ports 5-8.

The screenshot shows the 'Stack Mode Setup' window. It includes the following fields and options:

- Stack Topology:** Auto Detect
- Setting:** MASTER
- Current:** MASTER
- Stack Mode State:** Enable (dropdown menu)
- Stack Port:** A row of 12 checkboxes for ports 1 through 12. Ports 5, 6, 7, and 8 are checked.
- Apply:** Button
- Total Entries:** 2
- Stack Information Table:**

ID	MAC Address	Port Range	Mode	Version	Model Name
15	00-0d-88-00-00-00	1-12	MASTER	1.01-B36	GSW-1290
5	00-80-33-26-07-00	251-300	AUTO	4.01-B36	GSW-2492

**Figure 3- 13. Stack Mode Setup menu and Information table (stacking enabled)**

Variables in this window are described below:

Parameter	Description
<b>ID</b>	Displays the Switch's order in the stack. The Switch with a unit id of 1 is the master Switch.
<b>MAC Address</b>	Displays the unique address of the Switch assigned by the factory.
<b>Port Range</b>	Displays the total number of ports on the Switch. Note that the stacking port is included in the total count.
<b>Mode</b>	Displays the method used to determine the stacking order of the Switches in the Switch stack.
<b>Version</b>	Displays the version number of the stacking firmware.
<b>Model Name</b>	Displays the model name of the corresponding Switch in a stack.

When the stacked group is connected and properly configured, the virtual stack appears in the upper right-hand corner of the web page. Click on any unit in the virtual stack to see the real time display of the front panel of that unit.

The screenshot displays the LevelOne web interface for a GSW-1290 switch. On the left is a navigation menu with categories like Configuration, Security, and Management. The main content area is titled 'Stack Information' and contains the following sections:

**Stack Mode Setup**

- Stack Topology: Auto Detect
- Setting: MASTER
- Current: MASTER
- Stack Mode State: Enable
- Stack Port: A row of 12 checkboxes, all of which are checked.

**Stack Information Table**

ID	MAC Address	Port Range	Mode	Version	Model Name
15	00-0d-88-00-00-00	1-12	MASTER	1.01-B36	GSW-1290
5	00-80-33-26-07-00	251-300	AUTO	4.01-B36	GSW-2492

A red circle in the top right corner highlights a virtual stack icon, which is a small representation of the physical switch units stacked together.

Figure 3- 14. Stack Information web page

## Chapter 4

# System Configuration

- Port Configuration*
- Port Mirroring*
- Link Aggregation*
- LACP Port Settings*
- IGMP*
- IGMP Snooping*
- Static Router Ports Entry*
- Spanning Tree*
- STP Switch Settings*
- STP Port Settings*
- Forwarding & Filtering*
- Unicast Forwarding*
- Multicast Forwarding*
- Multicast Port Filtering Mode*
- VLANs*
- Static VLAN Entry*
- GVRP Setting*
- QoS*
- 802.1p Default Priority*
- 802.1p User Priority*
- QoS Output Scheduling*
- Traffic Segmentation*
- Bandwidth Control*
- MAC Notification*
- Global Settings*
- Port Settings*
- System Log Server*
- Port Security*
- SNTP Setting*
- Time Setting*
- Time Zone and DST*
- Access Profile Table*

The GSW-1290's Web interface is divided into six main folders: **Configuration**, **Security**, **Management**, **Monitoring**, **Maintenance**, and **Single IP Management**. This chapter describes all of the **Configuration** sub-folders and windows.

## Port Configuration

To configure basic port settings such as port speed, duplex, and learning state, use the **Port Configuration** window.

Click the Port Configuration link in the Configuration folder:

The screenshot shows the 'Port Configuration' window. At the top, there is a configuration form with the following fields: Unit (15), From (Port 1), To (Port 1), State (Disabled), Speed/Duplex (Auto), Flow Control (Disabled), Learning (Disabled), and an Apply button. Below the form is a table titled 'The Port Information Table' with the following data:

Port	State	Speed/Duplex	Flow Control	Connection	Learning
1	Enabled	Auto	Disabled	100M/Full/None	Enabled
2	Enabled	Auto	Disabled	Link Down	Enabled
3	Enabled	Auto	Disabled	Link Down	Enabled
4	Enabled	Auto	Disabled	Link Down	Enabled
5	Enabled	Auto	Disabled	Empty	Enabled
6	Enabled	Auto	Disabled	Empty	Enabled
7	Enabled	Auto	Disabled	Empty	Enabled
8	Enabled	Auto	Disabled	Empty	Enabled
9	Enabled	1000M/Full	Disabled	Link Down	Enabled
10	Enabled	1000M/Full	Disabled	Link Down	Enabled
11	Enabled	1000M/Full	Disabled	Link Down	Enabled
12	Enabled	1000M/Full	Disabled	Link Down	Enabled

Figure 4- 1. Port Configuration and Information table

To configure Switch ports:

1. Choose the **Unit** from the pull-down menu.
2. Choose the port or sequential range of ports using the **From...To...** port pull-down menus.
3. Use the remaining pull-down menus to configure the parameters described in the table below.

The configurable parameters for ports include the following:

Parameter	Description
-----------	-------------

**State** <Enabled> Toggle the State field to either enable or disable a given port.

**Speed/Duplex** <Auto> Toggle the Speed/Duplex field to either select the speed and duplex/half-duplex state of the port. *Auto* – auto-negotiation between 10 and 100 Mbps devices, full- or half-duplex. The Auto setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are *1000M/Full*, *1000M/Half*, *100M/Full*, *100M/Half*, *10M/Full*, and *10M/Half*. There is no automatic adjustment of port settings with any option other than *Auto*.

**Flow Control** Displays the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and Auto ports use an automatic selection of the two. The default is *Disabled*.

**Learning** Enable or disable MAC address learning for the selected ports. When *Enabled*, destination and source MAC addresses are automatically

listed in the forwarding table. When learning is *Disabled*, MAC addresses must be manually entered into the forwarding table. This is sometimes done for reasons of security or efficiency.

## Port Mirroring

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. Follow the steps below to set up port mirroring.

**Setup Port Mirroring**

Target Port Unit: 15 Port: Port 1

Status: Disabled

Source Unit: 15

Source Port	1	2	3	4	5	6	7	8	9	10	11	12
None	<input type="radio"/>											
Ingress	<input type="radio"/>											
Egress	<input type="radio"/>											
Both	<input type="radio"/>											

Apply

Note(1): The "Source Port" and "Target Port" should be different, or the setup will be invalid.

Note(2): The target port should be a non-trunked port.

The Trunking Ports: None

Figure 4- 2. Setup Port Mirroring menu

To configure a mirror port:

Select the Source Unit containing the port that is being mirrored.

Configure how the port is to be mirrored by selecting the direction that will be mirrored. Choose Ingress, Egress, or Both for the mirrored port by clicking the appropriate radio button for the port.

Select the Target Port using the Unit and Port drop-down menus.

Change the Status drop-down menu to *Enabled*.

Click **Apply** to let the changes take effect.



**NOTE:** You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port for the mirroring cannot be a member of a trunk group. Please note a target port and a source port cannot be the same port.

## Traffic Control

Use the **Traffic Control Setting** window to enable or disable storm control and adjust the threshold for multicast and broadcast storms, as well as DLF (Destination Look Up Failure). Traffic control settings are applied to individual Switch modules. The Traffic Control Setting menu is located in the QoS directory. Open the QoS folder in the Configuration folder and click the Traffic Control link.

**Traffic Control Setting**

Unit	Group	Broadcast Storm	Multicast Storm	Destination Lookup Fail	Threshold	Apply
15	1	Disabled	Enabled	Enabled	128	Apply

**Traffic Control Information Table**

Group[ports]	Broadcast Storm	Multicast Storm	Destination Lookup Fail	Threshold
1[1]	Disabled	Disabled	Disabled	128
2[2]	Disabled	Disabled	Disabled	128
3[3]	Disabled	Disabled	Disabled	128
4[4]	Disabled	Disabled	Disabled	128
5[5]	Disabled	Disabled	Disabled	128
6[6]	Disabled	Disabled	Disabled	128
7[7]	Disabled	Disabled	Disabled	128
8[8]	Disabled	Disabled	Disabled	128
9[9]	Disabled	Disabled	Disabled	128
10[10]	Disabled	Disabled	Disabled	128
11[11]	Disabled	Disabled	Disabled	128
12[12]	Disabled	Disabled	Disabled	128

**Figure 4- 3. Traffic Control Setting menu and Information table**

Traffic or storm control is used to stop broadcast, multicast or ARP request storms that may result when a loop is created. The Destination Look Up Failure control is a method of shutting down a loop when a storm is formed because a MAC address cannot be located in the Switch’s forwarding database and it must send a packet to all ports or all ports on a VLAN.

To configure Traffic Control, select the Unit (Unit ID of a Switch in a Switch stack – 15 for a Switch in standalone mode) you want to configure. Broadcast Storm, Multicast Storm and Destination Look Up Failure may be *Enabled* or *Disabled*. The Threshold value is the upper threshold at which the specified traffic control is switched on. This is the number of Broadcast, Multicast or DLF packets, in Kbps, received by the Switch that will trigger the storm traffic control measures. The Threshold value can be set from 0 to 255 packets. The Default setting is 128.

## Link Aggregation

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link a bandwidth intensive network device or devices – such as a server – to the backbone of a network.

The Switch allows the creation of up to six link aggregation groups, each group consisting of up to eight links (ports). The aggregated links must be contiguous (they must have sequential port numbers) except the two (optional) Gigabit ports – which can only belong to a single link aggregation group. A link aggregation group may not cross an 8-port boundary, starting with port 1 (a group may not contain ports 8 and 9, for example) and all of the ports in the group must be members of the same VLAN. Further, the aggregated links must all be of the same speed and should be configured as full duplex.

The configuration of the lowest numbered port in the group becomes the configuration for all of the ports in the aggregation group. This port is called the Master Port of the group, and all configuration options – including the VLAN configuration – that can be applied to the Master Port are applied to the entire link aggregation group.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link, on the Switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group – in the same way STP will block a single port that has a redundant link.

To configure port trunking, click on the **LACP** hyperlink in the **Configuration** folder and then click **Link Aggregation**:

Port Trunking Group			
Add New Trunking Group			Add
Current Trunking Group Entries			
Group ID	Group name	Modify	Delete
1	rLAN	Modify	×
2	local	Modify	×

Figure 4- 4. Port Trunking Group table

To configure port trunk groups, click the **Add** button to add a new trunk group and then use the **Port Trunking Configuration** window below to set up trunk groups. To change or delete a port trunk group, click the **Modify** or **Delete** option in the Current Trunking Group Entries table pictured above.

Figure 4- 5. Port Trunking Configuration menu

The user-changeable parameters are as follows:

Parameter	Description
<b>Group ID</b>	Select an ID number for the group.
<b>State</b>	Trunk groups can be toggled between <i>Enabled</i> and <i>Disabled</i> . This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.
<b>Type</b>	This pull-down menu allows you to select between <i>Static</i> and <i>LACP</i> (Link Aggregation Control Protocol.) LACP allows for the automatic detection of links in a Port Trunking Group.
<b>Master Port</b>	Choose the Master port for the trunk group.
<b>Member Unit</b>	Choose the Switch unit on which to set up a trunk group. Trunk groups must be confined to ports on a single Switch.
<b>Port Map</b>	Choose the members of the trunked group. Up to eight ports per group can be assigned to a group.
<b>Flooding Port</b>	A trunking group must designate one port to allow transmission of broadcasts and unknown unicasts.
<b>Active Port</b>	Shows the port that is currently forwarding packets.

## LACP Port Settings

The **LACP Port Mode Setup** window is used in conjunction with the Link Aggregation window to create port trunking groups on the Switch. Using the following window, the user may set which ports will be active and passive in processing and sending LACP control frames.

The screenshot shows the 'LACP Port Mode Setup' window. At the top, there is a title bar. Below it, there are four dropdown menus: 'Unit' (set to 15), 'From' (set to Port 1), 'To' (set to Port 1), and 'Mode' (set to Active). To the right of these is an 'Apply' button. Below the configuration fields is a table titled 'LACP Port Mode Table' with two columns: 'Port' and 'Mode'. The table lists ports 1 through 12 with their respective modes: ports 1 and 2 are Active, and ports 3 through 12 are Passive.

Unit	From	To	Mode	Apply
15	Port 1	Port 1	Active	Apply

Port	Mode
1	Active
2	Active
3	Passive
4	Passive
5	Passive
6	Passive
7	Passive
8	Passive
9	Passive
10	Passive
11	Passive
12	Passive

Figure 4- 6. LACP Port Mode Setup and Table

The user may set the following parameters:

Parameter	Description
<b>Unit</b>	This is the Unit ID of a Switch in a Switch stack. The number 15 indicates a GSW-1290 Switch in standalone mode.
<b>From/To</b>	A consecutive group of ports may be configured starting with the selected port.
<b>Mode</b>	<p><i>Active</i> – Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.</p> <p><i>Passive</i> – LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, at one end of the</p>

connection must have “active” LACP ports.

---

After setting the previous parameters, click **Apply** to allow your changes to be implemented. The LACP Port Table shows which ports are active and/or passive.

## IGMP

In order to use IGMP Snooping it must first be enabled for the entire Switch (see **Advanced Settings**). You may then fine-tune the settings for each VLAN using the **IGMP Snooping Settings** window. When enabled for IGMP snooping, the Switch can open or close a port to a specific Multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

### IGMP Snooping

Use this window to view IGMP Snooping status. To modify settings, click the **Modify** button for the VLAN ID you want to change.



VLAN ID	VLAN Name	State	Querier State	Modify
1	default	Disabled	Disabled	Modify
2	rLAN	Disabled	Disabled	Modify
3	5th_floor	Disabled	Disabled	Modify

**Figure 4- 7. Current IGMP Snooping Group Entries table**

Click the **Modify** button to bring up the **IGMP Snooping Settings** window pictured below.

IGMP Snooping Settings	
VLAN ID	2
VLAN Name	rLAN
Query Interval	125
Max Response Time	10
Robustness Value	2
Last Member Query Interval	1
Host Timeout	260
Route Timeout	260
Leave Timer	2
Querier State	Disabled
State	Disabled

Apply

[Show All IGMP Group Entries](#)

Figure 4- 8. IGMP Snooping Settings menu

The IGMP Snooping Settings are described below:

Parameter	Description
<b>VLAN ID</b>	The VLAN ID number.
<b>VLAN Name</b>	The VLAN name.
<b>Query Interval</b>	The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between 1 and 9,999 seconds are allowed. The default value is 125.
<b>Max Response Time</b>	This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The Max Response Time field allows an entry between 1 and 25 (seconds). The default value is 10.
<b>Robustness Variable</b>	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of 2 to 255. The default value is 2.
<b>Last Member Query Interval</b>	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. The default value is 1.

<b>Host Timeout</b>	This is the maximum amount of time in seconds allowed for a host to continue membership in a multicast group without the Switch receiving a host membership report. The default value is 260.
<b>Route Timeout</b>	This is the maximum amount of time in seconds a route is kept in the forwarding table without receiving a membership report. The default value is 260.
<b>Leave Timer</b>	This specifies the maximum amount of time in seconds between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. If no response to the membership query is received before the Leave Timer expires, the (multicast) forwarding entry for that host is deleted.
<b>Querier State</b>	Choose <i>Enabled</i> to enable transmitting IGMP Query packets. The default value is <i>Disabled</i> .
<b>State</b>	Select <i>Enabled</i> to implement IGMP Snooping. This is <i>Disabled</i> by default.

### Static Router Ports Entry

A static router port is a port that has a multicast router attached to it. Generally, this router would have a connection to a WAN or to the Internet. Establishing a router port will allow multicast packets coming from the router to be propagated through the network, as well as allowing multicast messages (IGMP) coming from the network to be propagated to the router.

A router port has the following behavior characteristics:

- All IGMP Report packets will be forwarded to the router port.
- IGMP queries (from the router port) will be flooded to all ports.

All UDP multicast packets will be forwarded to the router port. Because routers do not send IGMP reports or implement IGMP snooping, a multicast router connected to the router port of the Layer 3 Switch would not be able to receive UDP data streams unless the UDP multicast packets were all forwarded to the router port.

A router port will be dynamically configured when IGMP query packets, RIPv2 multicast, DVMRP multicast, and PIM-DM multicast packets are detected flowing into a port.

Open the **IGMP** folder and the click on the **Static Router Ports Entry** link to open the **Current Static Router Ports Entries** window, as shown below.

Current Static Router Ports Entries		
VLAN ID	VLAN Name	Modify
1	default	Modify
2	rLAN	Modify
3	5th_floor	Modify

**Figure 4- 9. Current Static Router Port Entries table**

The window displays all of the current entries to the Switch’s static router port table. To add or modify an entry, click the Modify button. This will open the Static Router Ports Settings window, as shown below.

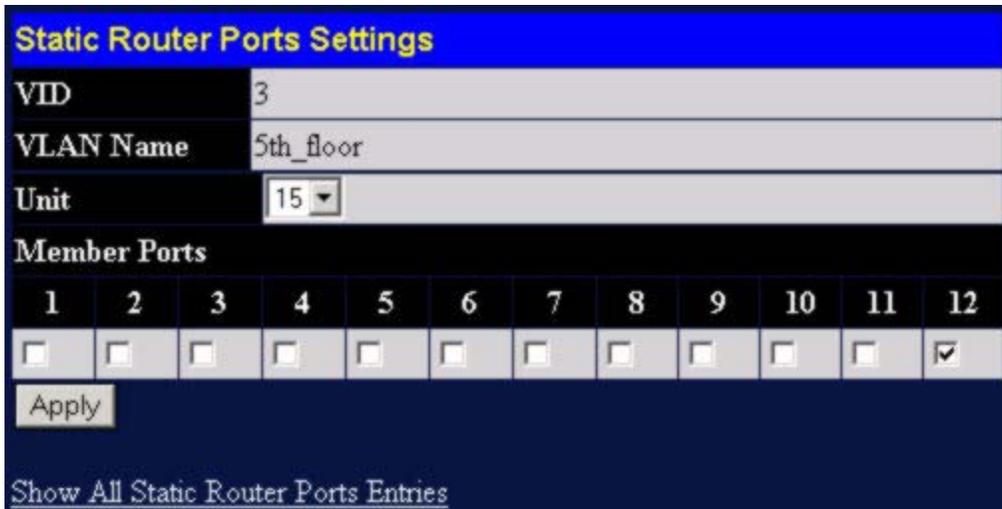


Figure 4- 10. Static Router Ports Settings menu

To configure a static router port(s):

1. Select the Unit containing the static router port.
2. Select the Port or Ports that will become static router ports.
3. Click **Apply** to let the changes take effect.

The following parameters are listed in the Static Router Port windows.

Parameter	Description
<b>VLAN ID (VID)</b>	This is the VLAN ID that, along with the VLAN name, identifies the VLAN where the multicast router is attached.
<b>VLAN Name</b>	This is the name of the VLAN where the multicast router is attached.
<b>Unit</b>	This is the Unit ID of the Switch in a Switch stack for which you are creating an entry into the Switch's static router port table.
<b>Member Ports</b>	There are the ports on the Switch that will have a multicast router attached to them.

## Spanning Tree

The Switch supports 802.1d Spanning Tree Protocol (STP) and 802.1w Rapid Spanning Tree Protocol (RSTP). 802.1d STP will be familiar to most networking professionals. However since 802.1w RSTP has been recently introduced to LevelOne managed Ethernet Switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1 d STP and 802.1w RSTP.

### 802.1w Rapid Spanning Tree

The Switch implements two versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEE 802.1w specification and a version compatible with the IEEE 802.1d STP. RSTP can operate with legacy equipment implementing IEEE 802.1d, however the advantages of using RSTP will be lost.

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1d STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent Switching innovations, in particular, certain Layer 3 function that are increasingly handled by Ethernet Switches. The basic function and much of the terminology is the same as STP. Most of the settings

configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

### Port Transition States

An essential difference between the two protocols is in the way ports transition to a forwarding state and the in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. RSTP combines the transition states disabled, blocking and listening used in 802.1d and creates a single state *Discarding*. In either case, ports do not forward packets; in the STP port transition states disabled, blocking or listening or in the RSTP port state discarding there is no functional difference, the port is not active in the network topology. The Comparing Port States table below compares how the two protocols differ regarding the port state transition.

Both protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently – with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, all links between bridges are sensitive to the status of the link. Ultimately this difference results faster detection of failed links, and thus faster topology adjustment. A drawback of 802.1d is this absence of immediate feedback from adjacent bridges.

802.1d STP	802.1w RSTP	Forwarding?	Learning?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	No	No
Learning	Learning	No	Yes
<i>Forwarding</i>	<i>Forwarding</i>	Yes	Yes

**Table 4- 1. Comparing Port States**

RSTP is capable of more rapid transition to a forwarding state – it no longer relies on timer configurations – RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

#### Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports will transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

#### P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

### 802.1d/802.1w Compatibility

RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1d format when necessary. However, any segment using 802.1 STP will not benefit from the rapid transition and rapid topology change detection of RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP.

### Switch Spanning Tree Settings

The Spanning Tree Protocol (STP) operates on two levels: on the Switch level, the settings are globally implemented. On the port level, the settings are implemented on a per user-defined group of ports basis.

Switch Spanning Tree Settings	
Spanning Tree Status	Disabled ▾
Bridge Max Age (6-40 Sec)	20
Bridge Hello Time (1-10 Sec)	2
Bridge Forward Delay (4-30 Sec)	15
Bridge Priority (0-61440)	32768
STP Version	rstp ▾
TX Hold Count(1-10)	3
Forwarding BPDU	Enabled ▾
Apply	
Designated Root Bridge	--
Root Priority	--
Cost to Root	--
Root Port	--
Time Topology Change(secs)	--
Topology Changes Count	--
Protocol Specification	--
Max Age	--
Hello Time	--
Forward Delay	--
Hold Time	--
<p><i>Note: 2*(Forward Delay-1) &gt;= Max Age, Max Age &gt;= 2*(Hello Time +1)</i></p>	

Figure 4- 11. Switch Spanning Tree Settings menu

Configure the following system-wide STP parameters and click the **Apply** button to implement them:

Parameter	Description
<b>Spanning Tree Status</b> <Disabled>	This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. This will enable or disable the Spanning Tree Protocol (STP), globally, for the Switch.
<b>Bridge Max Age (6 - 40 sec)</b> <20 >	The Max. Age can be set from 6 to 40 seconds. At the end of the Max. Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.
<b>Bridge Hello Time (1 - 10 sec)</b> < 2 >	The Hello Time can be set from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge.
<b>Bridge Forward Delay (4 - 30 sec)</b> <15 >	The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.
<b>Bridge Priority (0 - 61440)</b> <32768>	A Priority for the Switch can be set from 0 to 61440. This number is used in the voting process between Switches on the network to determine which Switch will be the root Switch. A low number indicates a high priority, and a high probability that this Switch will be elected as the root Switch.
<b>STP Version</b> <rstp >	Choose <i>rstp</i> (default) or <i>Stp Compatibility</i> . Both versions use STP parameters in the same way. RSTP is fully compatible with IEEE 802.1d STP and will function with legacy equipment.
<b>Tx Hold Count(1-10)</b> <3 >	This is the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. The default value is 3.
<b>Forwarding BPDU</b> <Enabled >	This can be <i>Enabled</i> or <i>Disabled</i> . When it is <i>Enabled</i> it allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is <i>Enabled</i> .



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

Observe the following formulas when setting the above parameters:

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

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

## STP Port Settings

**STP Port Settings**

Unit: 15 From: Port 3 To: Port 3 State: Enabled Cost: 0 Priority: 0 MigrationEdge: Yes P2P: No Apply

**The STP Port Information**

Port	Designated Bridge	State	Cost	Priority	Edge	P2P	STP Status	Role
1 A	N/A	Yes	*20000	128	No	Yes	Disabled	Disabled
2 M	N/A	Yes	*20000	128	No	Yes	Disabled	Disabled
3	8000/0050ba7120d6	Yes	*200000	128	No	Yes	Forwarding	Root
4	N/A	Yes	*20000	128	No	Yes	Disabled	Disabled
5	N/A	Yes	*20000	128	No	Yes	Disabled	Disabled
6	N/A	Yes	*20000	128	No	Yes	Disabled	Disabled
7	N/A	Yes	*20000	128	No	Yes	Disabled	Disabled
8	N/A	Yes	*20000	128	No	Yes	Disabled	Disabled
9	N/A	Yes	*20000	128	No	Yes	Disabled	Disabled
10	N/A	Yes	*20000	128	No	Yes	Disabled	Disabled
11	N/A	Yes	*20000	128	No	Yes	Disabled	Disabled
12	N/A	Yes	*20000	128	No	Yes	Disabled	Disabled

Figure 4- 12. STP Port Settings and Information menu

In addition to setting Spanning Tree parameters for use on the Switch level, the Switch allows for the configuration of groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings. An STP Group will use the Switch-level parameters entered above, with the addition of Port Priority and Port Cost.

An STP Group spanning tree works in the same way as the Switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected on the basis of port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the Switch level.

The STP on the Switch level blocks redundant links between Switches (and similar network devices). The port level STP will block redundant links within an STP Group.

It is advisable to define an STP Group to correspond to a VLAN group of ports.

The following fields can be set for STP port configuration:

Parameter	Description
<b>Unit</b>	This is the Unit ID of a Switch in a Switch stack. The number 15 indicates a GSW-1290 Switch in standalone mode.
<b>From/To</b>	A consecutive group of ports may be configured starting with the selected port.
<b>State</b>	This drop-down menu allows you to enable or disable STP for the selected group of ports.
<b>Cost</b>	A Port Cost can be set from 1 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets. Default port cost: 100Mbps port = 200000 Gigabit ports = 20000
<b>Priority</b>	A Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port.
<b>Migration</b>	Select Yes or No. Choosing Yes will enable the port to migrate from 802.1d STP status to 802.1w RSTP status. RSTP can coexist with standard STP, however the benefits of RSTP are not realized on a port where an 802.1d network connects to an 802.1w enabled network. Migration should be enabled (Yes) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment.
<b>Edge</b>	Select Yes or No. Choosing Yes designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. No indicates the port does not have edge port status.
<b>P2P</b>	Select Yes or No. Choosing Yes indicates a point-to-point (p2p) shared link. These are similar to edge ports however they are restricted in that a p2p port must operate in full duplex. Like edge ports, p2p ports transition to a forwarding state rapidly thus benefiting from RSTP.

---

## Forwarding & Filtering

The Switch allows permanent or static entries into the forwarding database (FDB). These FDB entries are MAC addresses that will not age out. In addition, multicast forwarding may be customized to conform to rules for the different ports by setting up multicast filter modes for each port.

### Unicast Forwarding

Open the **Forwarding & Filtering** folder and click on the **Unicast Forwarding** link. This will open the **Setup Static Unicast Forwarding Table** window, as shown below.

VLAN ID	MAC Address	Allowed to Go Unit	Port
1	00:00:00:00:00:03	15	Port 3

Add/Modify

Mac Address	VID	VLAN Name	Unit	Port	Delete
00:00:00:00:00:00	1	default	15	3	X
00:00:00:00:00:01	1	default	15	3	X
00:00:00:00:00:03	1	default	15	3	X

End of data!

Figure 4- 13. Setup Static Unicast Forwarding Setup and table

To add an entry, define the following parameters:

Parameter	Description
<b>VLAN ID</b>	The VLAN ID number of the VLAN on which the above Unicast MAC address resides.
<b>MAC Address</b>	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
<b>Allowed to Go to Unit</b>	Allows the designation of the module on which the above MAC address resides.
<b>Port</b>	Choose the port on which the MAC address resides. Selecting Port 0 means no ports are allowed.

Click on the **Add/Modify** button to add a unicast MAC address to the Switch's forwarding table, or to modify a previous entry.

## Multicast Forwarding

The following window describes how to set up Multicast forwarding on the Switch. Open the **Forwarding & Filtering** folder and click on the **Multicast Forwarding** link to see the entry window below:

Unit	VID	Multicast MAC Address											
15	2	00-00-00-00-00-01											
Port Settings		1	2	3	4	5	6	7	8	9	10	11	12
None		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress		<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>								

[Show All Multicast Forwarding Entries](#)

Figure 4- 14. Static Multicast Forwarding Settings menu

The **Static Multicast Forwarding Settings** window displays all of the entries made into the Switch’s static multicast forwarding table. Click the **Add** button to open the **Setup Static Multicast Forwarding Table** window, as shown below.

VLAN ID	MAC Address	Type	Modify	Delete
2	11:11:00:00:00:00	Static	<input type="button" value="Modify"/>	<input type="button" value="X"/>

Figure 4- 15. Setup Static Multicast Forwarding table

The following parameters can be set:

Parameter	Description
<b>Unit</b>	This is the Unit ID of a Switch in a Switch stack. The number 15 indicates a GSW-1290 Switch in standalone mode.
<b>VID</b>	The VLAN ID of the VLAN the MAC address below belongs to.
<b>Multicast MAC Address</b>	The MAC address of the static source of multicast packets. This must be a multicast MAC address.
<b>Port Settings</b>	Allows the selection of ports that will be members of the static multicast group and ports that are either forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. The options are

None and Egress. None means there are no restrictions on the port dynamically joining the multicast group. If None is chosen, then an end station attached to the port can join the multicast group using GMRP. Egress means the port is a static member of the multicast group.

### Multicast Port Filtering Mode

The following window describes how to set up Multicast port filtering on the Switch. Open the **Forwarding & Filtering** folder and click on the **Multicast Port Filtering Mode** link to see the entry window below:

**Multicast Port Filtering Mode Setup**

Unit	From	To	Mode	Apply
15	Port 1	Port 1	Forward All Groups	Apply

**Multicast Port Filtering Mode Table**

Port	Mode
1	Forward All Groups
2	Forward All Groups
3	Forward Unregistered Groups
4	Forward Unregistered Groups
5	Forward Unregistered Groups
6	Forward Unregistered Groups
7	Forward Unregistered Groups
8	Forward Unregistered Groups
9	Forward Unregistered Groups
10	Forward Unregistered Groups
11	Forward Unregistered Groups
12	Filter Unregistered Groups

**Figure 4- 16. Multicast Port Filtering Mode Setup and table**

The following parameters can be set:

Parameter	Description
<b>Unit</b>	This is the Unit ID of a Switch in a Switch stack. The number 15 indicates a GSW-1290 Switch in standalone mode.
<b>From/To</b>	A consecutive group of ports may be configured starting with the selected port.
<b>Mode</b>	This drop-down menu allows you to select the action the switch will take when it receives a multicast packet that is to be forwarded to one of the ports in the range specified above.  <i>Forward All Groups</i> – Instructs the switch to forward a multicast packet to

all multicast groups residing within the range of ports specified above.

*Forward Unregistered Groups* – Instructs the switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above.

*Filter Unregistered Groups* – Instructs the switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above

---

## VLANs

The Switch Web Manager's VLANs sub-folder is divided into two main windows, **802.1Q Static VLANs** and **802.1Q Port Settings**. Each is described after a short overview of VLANs.

### Understanding 802.1Q VLANs

This review of 802.1Q VLANs presents some basic background about how VLANs work according to the IEEE 802.1Q standard. VLANs operate according to the same rules regardless of whether the Switching environment is Layer 2 or Layer 3. The difference is primarily that in a Layer 3 Switch there is an added capability of unique association between a VLAN and an IP interface or subnet group.

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

### IEEE 802.1Q VLANs

Some relevant terms:

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

Untagging - The act of stripping 802.1Q VLAN information out of the packet header.

Ingress port - A port on a Switch where packets are flowing into the Switch and VLAN decisions must be made.

Egress port - A port on a Switch where packets are flowing out of the Switch, either to another Switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the GSW-1290 Switch. 802.1Q VLANs require tagging, which enables the VLANs to span an entire network (assuming all Switches on the network are IEEE 802.1Q-compliant).

Any port can be configured as either *tagging* or *untagging*. The *untagging* feature of IEEE 802.1Q VLANs allow VLANs to work with legacy Switches that don't recognize VLAN tags in packet headers. The *tagging* feature allows VLANs to span multiple 802.1Q VLAN compliant Switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

### 802.1Q VLAN Packet Forwarding

Packet forwarding decisions are made based upon the following three types of rules:

Ingress rules – rules relevant to the classification of received frames belonging to a VLAN.

Forwarding rules between ports – decides filter or forward the packet

Egress rules – determines if the packet must be sent tagged or untagged.

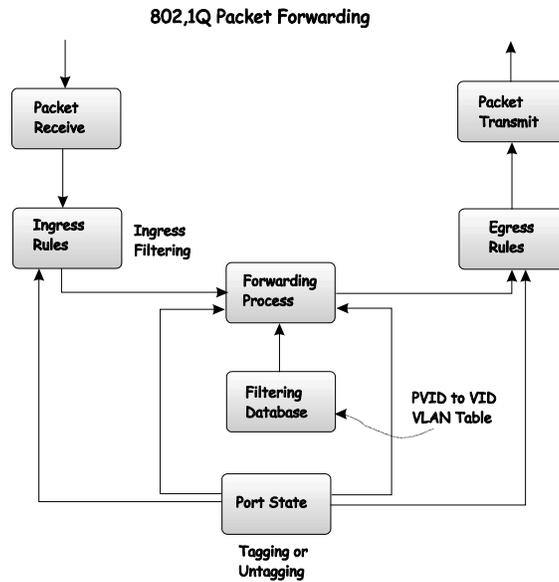


Figure 4- 17. 802.1Q Packet Forwarding

### 802.1Q VLAN Tags

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

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

IEEE 802.1Q Tag

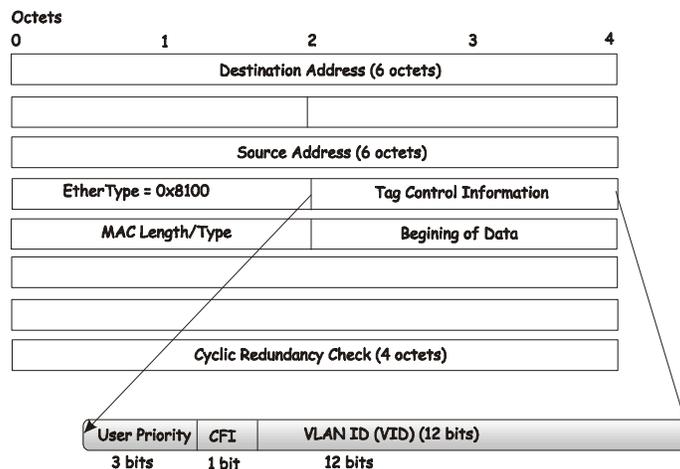


Figure 4- 18. IEEE 802.1Q Tag

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

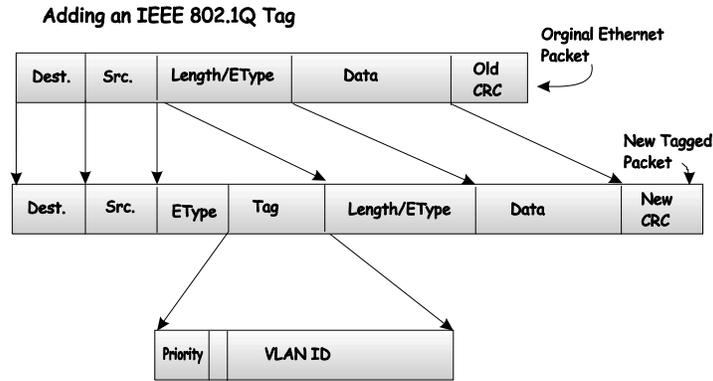


Figure 4- 19. Adding an IEEE 802.1Q Tag

## Port VLAN ID

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

Unfortunately, not all network devices are 802.1Q compliant. These devices are referred to as *tag-unaware*. 802.1Q devices are referred to as *tag-aware*.

Prior to the adoption 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address (found in the Switch's forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the Switch will drop the packet.

Within the Switch, different PVIDs mean different VLANs. (remember that two VLANs cannot communicate without an external router). So, VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given Switch (or Switch stack).

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

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

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

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

## Tagging and Untagging

Every port on an 802.1Q compliant Switch can be configured as *tagging* or *untagging*.

Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet forwarding decisions.

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

### Ingress Filtering

A port on a Switch where packets are flowing into the Switch and VLAN decisions must be made is referred to as an *ingress port*. If ingress filtering is enabled for a port, the Switch will examine the VLAN information in the packet header (if present) and decide whether or not to forward the packet.

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the Switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port will tag the packet with its own PVID as a VID (if the port is a tagging port). The Switch then determines if the destination port is a member of the same VLAN (has the same VID) as the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded and the destination port transmits it on its attached network segment.

This process is referred to as *ingress filtering* and is used to conserve bandwidth within the Switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

### 802.1Q Static VLANs

To create or modify an 802.1Q VLAN:

In the **Configuration** folder, open the **VLANs** folder and click the **Static VLAN Entry** link to open the following window:

802.1Q Static VLANs			
Add new 802.1Q VLAN			Add
Current 802.1Q Static VLANs Entries			
VLAN ID	VLAN name	Modify	Delete
1	default	Modify	X
2	rLAN	Modify	X
3	5th_floor	Modify	X

Figure 4- 20. 802.1Q Static VLANs Entries table

The first **802.1Q Static VLANs** window lists all previously configured VLANs by VLAN ID and name. To delete an existing 802.1Q VLAN, click the corresponding **Delete** button.

To create a new 802.1Q VLAN, click the **Add** button. A new window appears, use this to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new window.



Figure 4- 21. 802.1Q Static VLANs menu

To configure the newly created VLAN, select the Switch being configured from the **Unit** drop-down menu and provide a unique VLAN identifier and name. Configure the port settings for VLAN membership by selecting the appropriate options for each port. Click the **Apply** button to configure the VLAN port membership settings. A success or fail message appears to confirm whether the settings have been applied. To view the VLANs that have been thus far configured, click the [Show All Static VLAN Entries](#) hyperlink (see example below). To add another new VLAN entry, click the **Add** button again in the first **802.1Q Static VLANs** window.

See the table below for a description of the port VLAN membership settings.

The following fields can then be set in either the Add or Modify 802.1Q Static VLANs windows:

Parameter	Description
<b>Unit</b>	Choose the Switch that the VLAN will be created on.
<b>VID (VLAN ID)</b>	For a new VLAN entry, type in a unique identifier. This number is used to configure other settings such as GVRP status for ports in the VLAN.
<b>VLAN Name</b>	For a new VLAN entry type in a unique name. This name can be used to identify the VLAN for IP interface assignment. Remember that VLAN names are case-sensitive when referring to them for other applications (such as setting up IP interfaces).
<b>Port</b>	Configure each individual port to be specified as member or nonmember of the VLAN.
<b>Tag</b>	Specifies the port as either 802.1Q tagging or 802.1Q untagged. Checking the box will designate the port as Tagged.
<b>None</b>	Specifies the port as not being a static member of the VLAN, but with no

restrictions for joining the VLAN dynamically through GVRP.

**Egress** Select this to specify the port as a static member of the VLAN. Egress member ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.

**Forbidden** Select this to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

The illustration below displays the port settings for a new VLAN (engineering) with a VID of 11.

Unit	VID	VLAN Name											
15	11	engineering											
Port Settings		1	2	3	4	5	6	7	8	9	10	11	12
Tag		<input checked="" type="checkbox"/>											
None		<input type="radio"/>											
Egress		<input type="radio"/>											
Forbidden		<input type="radio"/>											

Apply

[Show All Static VLAN Entries](#)

Figure 4- 22. Add New Static VLAN Example menu

Click the [Show All Static VLAN Entries](#) link to return to the first **802.1Q Static VLANs** window, the new VLAN entry appears listed in the current entries table.

VLAN ID	VLAN name	Modify	Delete
1	default	Modify	X
2	rLAN	Modify	X
3	5th_floor	Modify	X
11	engineering	Modify	X

Figure 4- 23. 802.1Q Static VLANs With Added VLAN menu

To change the port settings of any listed VLAN, click the **Modify** button.

Now click the **Modify** button in the first **802.1Q Static VLANs** window for the newly created VLAN (engineering). A new window appears, use this to configure the port settings to the existing VLAN, exactly

as in the add new VLAN window. Notice that the VID and name cannot be changed. If you want to change the VID or VLAN Name it will be necessary to delete the existing entry and create a new one.

802.1Q Static VLANs												
Unit	VID	VLAN Name										
15	11	engineering										
Port Settings	1	2	3	4	5	6	7	8	9	10	11	12
Tag	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>						
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>						
Egress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>						
Forbidden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>						

Apply

[Show All Static VLAN Entries](#)

Figure 4- 24. 802.1Q Static VLANs – Modify menu

## GVRP Setting

Open the **802.1Q Port Settings** window and select the Unit and range of ports to configure. For the selected port or group of ports, choose to enable or disable Ingress checking and establish an acceptable packet rule. Ingress Checking is used to limit traffic by filtering incoming packets that have a PVID does not match the PVID of the port. 802.1Q port settings are also used to determine whether the Switch will share its VLAN configuration information with GARP VLAN Registration Protocol (GVRP) enabled Switches.

The window and table below describe how to configure the 802.1Q VLAN port settings for the Switch.

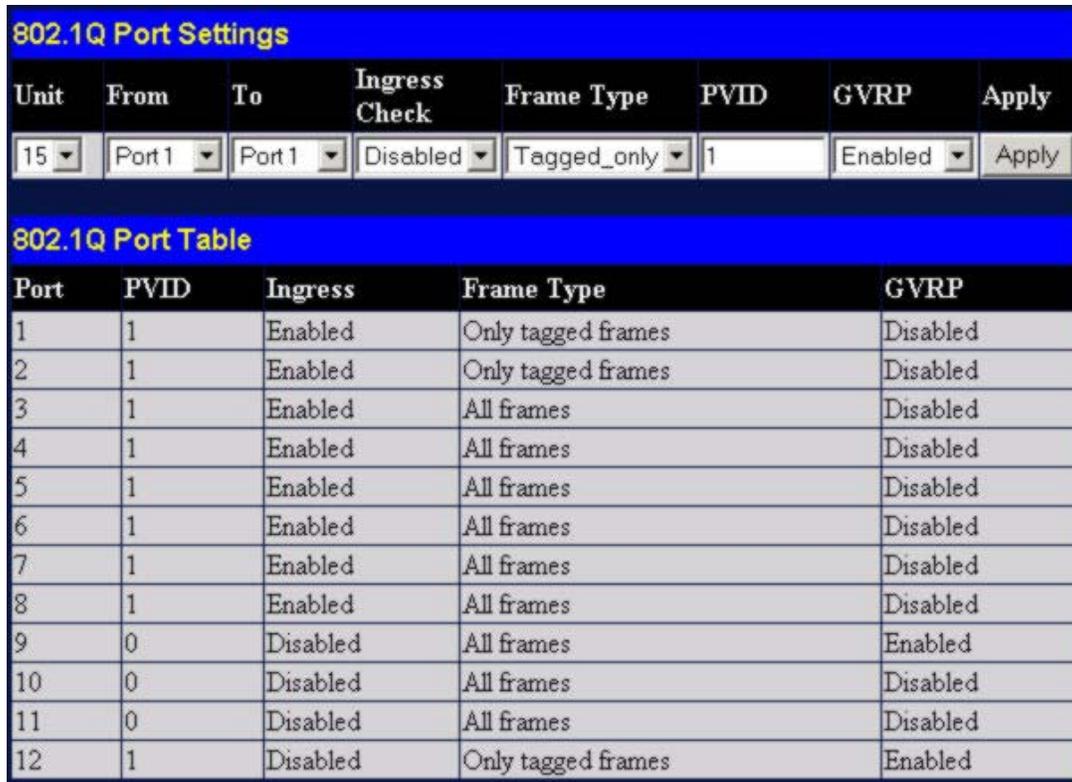


Figure 4- 25. 802.1Q Port Settings and entries table

Configure the 802.1 Port Settings:

Parameter	Description
<b>Unit</b>	Select the relevant Switch for configuration.
<b>From [ ] To [ ]</b>	Use these drop-down menus to specify the range of ports that will be included in the VLAN.
<b>Ingress Check</b>	This field can be toggled using the space bar between <i>Enabled</i> and <i>Disabled</i> . <i>Enabled</i> enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. <i>Disabled</i> disables Ingress filtering. Ingress Checking is disabled by default.
<b>Frame Type</b>	Allows you to specify the action the Switch will take when a packet is received. If you specify <i>Admit_all</i> the Switch will receive and forward all packets to this VLAN regardless of whether or not the packet has an 802.1Q VLAN tag or not. If you specify <i>Tagged_only</i> the Switch will drop and untagged packets it receives for this VLAN.
<b>PVID</b>	A Port VLAN Identifier is a classification mechanism that associates a port with a specific VLAN and is used to make forwarding decisions for untagged packets received by the port. For example, if port 2 is assigned a PVID of 3, then all untagged packets received on port 2 will be assigned to VLAN 3. This number is generally the same as the VID number assigned to the port in the Edit 802.1Q VLANs window above.

**GVRP**

The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is disabled by default.

**QoS**

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. The IEEE 802.1p Priority specification uses eight priority levels to classify data packets. In 802.1p compliant devices, a tag inserted into the packet header is used to identify the priority level of data packets.

The Switch implements 802.1p priority using four hardware queues instead of eight. Therefore the Switch must have a means of mapping the eight levels specified in the IEEE 802.1p standard to the four hardware queues used in the Switch. This is done using the Class of Service menu explained below. Further customization of priority classification can be done with the Output Scheduling menu, also explained below.

Individual ports may still be assigned priority using the eight levels as defined by the 802.1p standard.

It is important to note that changes in a networks QoS scheme should be carefully considered, planned for and if possible tested for efficiency. When set up properly, it QoS can allow efficient and timely delivery of data for video conferencing or IP telephony without causing unacceptable delays of other network traffic. If QoS is not well set up however, significant delays and excessive packet loss may result for data assigned to lower priority queues.

**802.1p Default Priority**

The Switch allows the assignment of a default 802.1p priority to each port on the Switch.

Click on the **802.1p Default Priority** link in the **QoS** sub-folder:

The screenshot shows a web interface for configuring port priorities. At the top, there is a blue header with the text "Port Default Priority assignment". Below this header is a form with five columns: "Unit", "From", "To", "Priority(0~7)", and "Apply". The "Unit" column has a dropdown menu with "15" selected. The "From" and "To" columns have dropdown menus with "Port 1" selected. The "Priority(0~7)" column has a text input field with "7" entered. The "Apply" column has a button labeled "Apply".

Below the form is another blue header with the text "The Port Priority Table". Underneath this header is a table with two columns: "Port" and "Priority". The table contains 12 rows of data:

Port	Priority
1	5
2	5
3	7
4	7
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	4

Figure 4- 26. Port Default Priority assignment menu

This page allows you to assign a default 802.1p priority to any given port on the Switch. The priority queues are numbered from 0 – the lowest priority – to 7 – the highest priority.

## 802.1p User Priority

The GSW-1290 allows the assignment of a User Priority to each of the 802.1p priorities.

User Priority Configuration	
Priority-0	Class-2
Priority-1	Class-0
Priority-2	Class-1
Priority-3	Class-3
Priority-4	Class-4
Priority-5	Class-5
Priority-6	Class-6
Priority-7	Class-7

Apply

Figure 4- 27. User Priority Configuration menu

Once you have assigned a priority to the port groups on the Switch, you can then assign this Class to each of the eight levels of 802.1p priorities.

## QoS Output Scheduling Configuration

QoS can be customized by changing the output scheduling used for the hardware queues in the Switch. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority queues are affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delay. If you choose to customize this setting, it is important to monitor network performance, especially during peak demand as bottlenecks can quickly develop if the QoS settings are not suitable.

QoS Output Scheduling Configuration	
Scheduling Mechznixm	Apply
RoundRobin ▾	Apply
QoS Output Scheduling Table	
Class	Scheduling Mechanism
Class_0	RoundRobin
Class_1	RoundRobin
Class_2	RoundRobin
Class_3	RoundRobin
Class_4	RoundRobin
Class_5	RoundRobin
Class_6	RoundRobin
Class_7	RoundRobin

**Figure 4- 28. QoS Output Scheduling Configuration menu**

Use the Scheduling Mechanism drop-down menu to select between a *RoundRobin* and a *Strict* mechanism for emptying the priority queues.

Click **Apply** to let your changes take effect.

### Traffic Segmentation

Traffic segmentation is used to limit traffic flow from a single port to a group of ports on either a single Switch (in standalone mode) or a group of ports on another Switch in a Switch stack. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive. It provides a method of directing traffic that does not increase the overhead of the Master Switch CPU.

Unit	Port	Configuration	Setup
15	Port 1	View	Setup
Current Traffic Segmentation Table			
Unit	Port Map		
15	1-12		
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			

Figure 4- 29. Traffic Segmentation table

The Unit drop-down menu at the top of the page allows you to select a Switch from a Switch stack using that Switch's Unit ID. The Port drop-down menu allows you to select a port from that Switch. This is the port that will be transmitting packets.

Unit	Port											
15	Port 1											
Setup Forwarding ports												
Unit	15											
Forward Port	1	2	3	4	5	6	7	8	9	10	11	12
	<input checked="" type="checkbox"/>											
Apply												
<a href="#">View Settings of Unit 15 Port 1</a>												

Figure 4- 30. Traffic Segmentation Setup menu

## Bandwidth Control

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port.

The screenshot shows the 'Bandwidth Settings' menu with the following configuration:

- Unit: 15
- From: Port 1
- To: Port 1
- Type: RX
- no\_limit: Disabled
- Rate: 1
- Apply button

Below the settings is the 'Port Bandwidth Table' with the following data:

Port	RX Rate (Mbit/sec)	TX Rate (Mbit/sec)
1	no_limit	no_limit
2	no_limit	no_limit
3	no_limit	no_limit
4	no_limit	no_limit
5	no_limit	no_limit
6	no_limit	no_limit
7	no_limit	no_limit
8	no_limit	no_limit
9	no_limit	no_limit
10	no_limit	no_limit
11	no_limit	no_limit
12	no_limit	no_limit

Figure 4- 31. Bandwidth Settings menu

The following parameters can be set or are displayed:

Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a Switch stack using that Switch's Unit ID. The number 15 indicates a Switch in standalone mode.
<b>From/To</b>	A consecutive group of ports may be configured starting with the selected port.
<b>Type</b>	This drop-down menu allows you to select between <i>RX</i> (receive,) <i>TX</i> (transmit,) and <i>Both</i> . This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
<b>no_limit</b>	This drop-down menu allows you to specify that the selected port will have no bandwidth limit. <i>Enabled</i> disables the limit.
<b>Rate</b>	This field allows you to enter the data rate, in kb/s, that will be the limit for the selected port.

## MAC Notification

MAC address notification is used to monitor MAC addresses as they are learned and entered into the Switch's MAC forwarding database.

### Global Settings



The screenshot shows a web-based configuration interface for MAC Notification Global Settings. The title bar is blue with yellow text. The settings are as follows:

Parameter	Value
State	Disabled
Interval (sec)	1
History size	1

An 'Apply' button is visible at the bottom right of the configuration area.

Figure 4- 32. MAC Notification Global Settings menu

The following parameters can be set:

Parameter	Description
<b>State</b>	This drop-down menu is used to enable or disable MAC notification on the selected Switch.
<b>Interval (sec)</b>	The time in seconds between notifications.
<b>History size</b>	The maximum number of entries that will be listed in the History log. Up to 500 entries can be specified.

---

## Port Settings

Enable or disable MAC notification for ports with the window below.

MAC Notification Port Settings				
Unit	From	To	State	Apply
15	Port 1	Port 1	Disabled	Apply

MAC Notification Port State Table	
Port	State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled

**Figure 4- 33. MAC Notification Port Settings menu**

The following parameters can be set:

Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a Switch stack using that Switch's Unit ID. Number 15 indicates a Switch in standalone mode.
<b>From/To</b>	A consecutive group of ports may be configured starting with the selected port.
<b>State</b>	This pull-down menu allows you to enable or disable MAC notification for the specified Switch and group of ports.

## System Log Server

Use the System Log to keep a record of warning and other pertinent system information. The Switch can send system log (SysLog) messages to up to four designated servers.

System Log Servers						
Add New System Log Server						Add
Current System Log Servers						
Index	Server IP	Severity	Facility	UDP Port	Status	Delete
<a href="#">1</a>	10.24.32.2	warning	Local0	514	Enabled	<input type="checkbox"/>
<a href="#">2</a>	10.24.47.45	warning	Local1	514	Disabled	<input type="checkbox"/>
<a href="#">3</a>	10.24.39.78	informational	Local0	514	Enabled	<input type="checkbox"/>

Figure 4- 34. System Log Servers entries table

Click the **Add** button to bring up the window pictured below. The parameters configured for adding System Log are described in the table below. To eliminate a System Log Server configuration, click the X in the Delete column for the configuration being removed.

System Log Server-Add	
Index	<input type="text" value="0"/>
Server IP	<input type="text" value="0.0.0.0"/>
Severity	<input type="text" value="Warning"/>
Facility	<input type="text" value="Local0"/>
UDP Port	<input type="text" value="0"/>
Status	<input type="text" value="Disabled"/>
<input type="button" value="Apply"/>	
<a href="#">Show All System Log Servers</a>	

Figure 4- 35. System Log Servers – Add menu

Configure these parameters for the system log:

Parameter	Description
<b>Index</b>	Syslog server settings index (1-4).
<b>Server IP</b>	The IP address of the Syslog server.
<b>Severity</b>	<p>This drop-down menu allows you to select the level of messages that will be sent. The options are <i>Warning</i>, <i>Informational</i>, and <i>ALL</i>.</p> <p>Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font means the facility values that the Switch currently supports.</p>
<b>Facility</b>	<p>Numerical Facility Code</p> <ul style="list-style-type: none"> <li>0 kernel messages</li> <li>1 user-level messages</li> <li>2 mail system</li> <li>3 system daemons</li> <li>4 security/authorization messages</li> <li>5 messages generated internally by syslog line printer subsystem</li> <li>7 network news subsystem</li> <li>8 UUCP subsystem</li> <li>9 clock daemon</li> <li>10 security/authorization messages</li> <li>11 FTP daemon</li> <li>12 NTP subsystem</li> <li>13 log audit</li> <li>14 log alert</li> <li>15 clock daemon</li> <li><b>16 local use 0 (local0)</b></li> <li><b>17 local use 1 (local1)</b></li> <li><b>18 local use 2 (local2)</b></li> <li><b>19 local use 3 (local3)</b></li> <li><b>20 local use 4 (local4)</b></li> <li><b>21 local use 5 (local5)</b></li> <li><b>22 local use 6 (local6)</b></li> <li><b>23 local use 7 (local7)</b></li> </ul>
<b>UDP Port</b>	Type the UDP port number used for sending Syslog messages.
<b>Status</b>	Choose <i>Enabled</i> or <i>Disabled</i> to activate or deactivate this

---

## Port Security

A given port's (or a range of port's) dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table can not be changed once the port lock is enabled. The port can be locked by using the Admin State pull-down menu to *Enabled*, and clicking **Apply**.

This is a security feature that prevents unauthorized computers (with source MAC addresses unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

**Port Security Settings**

Unit	From	To	Admin State	Max.Addr(0-10)	Lock Address Mode	Apply
15	Port 1	Port 1	Disabled	0	Permanent	Apply

**Port Security Table**

Port	Admin State	Max.Learning Addr	Lock Address Mode
1	Disabled	1	DeleteOnReset
2	Disabled	1	DeleteOnReset
3	Disabled	1	DeleteOnReset
4	Disabled	1	DeleteOnReset
5	Disabled	1	DeleteOnReset
6	Disabled	1	DeleteOnReset
7	Disabled	1	DeleteOnReset
8	Disabled	1	DeleteOnReset
9	Disabled	1	DeleteOnReset
10	Disabled	1	DeleteOnReset
11	Disabled	1	DeleteOnReset
12	Disabled	1	DeleteOnReset

Figure 4- 36. Port Security Settings menu and table

The following parameters can be set:

Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a Switch stack using that Switch's Unit ID. The number 15 indicates a Switch in standalone mode.
<b>From/To</b>	A consecutive group of ports may be configured starting with the selected port.
<b>Admin State</b>	This pull-down menu allows you to enable or disable Port Security (locked MAC address table for the selected ports.)
<b>Max.Addr(0-10)</b>	The number of MAC addresses that will be in the MAC address forwarding table for the selected Switch and group of ports.

table for the selected Switch and group of ports.

**Lock Address Mode** This pull-down menu allows you to select how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are *Permanent*, *DeleteOnReset*, and *DeleteOnTimeout*.

## SNTP Settings

The Simple Network Time Protocol (SNTP) (an adaptation of the Network Time Protocol (NTP)) is configured on the Switch using the following windows.

### Current Time and SNTP Settings

The screenshot displays three sections of the configuration interface:

- Current Time: Status**
  - Current Time: 0 days 05:24:25
  - Time Source: System Clock
- Current Time: SNTP Settings**
  - SNTP State: Disabled (dropdown menu)
  - SNTP Primary Server: 0.0.0.0 (text input)
  - SNTP Secondary Server: 0.0.0.0 (text input)
  - SNTP Poll Interval in Seconds: 720 (text input)
  - Apply button
- Current Time: Set Current Time**
  - Year: (dropdown menu)
  - Month: (dropdown menu)
  - Day: (dropdown menu)
  - Time in HH MM SS: (three dropdown menus)
  - Apply button

Figure 4- 37. Current Time and SNTP menu

The following parameters can set or are displayed:

Parameter	Description
<b>Current Time</b>	Displays the current system time.
<b>Time Source</b>	Displays the time source for the system.
<b>SNTP State</b>	Use this pull-down menu to enable or disable SNTP.
<b>SNTP Secondary Server</b>	This is the primary server the SNTP information will be taken from
<b>SNTP Poll Interval</b>	This is the interval between requests for updated SNTP information.

**in Seconds**

- Year** Enter the current year, if you want to update the system clock.
- Month** Enter the current month, if you want to update the system clock.
- Day** Enter the current day, if you want to update the system clock.
- Time in HH MM SS** Enter the current time in hours, minutes, and seconds, if you want to update the system clock.

**Time Zone and DST**

Adjust time zone settings for the Switch. See the table below for a description of the time zone settings.

Time Zone and DST Settings	
Daylight Saving Time State	Disabled
Daylight Saving Time Offset in Minutes	60
Time Zone Offset from GMT in +/-HH:MM	- 06 00
DST Repeating Settings	
From Which Week of the month	First
From Which Day of the Week	Sunday
From Which Month	April
From What Time HH:MM	00 00
To Which Week	Last
To Which Day	Sunday
To Which Month	October
To What Time HH:MM	00 00
DST Annual Settings	
From What Month	April
From What Date	29
From What Time	00 00
To What Month	October
To What Date	12
To What Time	00 00
Apply	

Figure 4- 38. Time Zone and DST Settings menu

The following parameters can set:

Parameter	Description
<b>Daylight Saving Time State</b>	Use this pull-down menu to enable or disable the DST Settings.
<b>Daylight Saving Time Offset in Minutes</b>	Use this pull-down menu to specify the amount of time that will constitute your local DST offset – 30, 60, 90, or 120 minutes.
<b>Time Zone Offset from GMT in +/- HH:MM</b>	Use these pull-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)
<i>DST Repeating Settings</i>	Repeating - Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.
<b>From: Which Week of the month</b>	Enter the week of the month that DST will start.
<b>From: Which Day of Week</b>	Enter the day of the week that DST will start on.
<b>From: Which Month</b>	Enter the month DST will start on.
<b>From: What Time HH:MM</b>	Enter the time of day that DST will start on.
<b>To: Which Week</b>	Enter the week of the month the DST will end.
<b>To: Which Day</b>	Enter the day of the week that DST will end.
<b>To: Which Month</b>	Enter the month that DST will end.
<b>To: What Time HH:MM</b>	Enter the time DST will end.
<i>DST Annual Settings</i>	Annual - Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.
<b>From: What Month</b>	Enter the month DST will start on, each year.
<b>From: What Date</b>	Enter the day of the week DST will start on, each year.
<b>From: What Time</b>	Enter the time of day DST will start on, each year.
<b>To: What Month</b>	Enter the month DST will end on, each year.
<b>To: What Date</b>	Enter the day of the week DST will end on, each year.

**To: What Time**      Enter the time of day that DST will end on, each year.

### Access Profile Table

Access profiles allow you to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of VLAN, MAC address or IP address.

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below in two parts.

To display the currently configured Access Profiles on the Switch, open the **Configuration** folder and click on the **Access Profile Table** link. This will open the **Access Profile Table** window, as shown below.

Profile ID	Mode	Type	Access Rule	Delete
1	Permit	IP	Modify	X
2	Deny	IP	Modify	X
3	Permit	Ethernet	Modify	X

**Figure 4- 39. Access Profile Table window**

To add an entry to the **Access Profile Table** window, click the **Add** button. This will open the **Access Profile Configuration** window, as shown below. There are two **Access Profile Configuration** windows – one for Ethernet (or MAC address-based) profile configuration and one for IP address-based profile configuration. You can Switch between the two **Access Profile Configuration** windows by using the Type drop-down menu, and clicking on the **Apply** button. The **Access Profile Configuration** window for Ethernet is shown below.

**Access Profile Configuration**

Profile ID(1-255)    1

Type    Ethernet

Vlan   

Source Mac     00-00-00-00-00-00

Destination Mac     00-00-00-00-00-00

802.1p   

Ethernet type   

Mode      Permit  Deny

Apply

[Show All Access Profile Table Entries](#)

**Figure 4- 40. Access Profile Configuration (Ethernet) menu**

The following parameters can be set for Ethernet type Access Profile configurations:

Parameter	Description
<b>Profile ID(1-255)</b>	Type in a unique identifier number for this profile set or allow an ID to be automatically assigned by checking the Auto Assign option. This value can be set from 1 to 255.
<b>Type</b>	Select profile based on Ethernet (MAC Address) or IP address. This will change the window according to the requirements for the type of profile. Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header.
<b>Vlan</b>	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
<b>Source Mac</b>	Source MAC Mask - Enter a MAC address mask for the source MAC address.
<b>Destination Mac</b>	Destination MAC Mask - Enter a MAC address mask for the destination MAC address.
<b>802.1p</b>	Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.
<b>Ethernet type</b>	Selecting this option instructs the Switch to examine the Ethernet type value of each packet header and use this as the, or part of the criterion for forwarding.
<b>Mode</b>	Select Permit to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).  Select Deny to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.

---

The page shown below is the **Access Profile Configuration** menu for IP.

IP based Access Profile configurations use a different parameters set. See the table below for a description of the various settings.

Access Profile Configuration	
Profile ID(1-255)	<input type="text" value="1"/>
Type	<input type="text" value="IP"/>
Vlan	<input type="checkbox"/>
Source IP Mask	<input type="checkbox"/> <input type="text" value="0.0.0.0"/>
Destination IP Mask	<input type="checkbox"/> <input type="text" value="0.0.0.0"/>
Dscp	<input type="checkbox"/>
Protocol	<input type="checkbox"/> <input checked="" type="radio"/> ICMP <input type="checkbox"/> type <input type="checkbox"/> code <input type="checkbox"/> <input checked="" type="radio"/> IGMP <input type="checkbox"/> type <input type="checkbox"/> <input checked="" type="radio"/> TCP <input type="checkbox"/> src port mask <input type="text" value="0000"/> <input type="checkbox"/> dest port mask <input type="text" value="0000"/> <input type="checkbox"/> flag bit <input type="checkbox"/> urg <input type="checkbox"/> ack <input type="checkbox"/> psh <input type="checkbox"/> rst <input type="checkbox"/> syn <input type="checkbox"/> fin <input type="checkbox"/> <input checked="" type="radio"/> UDP <input type="checkbox"/> src port mask <input type="text" value="0000"/> <input type="checkbox"/> dest port mask <input type="text" value="0000"/> <input type="checkbox"/> protocol id <input type="checkbox"/> user mask <input type="text" value="00000000"/>
Mode	<input type="checkbox"/> <input checked="" type="radio"/> Permit <input type="radio"/> Deny
<input type="button" value="Apply"/>	
<a href="#">Show All Access Profile Table Entries</a>	

Figure 4- 41. Access Profile Configuration (IP) window

The following parameters can be set:

Parameter	Description
<b>Profile ID(1-255)</b>	Type in a unique identifier number for this profile set or allow an ID to be automatically assigned by checking the Auto Assign option. This value can be set from 1 to 255.
<b>Type</b>	Select profile based on Ethernet (MAC Address) or IP address. This will change the menu according to the requirements for the type of profile. Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header.
<b>Vlan</b>	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
<b>Source IP Mask</b>	Source IP Mask - Enter an IP address mask for the source IP address.
<b>Destination IP Mask</b>	Destination IP Mask - Enter an IP address mask for the destination MAC address.
<b>Dscp</b>	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
<b>Protocol</b>	<p>Selecting this option instructs the Switch to examine the protocol type value in each frame's header. You must then specify what protocol(s) to include according to the following guidelines:</p> <p>Select ICMP to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.</p> <p>Select type to further specify that the access profile will apply an ICMP type value, or specify code to further specify that the access profile will apply an ICMP cod value.</p> <p>Select IGMP to instruct the Switch to examine the Internet Group Management Protocol (ICMP) field in each frame's header.</p> <p>Select type to further specify that the access profile will apply an IGMP type value</p> <p>Select TCP to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask, a destination port mask or a flag bite.</p> <p>src port mask – Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff).</p> <p>dest port mask – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff).</p> <p>flag bite – Specify a flag bite in the TCP header.</p> <p>Select UDP to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask.</p> <p>src port mask – Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff).</p> <p>dest port mask – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff).</p> <p>protocol id – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffffffff).</p>
<b>Mode</b>	Select Permit to specify that the packets that match the access profile are

forwarded by the Switch, according to any additional rule added (see below).

Select Deny to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.

To establish the rule for a previously created Access Profile, select the Access Profile entry from the **Access Profile Table** window and then click the **Modify** button for that individual entry.

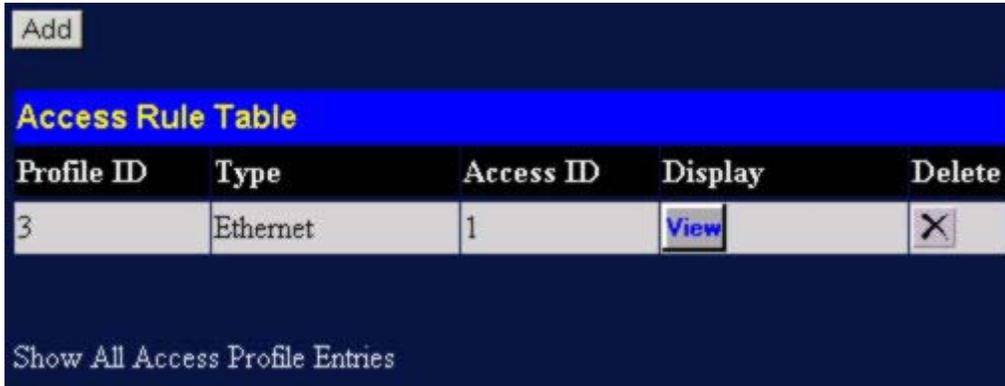


Figure 4- 42. Access Rule Table window

To create a new rule set for the access profile, click the **Add** button. Click on **View** to see the settings for the rule entry. A new window is displayed. To remove a previously created rule, select it and click the **Delete** button.

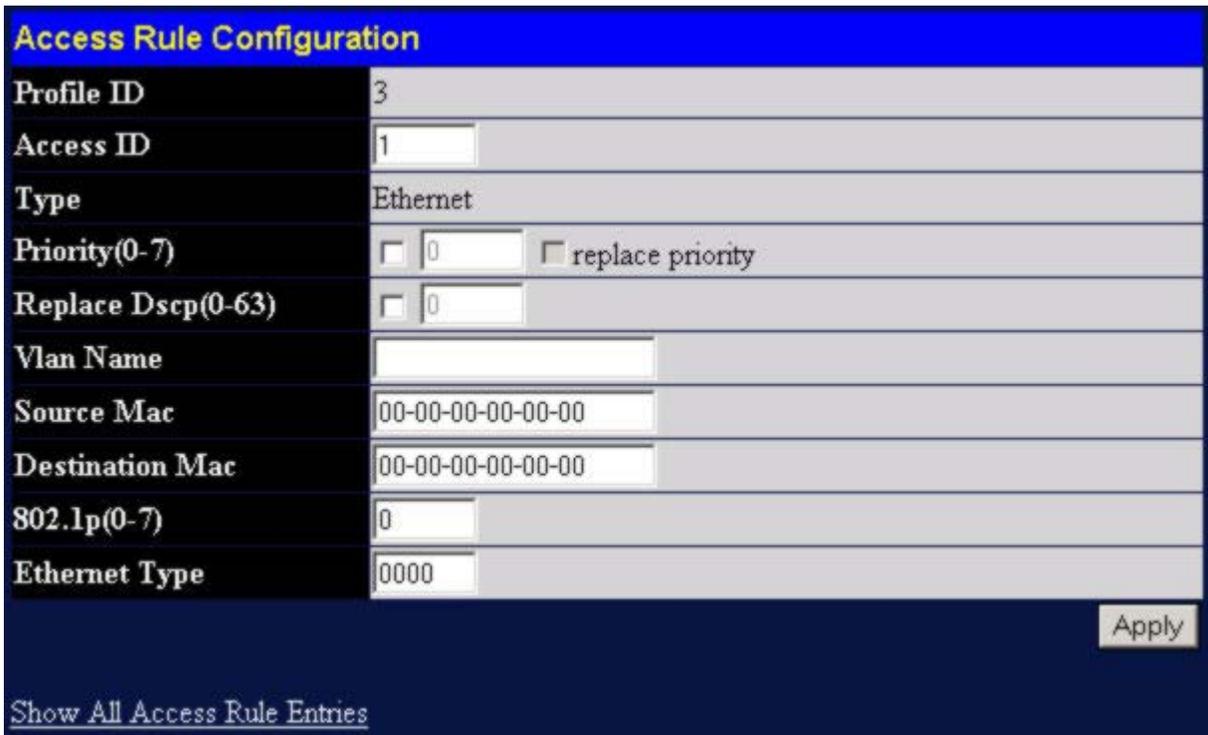


Figure 4- 43. Access Rule Configuration (Ethernet) menu

Configure the Access Rule Configuration settings and click the **Apply** button to enter it in the Access Rules table. See the table below for a description of the rule parameters.

The following parameters can be set:

Parameter	Description
<b>Profile ID</b>	This is the identifier number for this profile set.
<b>Access ID</b>	Type in a unique identifier number for this access. This value can be set from 1 to 255.
<b>Type</b>	Select profile based on Ethernet (MAC Address) or IP address. This will change the menu according to the requirements for the type of profile. Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header.
<b>Priority(0-7)</b>	Specify the priority tag, located in the packet header that will be identified by the Switch.
<b>Replace Dscp(0-63)</b>	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
<b>Vlan Name</b>	Allows the entry of a name for a previously configured VLAN.
<b>Source Mac</b>	Source MAC Address - Enter a MAC Address for the source MAC address.
<b>Destination Mac</b>	Destination MAC Address - Enter a MAC Address mask for the destination MAC address.
<b>802.1p(0-7)</b>	Enter a value from 0 to 7 to specify that the access profile will apply only to packets with this 802.1p priority value.
<b>Ethernet Type</b>	Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value (hex 0x0-0xffff) in the packet header. The Ethernet type value may be set in the form: hex 0x0-0xffff, which means the user may choose any combination of letters and numbers ranging from a-f and from 0-9999.

---

**Figure 4- 44. Access Rule Configuration (IP) window**

Configure the Access Rule Configuration settings on the window above.

The following parameters can be set:

Parameter	Description
<b>Profile ID</b>	This is the identifier number for this profile set.
<b>Access ID</b>	Type in a unique identifier number for this access. This value can be set from 1 to 255.
<b>Type</b>	Select profile based on Ethernet (MAC Address) or IP address. This will change the menu according to the requirements for the type of profile. Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header.
<b>Priority(0-7)</b>	Specify the priority tag, located in the packet header that will be identified by the Switch.
<b>Dscp(0-63)</b>	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
<b>Vlan Name</b>	Allows the entry of a name for a previously configured VLAN.
<b>Source IP</b>	Source IP Address - Enter an IP Address mask for the source IP address.
<b>Destination IP</b>	Destination IP Address- Enter an IP Address mask for the destination IP address.
<b>Dscp(0-63)</b>	This field allows the user to enter a DSCP value in the space provided, which will instruct the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding. The user may choose a value between 0 and 63.
<b>Protocol</b>	This field allows the user to modify the protocol used to configure the Access Rule Table window; depending on which protocol the user has chosen in the Access Profile Table window.



**Chapter 5**

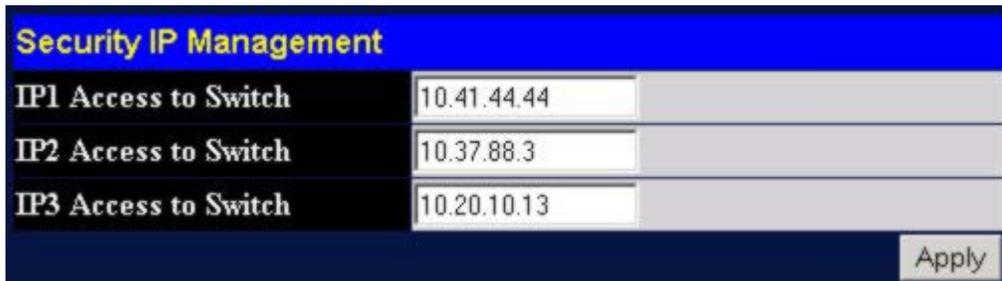
## Security Management

- Trusted Host*
- Port Access Entity*
- 802.1X Authenticator Settings*
- PAE System Control*
- 802.1X Capability Settings*
- Initialize Port(s)*
- Reauthenticate Port(s)*
- Radius Server*

### Trusted Host

The **Security IP Management** window allows you to specify the IP addresses of management stations (PCs) on your network that will be allowed to access the Switch’s Web-based management agent.

You can enter up to three IP addresses of local hosts (on the same subnet as the Switch) that will be allowed to manage the Switch. It is recommended that the IP address of the local host that will be used to manage the Switch be entered here to avoid possible frequent disconnection from the Switch’s Web-based management agent.



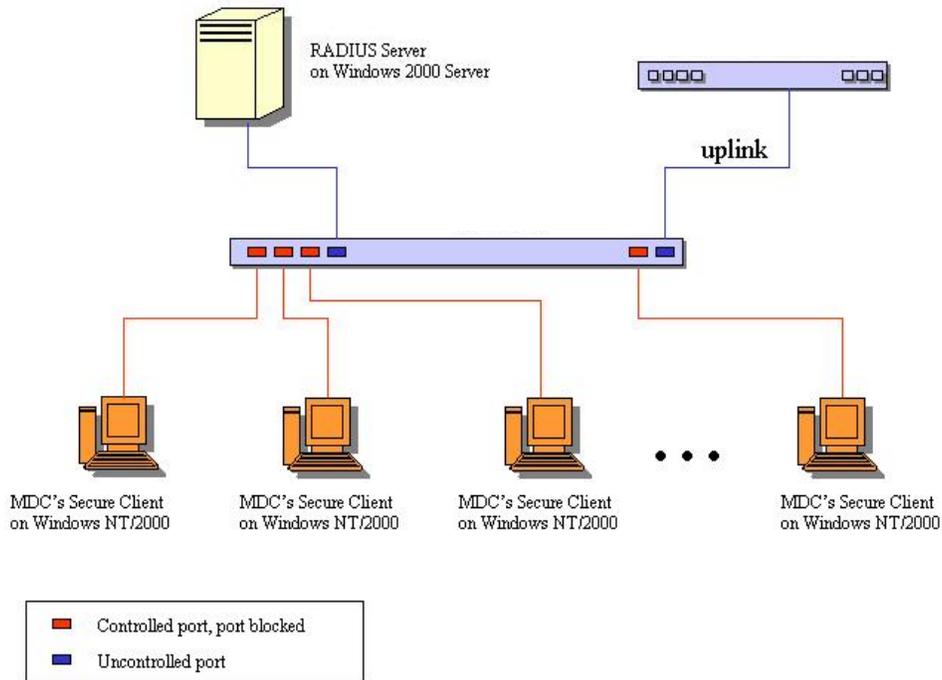
**Figure 5- 1. Security IP Management window**

The following fields can be set:

Parameter	Description
<b>IP1 Access to Switch</b>	Enter the IP address of a management station that will be used to manage the Switch. This IP address must be on the same subnet as the Switch.
<b>IP2 Access to Switch</b>	Enter the IP address of a management station that will be used to manage the Switch. This IP address must be on the same subnet as the Switch.
<b>IP3 Access to Switch</b>	Enter the IP address of a management station that will be used to manage the Switch. This IP address must be on the same subnet as the Switch.

## Port Access Entity

The Switch is an implementation of the server side of IEEE 802.1X-Port Based Network Access Control. Through this mechanism, users have to be authorized before being able to access the network. See the following figure:



**Figure 4- 45. Typical 802.1X Configuration Prior to User Authentication**

Once the user is authenticated, the Switch unblocks the port that is connected to the user as shown in the next figure.

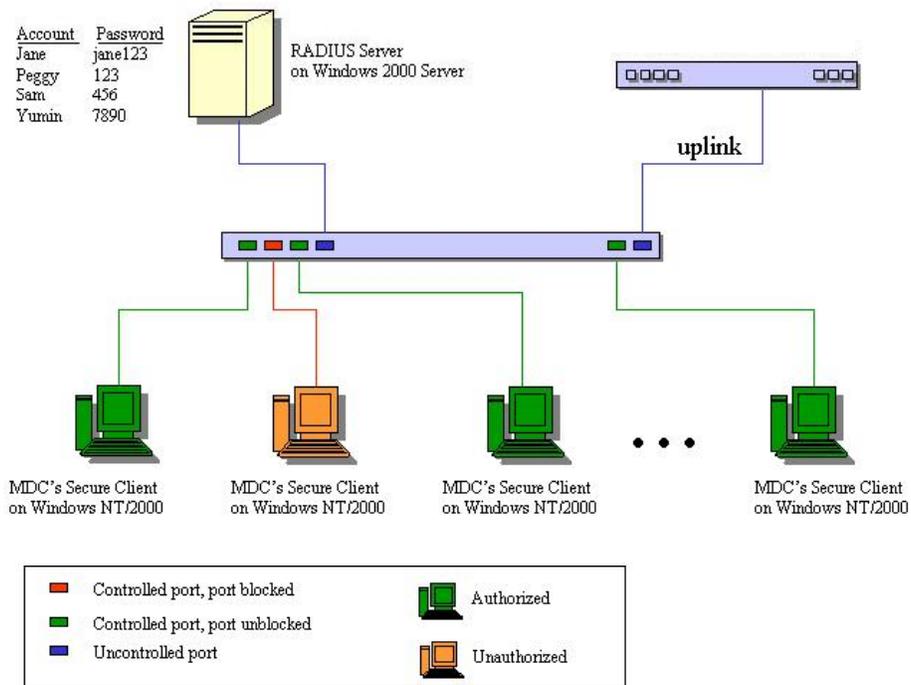


Figure 4- 46. Typical 802.1X Configuration with User Authentication

The user's information, including account number, password, and configuration details such as IP address and billing information, is stored in a centralized RADIUS server.

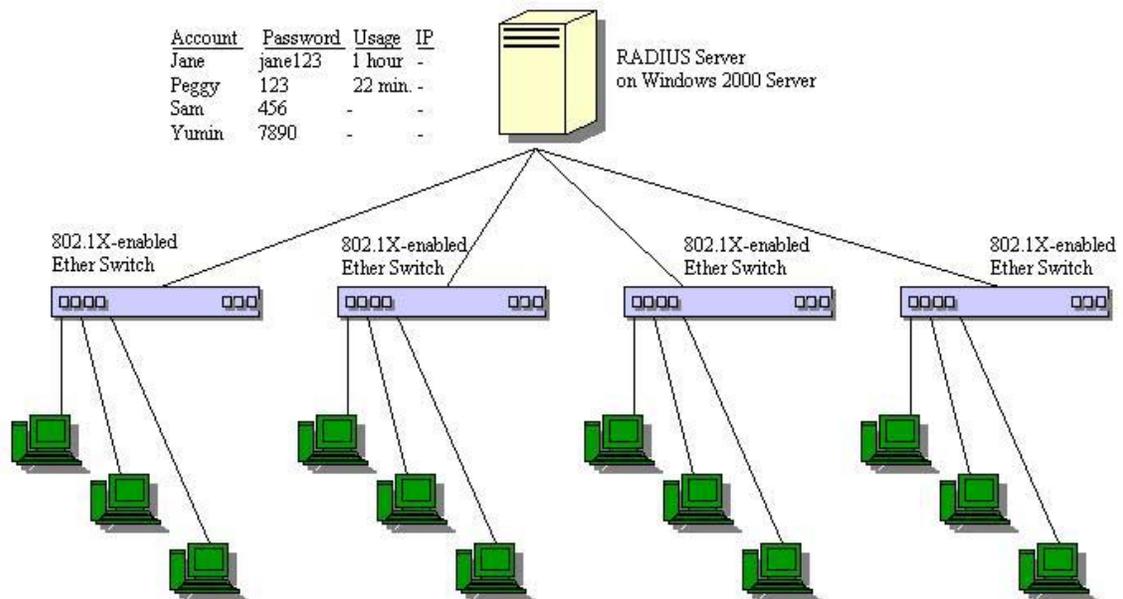


Figure 4- 47. Typical Configuration with 802.1X Fully Implemented

State Machine Name
Port Timers state machine
Authenticator PAE state machine
The Authenticator Key Transmit state machine
Reauthentication Timer state machine
Backend Authentication state machine
Controlled Directions state machine
The Key Receive state machine

**Table 4- 2. Conformance to IEEE 802.1X Standards**

## 802.1X Authenticator Settings

To display the current 802.1X Authenticator Settings on the Switch, open the **Security** folder, and then the **Port Access Entity** folder and finally click on the **802.1X Authenticator Settings** link:

Unit: 15

### 802.1X Authenticator Settings

Port	AdmDir	PortControl	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled
<a href="#">1</a>	both	Auto	30	60	30	30	2	3600	no
<a href="#">2</a>	both	Auto	30	60	30	30	2	3600	no
<a href="#">3</a>	both	Auto	30	60	30	30	2	3600	no
<a href="#">4</a>	both	Auto	30	60	30	30	2	3600	no
<a href="#">5</a>	both	Auto	30	60	30	30	2	3600	no
<a href="#">6</a>	both	Auto	30	60	30	30	2	3600	no
<a href="#">7</a>	both	Auto	30	60	30	30	2	3600	no
<a href="#">8</a>	both	Auto	30	60	30	30	2	3600	no
<a href="#">9</a>	both	Auto	30	60	30	30	2	3600	no
<a href="#">10</a>	both	Auto	30	60	30	30	2	3600	no
<a href="#">11</a>	both	Auto	30	60	30	30	2	3600	no
<a href="#">12</a>	both	Auto	30	60	30	30	2	3600	no

**Figure 4- 48. 802.1X Authenticator Settings entries table**

To configure the 802.1X Authenticator settings for a given port, click on the blue port number under the Port heading. This will open the second **802.1X Authenticator Settings** window, as shown below.

802.1X Authenticator Settings	
Unit	15
From	Port 12
To	Port 12
AdmDir	both
PortControl	Auto
TxPeriod	30
QuietPeriod	60
SuppTimeout	30
ServerTimeout	30
MaxReq	2
ReAuthPeriod	3600
ReAuth	Disabled

Apply

Show Authenticators Setting for Unit 15

Figure 4- 49. 802.1X Authenticator Settings add/modify menu

The following Authenticator Settings parameters can be set:

Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a Switch stack using that Switch's Unit ID. The number 15 indicates a Switch in standalone mode.
<b>From/To</b>	A consecutive group of ports may be configured starting with the selected port.
<b>AdmDir</b>	From the pull-down menu, select whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.  This allows you to control the port authorization state.
<b>PortControl</b>	Select <i>Force_authorized</i> to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client.  If <i>Force_unauthorized</i> is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface.  If <i>Auto</i> is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received

through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

The default setting is *Auto*.

<b>TxPeriod</b>	Select the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.
<b>QuietPeriod</b>	Select the time interval between authentication failure and the start of a new authentication attempt.
<b>SuppTimeout</b>	Select the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.
<b>ServerTimeout</b>	Select the length of time to wait for a response from a Radius server.
<b>MaxReq</b>	Select the maximum number of times to retry sending packets to the supplicant.
<b>ReAuthPeriod</b>	Select the time interval between successive re-authentications.
<b>ReAuth</b>	Enable or disable reauthentication.

---

## PAE System Control

To set the port authenticating settings, open the **Security** folder, and then the **Port Access Entity** folder, and then the **PAE System Control** folder. Finally click on the **802.1X Capability Settings** link.

### 802.1X Capability Settings

Unit	From	To	Capability	Apply
15	Port 1	Port 1	Authenticator	Apply

Port	Capability
1	None
2	None
3	None
4	None
5	None
6	None
7	None
8	None
9	None
10	None
11	None
12	None

**Figure 4- 50. 802.1X Capability Settings window**

To set up the Switch’s 802.1X port-based authentication, select which ports are to be configured in the From and To fields. Next, enable the ports by selecting *Authenticator* from the drop-down menu under Capability.

Click **Apply** to make your changes take effect.

### Initialize Port(s)

Existing 802.1x port settings are displayed and can be configured using the window below.

Open the **Security** folder, and then the **Port Access Entity** folder, and then the **PAE System Control** folder. Finally click on the **Initialize Port(s)** link:

The screenshot shows a web interface for configuring ports. At the top, there are dropdown menus for 'Unit' (set to 15), 'From' (set to Port 1), and 'To' (set to Port 12), along with an 'Apply' button. Below this is a blue header for the 'Initialize Port Table'. The table has six columns: Port, MAC Address, Auth PAE State, Backend\_State, Oper Dir, and PortStatus. The rows show ports 1 through 12, all with 'N/A' for MAC Address, 'N/A' for Backend\_State, 'both' for Oper Dir, and 'authorized' for PortStatus.

Port	MAC Address	Auth PAE State	Backend_State	Oper Dir	PortStatus
1	---	N/A	N/A	both	authorized
2	---	N/A	N/A	both	authorized
3	---	N/A	N/A	both	authorized
4	---	N/A	N/A	both	authorized
5	---	N/A	N/A	both	authorized
6	---	N/A	N/A	both	authorized
7	---	N/A	N/A	both	authorized
8	---	N/A	N/A	both	authorized
9	---	N/A	N/A	both	authorized
10	---	N/A	N/A	both	authorized
11	---	N/A	N/A	both	authorized
12	---	N/A	N/A	both	authorized

Figure 4- 51. Initialize Port window

This window allows you to initialize a port or group of ports. The Initialize Port Table in the bottom half of the window displays the current status of the port(s) once you have clicked **Apply**.

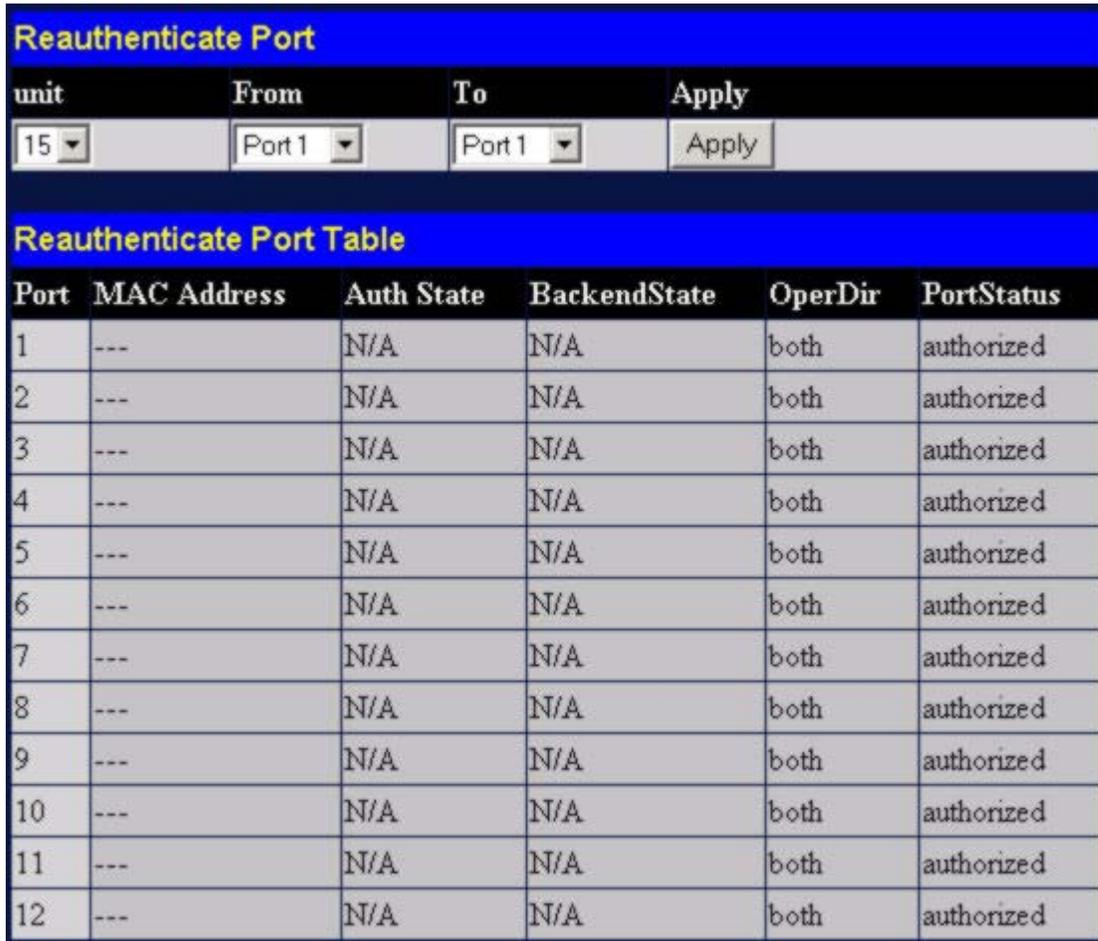
This window displays the following information:

Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a switch stack using that Switch's Unit ID. The number 15 indicates a Switch in standalone mode.
<b>From/To</b>	A consecutive group of ports may be configured starting with the selected port.
<b>Port</b>	The port number.
<b>MAC Address</b>	The MAC address of the switch where the port resides
<b>Auth PAE State</b>	The Authenticator PAE State will display one of the following: <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth, and N/A.</i>
<b>Backend_State</b>	The Backend Authentication State will display one of the following: <i>Request, Response, Success, Fail, Timeout, Idle, Initialize, and N/A.</i>
<b>Oper Dir</b>	The Operational Controlled Directions are <i>both</i> and <i>in</i> .
<b>PortStatus</b>	The status of the controlled port can be <i>authorized, unauthorized, or N/A.</i>

### Reauthenticate Port(s)

This window allows you to reauthenticate a port or group of ports. The Reauthenticate Port Table displays the current status of the port(s) once you have clicked **Apply**.

Open the **Security** folder, and then the **Port Access Entity** folder, and then the **PAE System Control** folder. Finally click on the **Reauthenticate Port(s)** link:



**Figure 4- 52. Reauthenticate Port window**

This window displays the following information:

Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a switch stack using that Switch's Unit ID. The number 15 indicates a Switch in standalone mode.
<b>From/To</b>	A consecutive group of ports may be configured starting with the selected port.
<b>Port</b>	The port number.
<b>MAC Address</b>	The MAC address of the switch where the port resides
<b>Auth State</b>	The Authenticator State will display one of the following: <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth, and N/A.</i>
<b>Backend_State</b>	The Backend State will display one of the following: <i>Request, Response, Success, Fail, Timeout, Idle, Initialize, and N/A.</i>
<b>OperDir</b>	The Operational Controlled Directions are <i>both</i> and <i>in</i> .
<b>PortStatus</b>	The status of the controlled port can be <i>authorized, unauthorized, or N/A.</i>

## Radius Server

The RADIUS feature of the Switch allows you to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

## Radius Server

Click the Radius Server link in the Radius Server folder under Port Access Entity in the Security folder under Configuration.

Succession	Radius Server	Auth UDP Port	Acct UDP Port	Status
First	10.1.4.78	1812	1813	Active
Second	20.5.68.27	1812	1813	Active
Third	200.56.8.23	1812	1813	Active

Figure 4- 53. Authentic Radius Server Setting window

The following parameters can be set:

Parameter	Description
<b>Succession</b>	RADIUS server settings index.
<b>Radius Server</b>	Type in the IP address of the RADIUS server.
<b>Authentic Port</b>	This is the UDP port on the RADIUS server that will be used to authenticate users. The default is <i>1812</i> .
<b>Accounting Port</b>	This is the UDP port on the RADIUS server that will be used to log authentication events. The default is <i>1813</i> .
<b>Key</b>	Type the shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used.
<b>Confirm Key</b>	Retype the Key information from the Key field above.

**Status**

This drop-down menu allows you to select *Valid* or *Invalid*.

---

## Chapter 6

# SNMP Management

## **SNMPV3**

**SNMP User Table**

**SNMP View Table**

**SNMP Group Table**

**SNMP Community Table**

**SNMP Host Table**

**SNMP Engine ID**

## **SNMPV3**

The GSW-1290 incorporates a flexible SNMP management for the Switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 windows to select the SNMP version used for specific tasks.

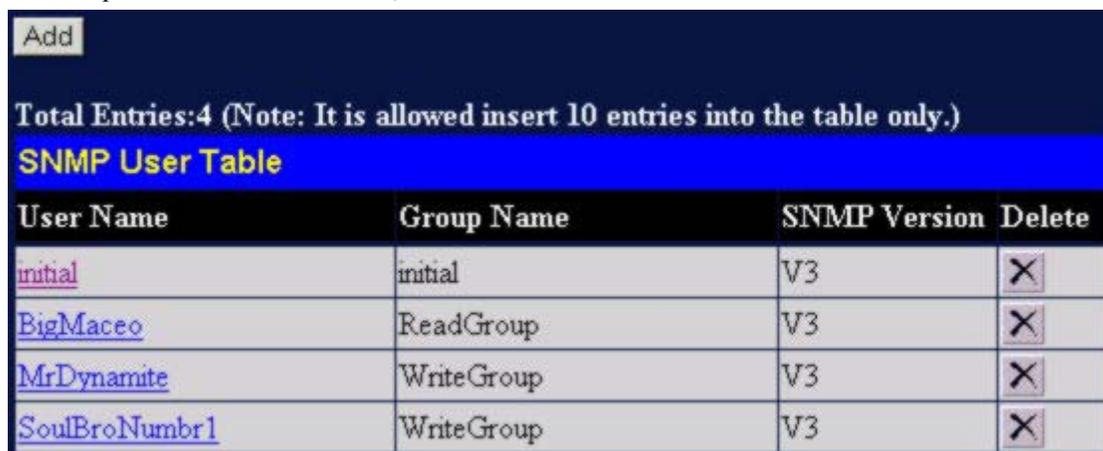
The GSW-1290 supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The SNMP version used to monitor and control the Switch can be specified by the administrator. The three versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP settings are configured using the windows located on the **SNMP V3** folder of the web manager. Workstations on the network that are allowed SNMP privileged access to the Switch can be restricted with the **Security IP Management** window (located in the **Security** folder under **Trusted Host**).

## **SNMP User Table**

The SNMP User Table displays all of the SNMP User's currently configured on the Switch.

Open the **Management** folder and then the **SNMPV3** folder. Finally click on the **SNMP User Table** link. This will open the **SNMP User Table**, as shown below.



The screenshot shows a web interface window titled "SNMP User Table". At the top left is an "Add" button. Below it, the text reads "Total Entries:4 (Note: It is allowed insert 10 entries into the table only.)". The main content is a table with the following data:

User Name	Group Name	SNMP Version	Delete
<a href="#">initial</a>	initial	V3	<input type="checkbox"/>
<a href="#">BigMaceo</a>	ReadGroup	V3	<input type="checkbox"/>
<a href="#">MrDynamite</a>	WriteGroup	V3	<input type="checkbox"/>
<a href="#">SoulBroNumbr1</a>	WriteGroup	V3	<input type="checkbox"/>

**Figure 6- 1. SNMP User Table window**

To delete an existing SNMP User Table entry, click on the X icon below the **Delete** heading corresponding to the entry you want to delete.

## SNMP User Table Display

To display the detailed entry for a given user, click on the blue **User Name**. This will open the **SNMP User Table Display** window, as shown below.

SNMP User Table Display	
User Name	BigMaceo
Group Name	ReadGroup
SNMP Version	V3
Auth-Protocol	None
Priv-Protocol	None
<a href="#">Show All SNMP User Table Entries</a>	

Figure 6- 2. SNMP User Table Display window

The following parameters are displayed:

Parameter	Description
<b>User Name</b>	An alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
<b>Group Name</b>	This name is used to specify the SNMP group created can request SNMP messages.
<b>SNMP Version</b>	V1 – Indicates that SNMP version 1 will be used. V2 – Indicates that SNMP version 2 will be used. V3 – Indicates that SNMP version 3 will be used.
<b>Auth-Protocol</b>	None – Indicates that no authorization protocol is in use. MD5 – Indicates that the HMAC-MD5-96 authentication level will be used. SHA – Indicates that the HMAC-SHA authentication protocol will be used.
<b>Priv-Protocol</b>	None – Indicates that no authorization protocol is in use. DES – Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.

To add a new entry to the **SNMP User Table Configuration**, click on the **Add** button on the **SNMP User Table** window. This will open the **SNMP User Table Configuration** window, as shown below.

## SNMP User Table Configuration

**Figure 6- 3. SNMP User Table Configuration menu**

The following parameters can set:

Parameter	Description
<b>User Name</b>	An alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
<b>Group Name</b>	This name is used to specify the SNMP group created can request SNMP messages.
<b>SNMP V3 Encryption</b>	Check this to specify that SNMP version 3 will be used.
<b>Auth-Protocol</b>	<i>MD5</i> – Specifies that the HMAC-MD5-96 authentication level will be used. <i>SHA</i> – Specifies that the HMAC-SHA authentication protocol will be used.
<b>Priv-Protocol</b>	<i>None</i> – Specifies that no authorization protocol is in use. <i>DES</i> – Specifies that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.

## SNMP View Table

The SNMP View Table is used to assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager.

View Name	Subtree	View Type	Delete
restricted	1.3.6.1.2.1.1	Included	X
restricted	1.3.6.1.2.1.11	Included	X
restricted	1.3.6.1.6.3.10.2.1	Included	X
restricted	1.3.6.1.6.3.11.2.1	Included	X
restricted	1.3.6.1.6.3.15.1.1	Included	X
CommunityView	1	Included	X
CommunityView	1.3.6.1.6.3	Excluded	X
CommunityView	1.3.6.1.6.3.1	Included	X

Figure 6- 4. SNMP View Table window

To delete an existing **SNMP View Table** entry, click the **X** button listed under Delete on the far left that corresponds to View Name. To create a new entry, click the **Add** button, a separate window will appear.

## SNMP View Table Configuration

Figure 6- 5. SNMP View Table Configuration window

The SNMP Group created with this table maps SNMP users (identified in the **SNMP User Table** window) to the views created in the previous window.

The following parameters can set:

Parameter	Description
<b>View Name</b>	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
<b>Subtree OID</b>	Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
<b>View Type</b>	Select <i>Included</i> to include this object in the list of objects that an SNMP manager can access. Select <i>Excluded</i> to exclude this object from the list.

manager can access. Select *Excluded* to exclude this object from the list of objects that an SNMP manager can access.

## SNMP Group Table

An SNMP Group created with this table maps SNMP users (identified in the **SNMP User Table** window) to the views created in the previous window.

Add			
Total Entries:9 (Note: It is allowed insert 30 entries into the table only.)			
SNMP Group Table			
Group Name	Security Model	Security Level	Delete
<a href="#">public</a>	SNMPv1	NoAuthNoPriv	X
<a href="#">public</a>	SNMPv2	NoAuthNoPriv	X
<a href="#">initial</a>	SNMPv3	NoAuthNoPriv	X
<a href="#">private</a>	SNMPv1	NoAuthNoPriv	X
<a href="#">private</a>	SNMPv2	NoAuthNoPriv	X
<a href="#">ReadGroup</a>	SNMPv1	NoAuthNoPriv	X
<a href="#">ReadGroup</a>	SNMPv2	NoAuthNoPriv	X
<a href="#">WriteGroup</a>	SNMPv1	NoAuthNoPriv	X
<a href="#">WriteGroup</a>	SNMPv2	NoAuthNoPriv	X

Figure 6- 6. SNMP Group Table window

To delete an existing SNMP Group Table entry, click the corresponding X icon under the **Delete** heading.

## SNMP Group Table Display

To display the current settings for an existing SNMP Group Table entry, click the blue link for the entry under the Group Name heading.

SNMP Group Table Display	
Group Name	ReadGroup
Read View Name	CommunityView
Write View Name	
Notify View Name	CommunityView
Security Model	SNMPv1
Security Level	NoAuthNoPriv
<a href="#">Show All SNMP Group Table Entries</a>	

Figure 6- 7. SNMP Group Table Display window

To add a new entry to the Switch’s SNMP Group Table, click the **Add** button in the upper left-hand corner of the **SNMP Group Table** window. This will open the **SNMP Group Table Configuration** window, as shown below.

## SNMP Group Table Configuration

Figure 6- 8. SNMP Group Table Configuration window

The following parameters can be set:

Parameter	Description
<b>Group Name</b>	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
<b>Read View Name</b>	This name is used to specify the SNMP group created can request SNMP messages.
<b>Write View Name</b>	Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.
<b>Notify View Name</b>	Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.
<b>Security Model</b>	<p><i>SNMPv1</i> – Specifies that SNMP version 1 will be used.</p> <p><i>SNMPv2</i> – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p><i>USM</i> – (User-based Security Module) Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network.</p>
<b>Security Level</b>	<p><i>NoAuthNoPriv</i> – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>AuthNoPriv</i> – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>AuthPriv</i> – Specifies that authorization will be required, and that packets</p>

sent between the Switch and a remote SNMP manger will be encrypted.

## SNMP Community Table

Use this table to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent.

An MIB view that defines the subset of all MIB objects that will be accessible to the SNMP community.

Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

Community Name	View Name	Access Right	Delete
private	CommunityView	Read_Write	X
public	CommunityView	Read_Only	X

Figure 6- 9. SNMP Community Table Configuration window

The following parameters can set:

Parameter	Description
<b>Community Name</b>	Type an alphanumeric string of up to 33 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
<b>View Name</b>	Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
<b>Access Right</b>	<p><i>Read_Only</i> – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the Switch.</p> <p><i>Read_Write</i> – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the Switch.</p>



## SNMP Host Table

Use the **SNMP Host Table** to set up SNMP trap recipients.

Open the **Management** folder, and then the **SNMPV3** folder. Finally, click on the **SNMP Host Table** link. This will open the **SNMP Host Table** window, as shown below.

To delete an existing SNMP Host Table entry, click the corresponding **X** icon under the **Delete** heading.

To display the current settings for an existing SNMP Group Table entry, click the blue link for the entry under the Host IP Address heading.

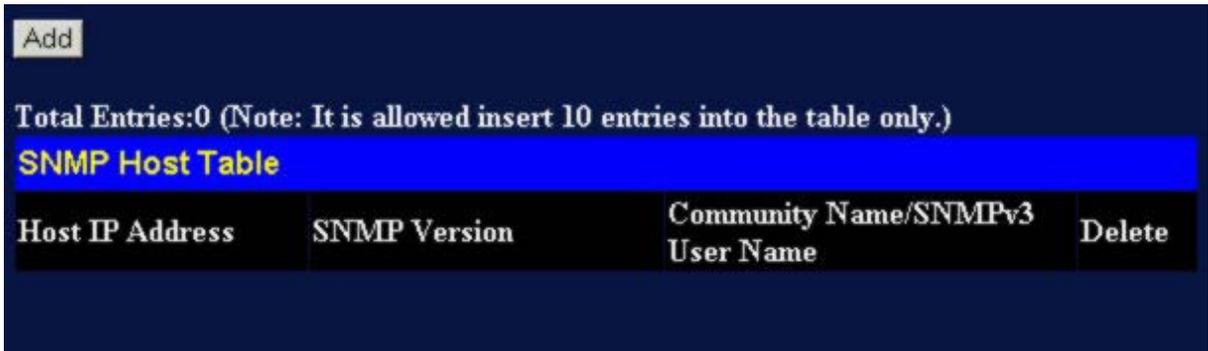


Figure 6- 10. SNMP Host Table window

To add a new entry to the Switch’s SNMP Group Table, click the Add button in the upper left-hand corner of the SNMP Host Table window. This will open the SNMP Host Table Configuration window, as shown below.

## SNMP Host Table Configuration

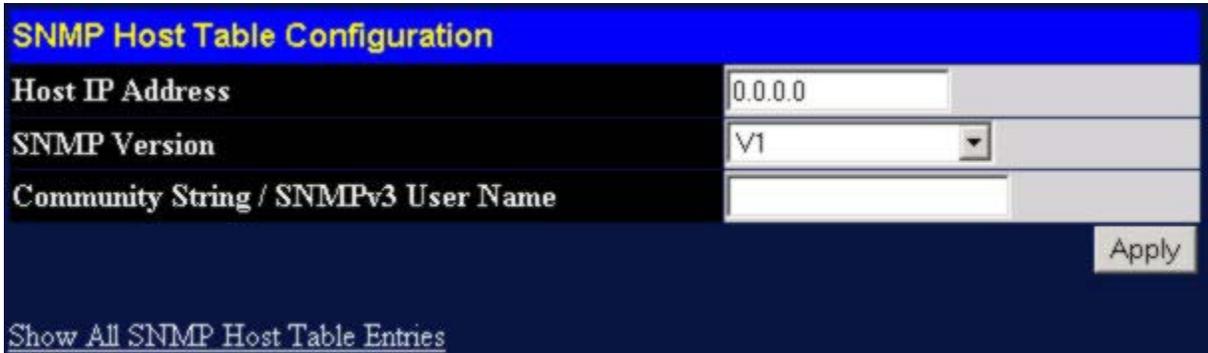


Figure 6- 11. SNMP Host Table Configuration window

The following parameters can set:

Parameter	Description
<b>IP Address</b>	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
<b>SNMP Version</b>	V1 – Specifies that SNMP version 1 will be used. V2c – Specify that SNMP version 2c will be used. V3-NoAuth-NoPriv – Specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level. V3-Auth-NoPriv – Specify that the SNMP version 3 will be used, with an Auth-NoPriv security level. V3-Auth-Priv – Specify that the SNMP version 3 will be used, with an Auth-Priv security level.

**Community String or SNMP V3 User Name**      Type in the community string or SNMP V3 user name as appropriate.

---

## SNMP Engine ID

The Engine ID is a unique identifier used for SNMP V3 implementations. This is an alphanumeric string used to identify the SNMP engine on the Switch.

To display the Switch's SNMP Engine ID, open the **Management** folder, and then the **SNMPV3** folder. Finally, click on the **SNMP Engine ID** link. This will open the **SNMP Engine ID Configuration** window, as shown below.



**Figure 6- 12. SNMP Engine ID Configuration window**

To change the Engine ID, type the new Engine ID in the space provided and click the **Apply** button.

## Chapter 7

# Network and System Monitoring

*Port Utilization*

*Packets*

*Received (RX)*

*Unicast / Multicast / Broadcast (RX)*

*Transmitted (TX)*

*Errors*

*Received (RX)*

*Transmitted (TX)*

*Size*

*Packet Size*

*MAC Address*

*Switch History*

*IGMP Snooping*

*Browse Router Port*

*VLAN Status*

*Session Table*

*Authenticator State*

The GSW-1290 provides extensive network monitoring capabilities that can be viewed from the **Monitoring** folder.



## Port Utilization

The **Port Utilization** window displays the percentage of the total available bandwidth being used on the port.

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

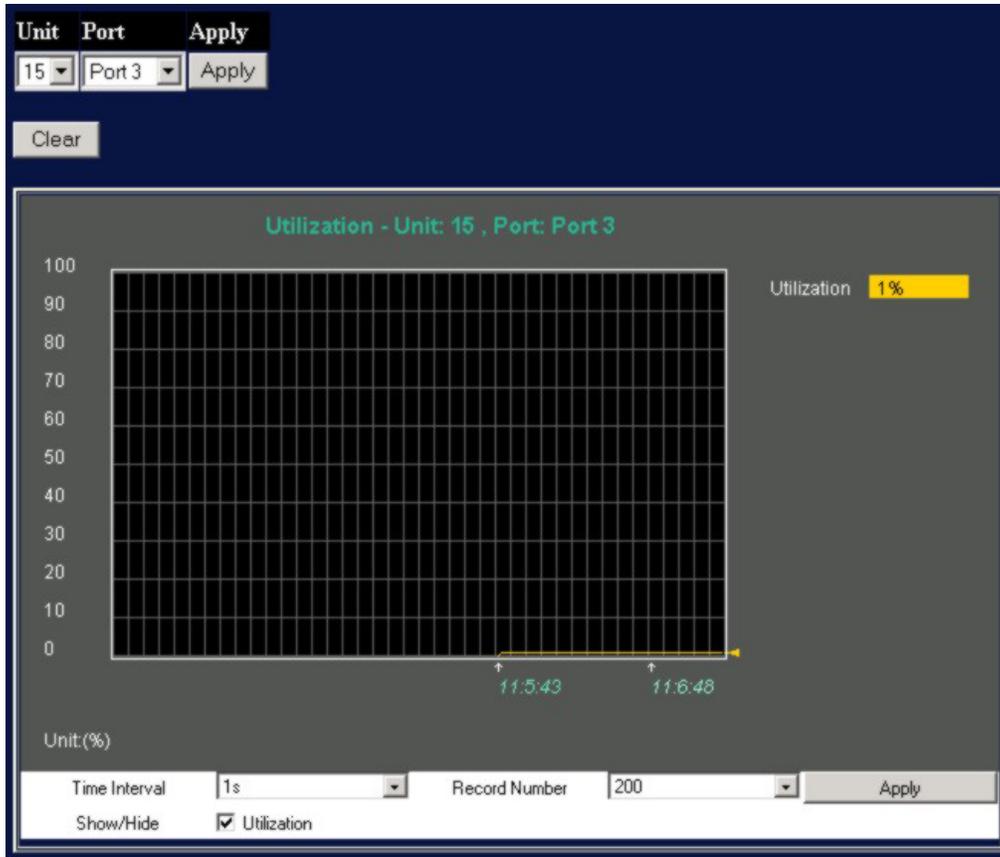


Figure 7- 1. Utilization window

The following field can be set:

Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a Switch stack using that Switch's Unit ID. The number 15 indicates a Switch in standalone mode.
<b>Port</b>	Allows you to specify a port to monitor from the Switch selected above.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<b>Time Interval &lt;1s&gt;</b>	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
<b>Record Number &lt;200&gt;</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
<b>Show/Hide</b>	Check to display Utilization.

## Packets

Various statistics can be viewed as either a line graph or a table:

*Received Packets*

*Received Unicast/Multicast/Broadcast Packets*

*Transmitted Packet*

### Received Packets

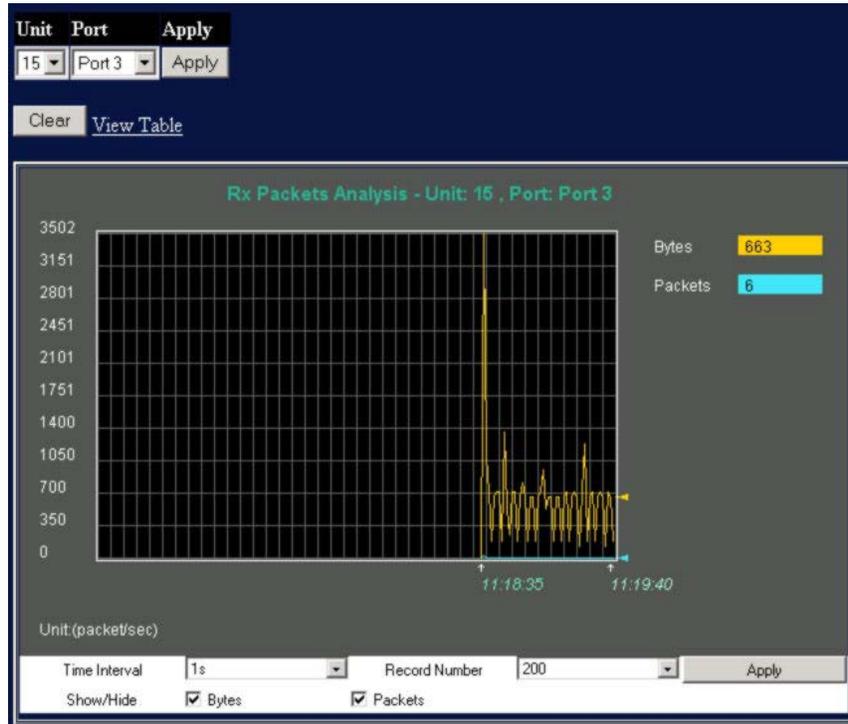


Figure 7- 2. Rx Packets Analysis (line graph for Bytes & Packets) window

View LineChart

Unit: 15 , Port: Port 3 | Time Interval: 1s | OK

Rx Packets	Total	Rate(1/Sec)	Max Rate
Bytes	40263572	128	3502
Packets	310025	2	30

Rx Packets	Total	Rate(1/Sec)	Max Rate
Unicast	14103	2	30
Multicast	54684	0	0
Broadcast	241238	0	1

Tx Packets	Total	Rate(1/Sec)	Max Rate
Bytes	8693148	461	48715
Packets	78942	3	45

Figure 7- 3. Rx Packets Analysis (table for Bytes & Packets) window

Select the desired Switch using the Unit drop-down menu and the desired port using the Port drop-down menu. The Time Interval field sets the interval at which the error statistics are updated.

The following field can be set:

Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a Switch stack using that Switch's Unit ID. 15 indicates a Switch in standalone mode.
<b>Port</b>	Allows you to specify a port to monitor – from the Switch selected above.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<b>View Table</b>	Clicking this button instructs the Switch to display a table rather than a line graph.
<b>View Line Chart</b>	Clicking this button instructs the Switch to display a line graph rather than a table.
<b>Bytes</b>	Counts the number of bytes received on the port.
<b>Packets</b>	Counts the number of packets received on the port.
<b>Time Interval &lt;1s&gt;</b>	The time between updates received from the Switch, in seconds. The default is 1s.
<b>Record Number &lt;200&gt;</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
<b>Show/Hide</b>	Check whether to display Bytes and Packets.

### Received Unicast/Multicast/Broadcast Packets

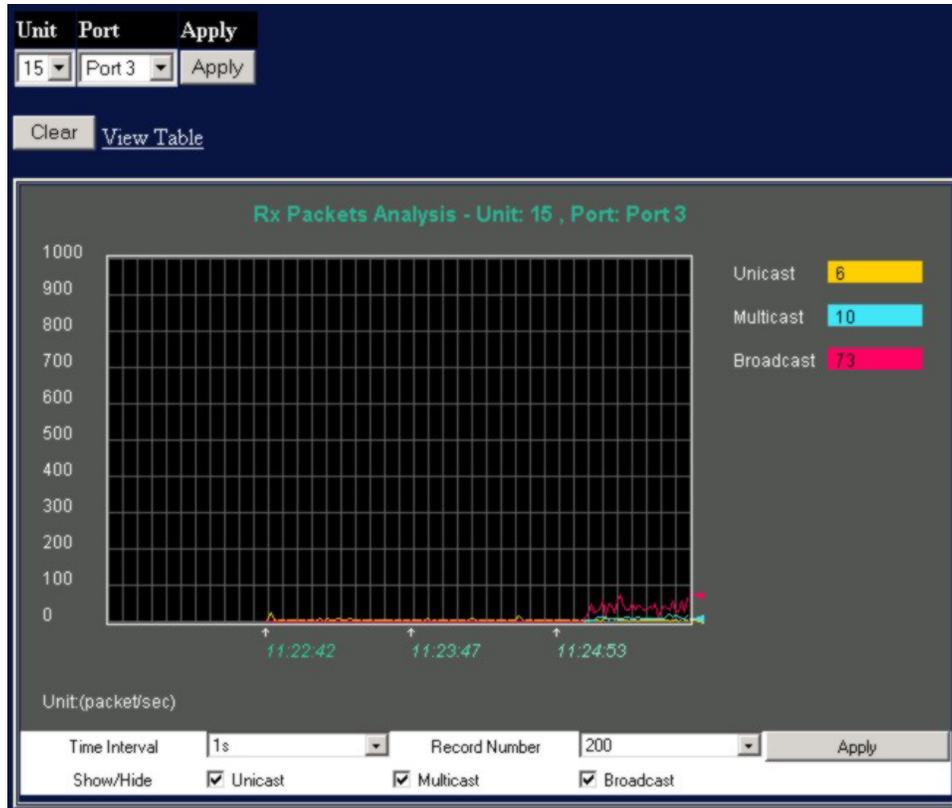
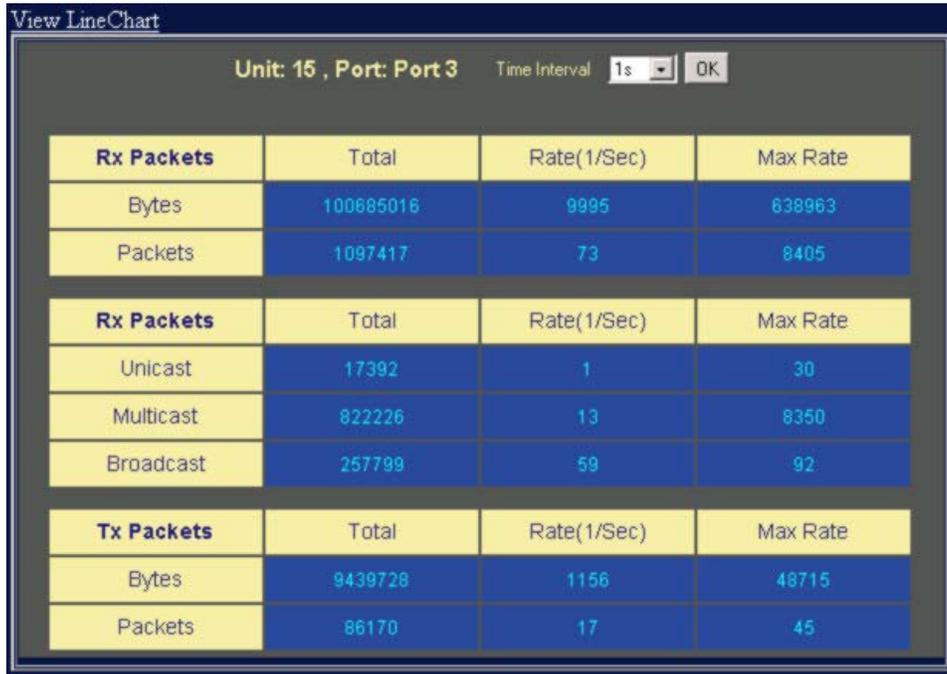


Figure 7- 4. Rx Packets Analysis (line graph for Unicast, Multicast, & Broadcast) window



**Figure 7- 5. Rx Packets Analysis (table for Unicast, Multicast, & Broadcast) window**

Select the desired Switch using the Unit drop-down menu and the desired port using the Port drop-down menu. The Time Interval field sets the interval at which the error statistics are updated.

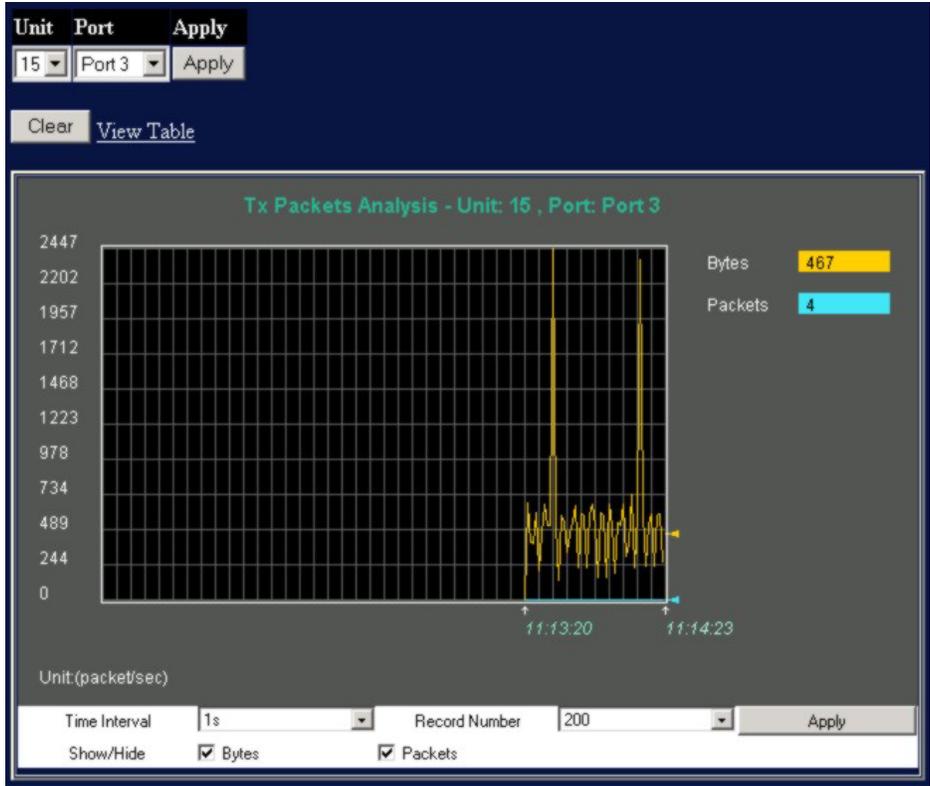
The following fields can be set:

Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a Switch stack using that Switch's Unit ID. The number 15 indicates a Switch in standalone mode.
<b>Port</b>	Allows you to specify a port to monitor – from the Switch selected above.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<b>View Table</b>	Clicking this button instructs the Switch to display a table rather than a line graph.
<b>View Line Chart</b>	Clicking this button instructs the Switch to display a line graph rather than a table.
<b>Unicast</b>	Counts the total number of good packets that were received by a unicast address.
<b>Multicast</b>	Counts the total number of good packets that were received by a multicast address.
<b>Broadcast</b>	Counts the total number of good packets that were received by a broadcast address.
<b>Time Interval &lt;1s&gt;</b>	The time between updates received from the Switch, in seconds. The default is 1s.
<b>Record Number &lt;200&gt;</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 200.

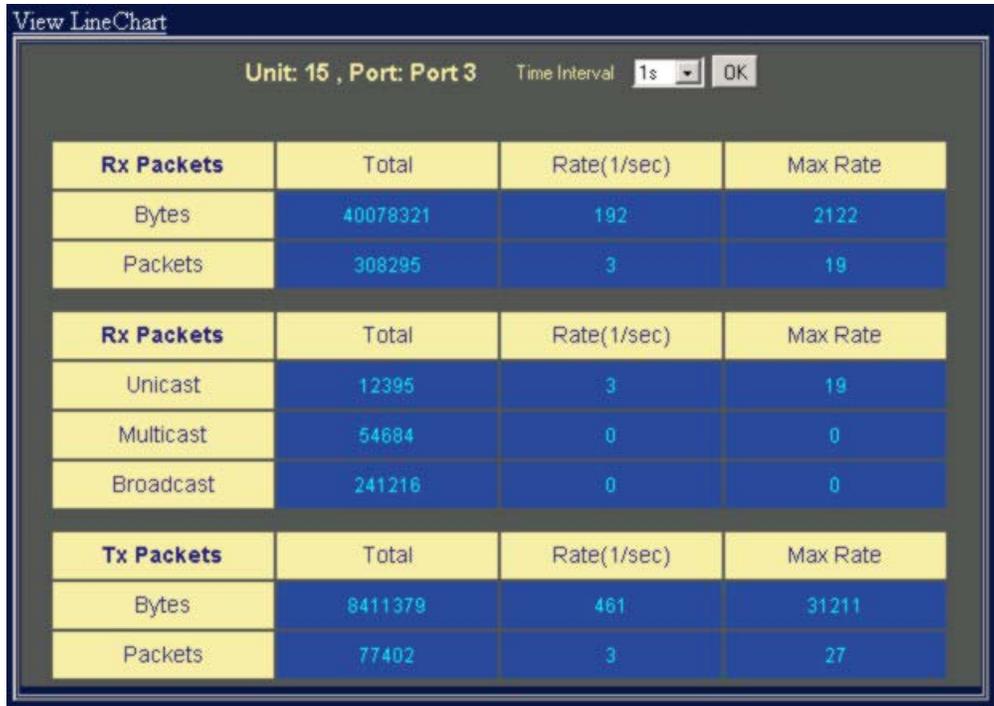
**Show/Hide**

Check whether or not to display Multicast, Broadcast, and Unicast Packets.

**Transmitted Packets**



**Figure 7- 6. Tx Packets Analysis (graph for Bytes & Packets) window**



**Figure 7- 7. Tx Packets Analysis (table for Bytes & Packets) window**

Select the desired Switch using the Unit drop-down menu and the desired port using the Port drop-down menu. The Time Interval field sets the interval at which the error statistics are updated.

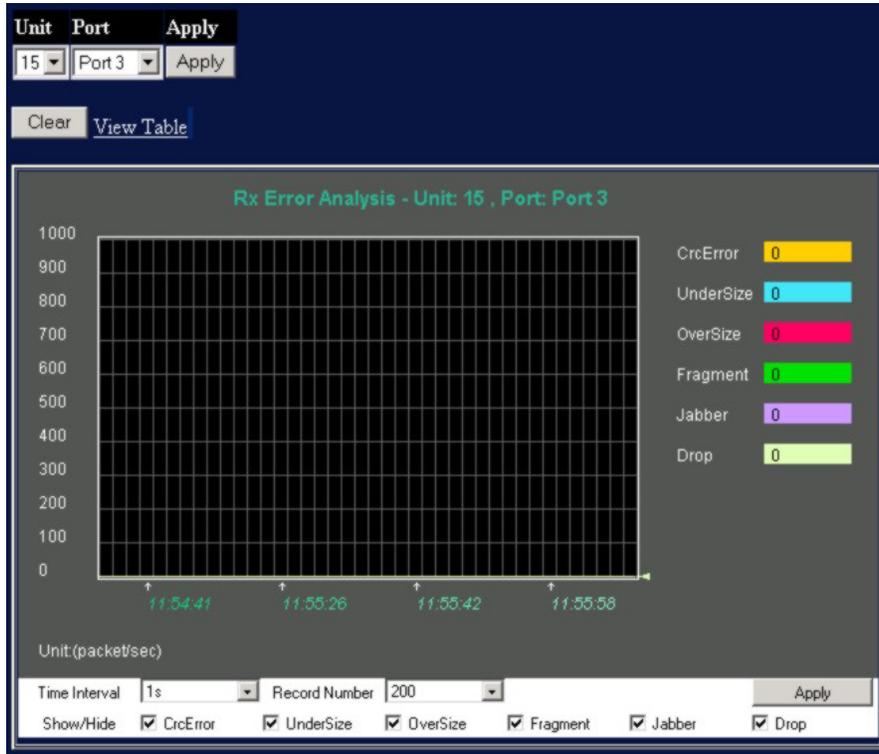
The following fields can be set or are displayed:

Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a Switch stack using that Switch's Unit ID. The number 15 indicates a Switch in standalone mode.
<b>Port</b>	Allows you to specify a port to monitor – from the Switch selected above.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<b>View Table</b>	Clicking this button instructs the Switch to display a table rather than a line graph.
<b>View Line Chart</b>	Clicking this button instructs the Switch to display a line graph rather than a table.
<b>Bytes</b>	Counts the number of bytes successfully sent from the port.
<b>Packets</b>	Counts the number of packets successfully sent on the port.
<b>Time Interval &lt;1s&gt;</b>	The time between updates received from the Switch, in seconds. The default is 1s.
<b>Record Number &lt;200&gt;</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
<b>Show/Hide</b>	Check whether to display Bytes and Packets.

## Errors

Various statistics can be viewed as either a line graph or a table:

**Received Errors**  
**Transmitted Errors**  
**Received Errors**



**Figure 7- 8. Rx Error Analysis (graph)**

View LineChart

Unit: 15 , Port: Port 3 Time Interval: 1s OK

Rx Error	Total	Rate(1/Sec)	Max Rate
CrcError	0	0	0
UnderSize	0	0	0
OverSize	0	0	0
Fragment	0	0	0
Jabber	0	0	0
Drop	372	0	0

**Figure 7- 9. Rx Error Analysis (table)**

Select the desired Switch using the Unit drop-down menu and the desired port using the Port drop-down menu. The Time Interval field sets the interval at which the error statistics are updated.

The following fields can be set or are displayed:

Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a Switch stack using that Switch's Unit ID. 15 indicates a Switch in standalone mode.
<b>Port</b>	Allows you to specify a port to monitor – from the Switch selected above.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<b>View Table</b>	Clicking this button instructs the Switch to display a table rather than a line graph.
<b>View Line Chart</b>	Clicking this button instructs the Switch to display a line graph rather than a table.
<b>CrcError</b>	Counts otherwise valid frames that did not end on a byte (octet) boundary.
<b>UnderSize</b>	The number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersize frames usually indicate collision fragments, a normal network occurrence.
<b>OverSize</b>	Counts packets received that were longer than 1518 octets, or if a VLAN frame 1522 octets, and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.
<b>Fragment</b>	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
<b>Jabber</b>	The number of frames with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522.
<b>Drop</b>	The number of frames that are dropped by this port since the last Switch reboot.
<b>Time Interval &lt;1s&gt;</b>	The time between updates received from the Switch, in seconds. The default is 1s.
<b>Record Number &lt;200&gt;</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
<b>Show/Hide</b>	Check whether or not to display CrcError, UnderSize, OverSize, Fragment, Jabber, and Drop errors.

---

## Transmitted Errors

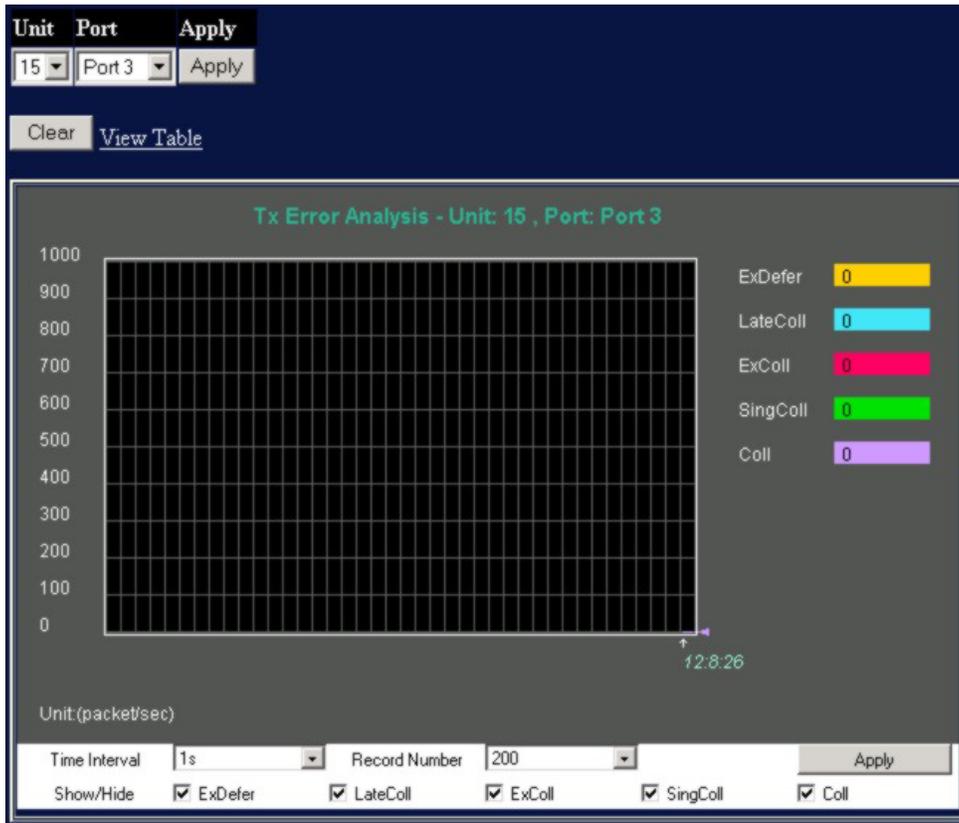


Figure 7- 10. Tx Error Analysis (graph)

View LineChart

Unit: 15 , Port: Port 3    Time Interval: 1s    OK

Tx Error	Total	Rate(1/Sec)	Max Rate
ExDefer	0	0	0
LateColl	0	0	0
ExColl	0	0	0
SingColl	0	0	0
Coll	0	0	0

Figure 7- 11. Tx Error Analysis (table)

Select the desired Switch using the Unit drop-down menu and the desired port using the Port drop-down menu. The Time Interval field sets the interval at which the error statistics are updated.

The following fields can be set:

Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a Switch stack using that Switch's Unit ID. The number 15 indicates a Switch in standalone mode.
<b>Port</b>	Allows you to specify a port to monitor – from the Switch selected above.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.
<b>View Table</b>	Clicking this button instructs the Switch to display a table rather than a line graph.
<b>View Line Chart</b>	Clicking this button instructs the Switch to display a line graph rather than a table.
<b>ExDefer (Excessive Deferral)</b>	The number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.
<b>LateColl (Late Collision)</b>	Late Collisions. The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
<b>ExColl (Excessive Collision)</b>	Excessive Collisions. The number of frames for which transmission failed due to excessive collisions.
<b>SingColl (Single Collision)</b>	Single Collision Frames. The number of successfully transmitted frames for which transmission is inhibited by more than one collision.
<b>Coll (Collision)</b>	An estimate of the total number of collisions on this network segment.
<b>Time Interval &lt;1s&gt;</b>	The time between updates received from the Switch, in seconds. The default is 1s.
<b>Record Number &lt;200&gt;</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
<b>Show/Hide</b>	Check whether to display ExDefer, LateColl, ExColl, SingColl, and Coll errors.

## Packet Size

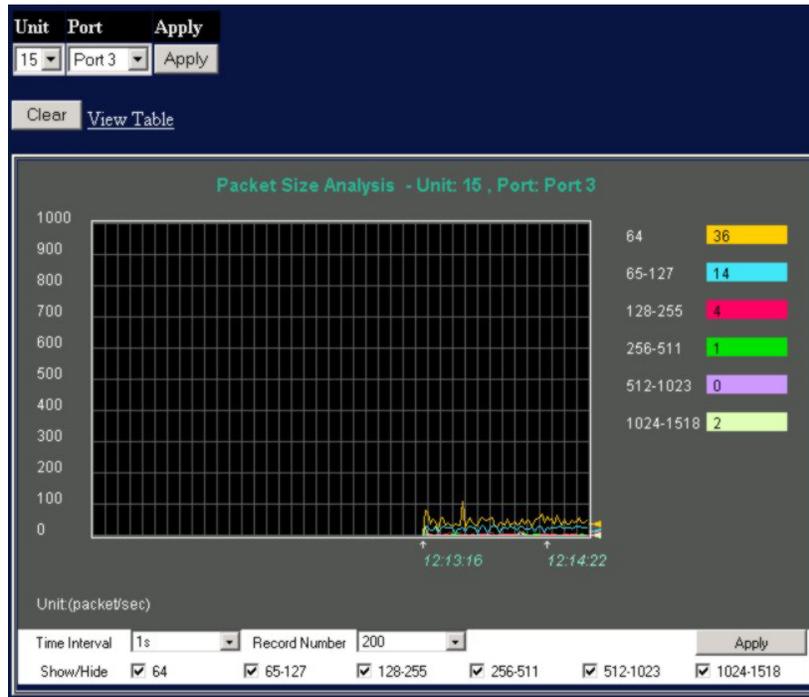


Figure 7- 12. Packet Size Analysis (line graph) window

View Line Chart

Unit: 15 , Port: Port 3 Time Interval 1s OK

Packet Size	Total	Rate(1/Sec)	Max Rate
64	2281322	55	4212
65-127	2992209	27	5692
128-255	25711	2	17
256-511	8186	3	15
512-1023	655	0	8
1024-1518	20084	2	43

Figure 7- 13. Packet Size Analysis (table) window

Select the desired Switch using the Unit drop-down menu and the desired port using the Port drop-down menu. The Time Interval field sets the interval at which the error statistics are updated.

The following field can be set:

Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a Switch stack using that Switch's Unit ID. 15 indicates a Switch in standalone mode.
<b>Port</b>	Allows you to specify a port to monitor – from the Switch selected above.
<b>Clear</b>	Clicking this button clears all statistics counters on this window.

<b>View Table</b>	Clicking this button instructs the Switch to display a table rather than a line graph.
<b>View Line Chart</b>	Clicking this button instructs the Switch to display a line graph rather than a table.
<b>64</b>	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
<b>65-127</b>	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
<b>128-255</b>	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
<b>256-511</b>	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
<b>512-1023</b>	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
<b>1024-1518</b>	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
<b>Time Interval &lt;1s&gt;</b>	The time between updates received from the Switch, in seconds. The default is 1s.
<b>Record Number &lt;200&gt;</b>	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
<b>Show/Hide</b>	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.

---

## **MAC Address**

This allows the Switch's dynamic MAC address forwarding table to be viewed. When the Switch learns an association between a MAC address and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.

**MAC Address Table**

VID	MAC Address	Unit	Port	Learned
1	00-00-00-00-00-01	15	3	Permanent
1	00-00-00-00-00-03	15	3	Permanent
1	00-00-48-af-62-23	15	3	Dynamic
1	00-00-55-46-03-00	15	3	Dynamic
1	00-00-55-56-67-78	15	3	Dynamic
1	00-00-5e-00-01-0a	15	3	Dynamic
1	00-00-5e-00-01-5f	15	3	Dynamic
1	00-00-e2-34-22-89	15	3	Dynamic
1	00-00-e2-64-e3-3e	15	3	Dynamic
1	00-01-02-03-04-00	15	3	Dynamic
1	00-01-02-03-04-01	15	3	Dynamic
1	00-01-02-03-92-17	15	3	Dynamic
1	00-01-02-03-92-27	15	3	Dynamic
1	00-01-02-03-92-58	15	3	Dynamic
1	00-01-06-30-10-63	15	3	Dynamic
1	00-01-30-12-13-02	15	3	Dynamic
1	00-01-33-26-33-00	15	3	Dynamic
1	00-02-06-12-34-56	15	3	Dynamic
1	00-03-09-18-10-01	15	3	Dynamic
1	00-03-11-04-10-00	15	3	Dynamic

Total Entries: 315

Figure 7- 14. MAC Address Table window

The following fields can be set:

Parameter	Description
<b>VLAN ID</b>	Allows you to enter a VLAN ID.
<b>MAC Address</b>	Allows you to specify a MAC Address.
<b>Unit - Port</b>	Enter the desired switch unit and port number.

## Switch History

The **Switch History** window displays the Switch's history log, as compiled by the Switch's management agent.

Switch History		
Sequence	Time	Log Text
23629	0 days 02:46:14	Topology changed
23628	0 days 02:46:13	Topology changed
23627	0 days 02:46:12	Topology changed
23626	0 days 02:46:11	Topology changed
23625	0 days 02:46:10	Topology changed
23624	0 days 02:46:09	Topology changed
23623	0 days 02:46:08	Topology changed
23622	0 days 02:46:07	Topology changed
23621	0 days 02:46:06	Topology changed
23620	0 days 02:46:05	Topology changed
23619	0 days 02:46:04	Topology changed
23618	0 days 02:46:03	Topology changed
23617	0 days 02:46:02	Topology changed
23616	0 days 02:46:01	Topology changed
23615	0 days 02:46:00	Topology changed
23614	0 days 02:45:59	Topology changed
23613	0 days 02:45:58	Topology changed
23612	0 days 02:45:57	Topology changed
23611	0 days 02:45:56	Topology changed
23610	0 days 02:45:55	Topology changed
Clear		Next

**Figure 7- 15. Switch History window**

The Switch can record event information in its own logs, to designated SNMP trap receiving stations, and to the PC connected to the console manager. Clicking **Next** at the bottom of the window will allow you to display all the switch Trap Logs.

The information is described as follows:

Parameter	Description
<b>Sequence</b>	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
<b>Time</b>	Displays the time in days, hours, and minutes since the Switch was last restarted.
<b>Log Text</b>	Displays text describing the event that triggered the history log entry.

## IGMP Snooping

This allows the Switch's IGMP Snooping table to be viewed. IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch. The number of IGMP reports that were snooped is also displayed in the Reports field.

Vid :	<input type="text" value="1"/>	<input type="button" value="Search"/>		
Total Entries : 4				
<b>IGMP Snooping Table</b>				
VLAN ID	Multicast Group	MAC Address	Queries	Reports
1	0.0.0.0	00:00:00:00:00:00	Disabled	0
Unit	Port Map			
15				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

Figure 7- 16. IGMP Snooping Table window

The following field can be set:

Parameter	Description
<b>Multicast Group</b>	The IP address of the multicast group.
<b>MAC Address</b>	The MAC address of the multicast group.
<b>Reports</b>	The total number of reports received for this group.

## Browse Router Port

This displays which of the Switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by **S**. A router port that is dynamically configured by the Switch is designated by **D**.

Browse Router Port																									
VLAN ID													VLAN Name												
1													default												
Units	Ports																								
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
15																									
1																									
2																									
3																									
4																									
5																									
6																									
7																									
8																									
9																									
10																									
11																									
12																									

Figure 7- 17. Browse Router Port window



## Authenticator State

The **Authenticator Status** window is found in the **Monitoring** folder. This window allows you to view the setting/status of the Auth PAE State, Backend\_State, and Port Status.

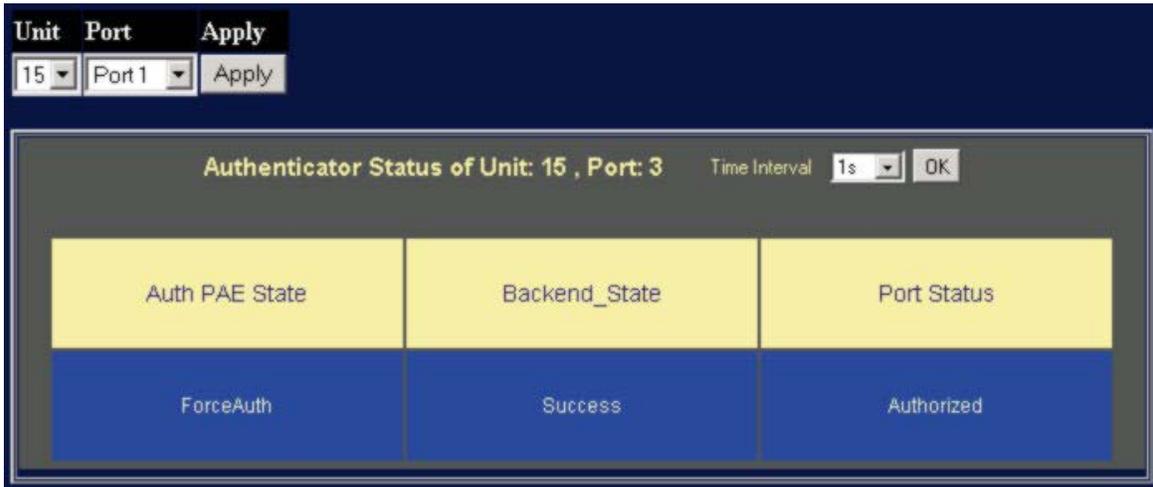


Figure 7- 20. Authenticator Status window

## Chapter 8

# System Maintenance

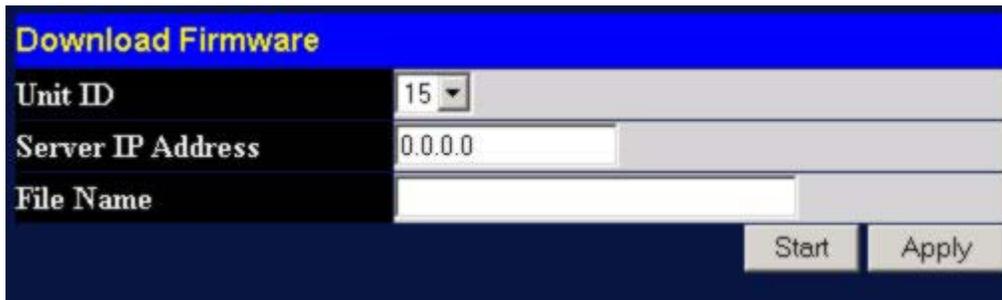
**TFTP Services**  
**Download Firmware**  
**Download Configuration File**  
**Save Settings**  
**Save History Log**  
**PING Test**  
**Save Changes**  
**Factory Reset**  
**Restart System**  
**Logout**

## TFTP Services

Trivial File Transfer Protocol (TFTP) services allow the Switch firmware to be upgraded by transferring a new firmware file from a TFTP server to the Switch. A configuration file can also be loaded into the Switch from a TFTP server, Switch settings can be saved to the TFTP server, and a history log can be uploaded from the Switch to the TFTP server.

### Download Firmware

To update the Switch's firmware, click on the Maintenance folder and then the TFTP Service folder and then the Download Firmware link:



**Figure 8- 1. Download Firmware window**

Use the Unit ID drop-down menu to select which Switch of a Switch stack you want to update the firmware on. This allows the selection of a particular Switch from a Switch stack if you have installed the optional stacking module and have properly interconnected the Switches. The number 15 indicates a Switch in standalone mode.

Enter the IP address of the TFTP server in the Server IP Address field.

The TFTP server must be on the same IP subnet as the Switch.

Enter the path and the filename to the firmware file on the TFTP server. The TFTP server must be running TFTP server software to perform the file transfer. TFTP server software is a part of many network management software packages – such as NetSight, or can be obtained as a separate program.

Click **Start** to record the IP address of the TFTP server.

## Download Configuration File

To download a configuration file from a TFTP server, click on the **Maintenance** folder and then the **TFTP Service** folder and then the **Download Configuration File** link:



**Figure 8- 2. Use Configuration File on Server window**

Enter the IP address of the TFTP server and specify the location of the Switch configuration file on the TFTP server.

Click **Apply** to record the IP address of the TFTP server.

Click **Start** to initiate the file transfer.

## Save Settings

To upload the Switch settings to a TFTP server, click on the **Maintenance** folder and then the **TFTP Service** folder and then the **Save Settings** link:



**Figure 8- 3. Save Settings To TFTP Server window**

Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server. Click **Apply** to make the changes current.

Click **Start** to initiate the file transfer.

## Save History Log

To upload the Switch history log file to a TFTP server, click on the **Maintenance** folder and then the **TFTP Service** folder and then the **Save History Log** link:



**Figure 8- 4. Save Switch History To TFTP Server window**

Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server. Click **Apply** to make the changes current. Click **Start** to initiate the file transfer.

## Ping Test

PING is a small program that sends data packets to the IP address you specify. The destination node then returns the packets to the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.



Figure 8- 5. Ping Test window

The **Infinite times** checkbox, in the **Number of Repetitions** field, tells PING to keep sending data packets to the specified IP address until the program is stopped.

## Save Changes

The GSW-1290 has two levels of memory; normal RAM and non-volatile or NV-RAM. Configuration changes are made effective clicking the **Apply** button. When this is done, the settings will be immediately applied to the Switching software in RAM, and will immediately take effect.

Some settings, though, require you to restart the Switch before they will take effect. Restarting the Switch erases all settings in RAM and reloads the stored settings from the NV-RAM. Thus, it is necessary to save all setting changes to NV-RAM before rebooting the Switch.

To retain any configuration changes permanently, click the **Save Configuration** button in window below.

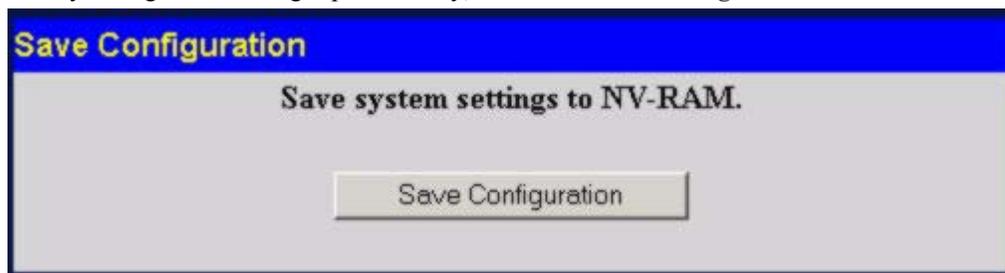


Figure 8- 6. Save Configuration window

Once the Switch configuration settings have been saved to NV-RAM, they become the default settings for the Switch. These settings will be used every time the Switch is rebooted.

## Factory Reset

The Factory Reset function has several options when resetting the Switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.

Please note that the Reset System option will enter the factory default parameters into the Switch's non-volatile RAM, and then restart the Switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. Reset System will return the Switch's configuration to the state it was when it left the factory.

Reset gives the option of retaining the Switch's User Accounts and History Log while resetting all other configuration parameters to their factory defaults. If the Switch is reset with this option enabled, and Save Changes is not executed, the Switch will return to the last saved configuration when rebooted.

The Reset Config option will reset all of the Switch's configuration parameters to their factory defaults, without saving these default values to the Switch's non-volatile RAM. If the Switch is reset with this option enabled, and Save Changes is not executed, the Switch will return to the last saved configuration when rebooted.

In addition, the Reset System option is added to reset all configuration parameters to their factory defaults, save these parameters to the Switch's non-volatile RAM, and then restart the Switch. This option is equivalent to Reset Config (above) followed by Save Changes.

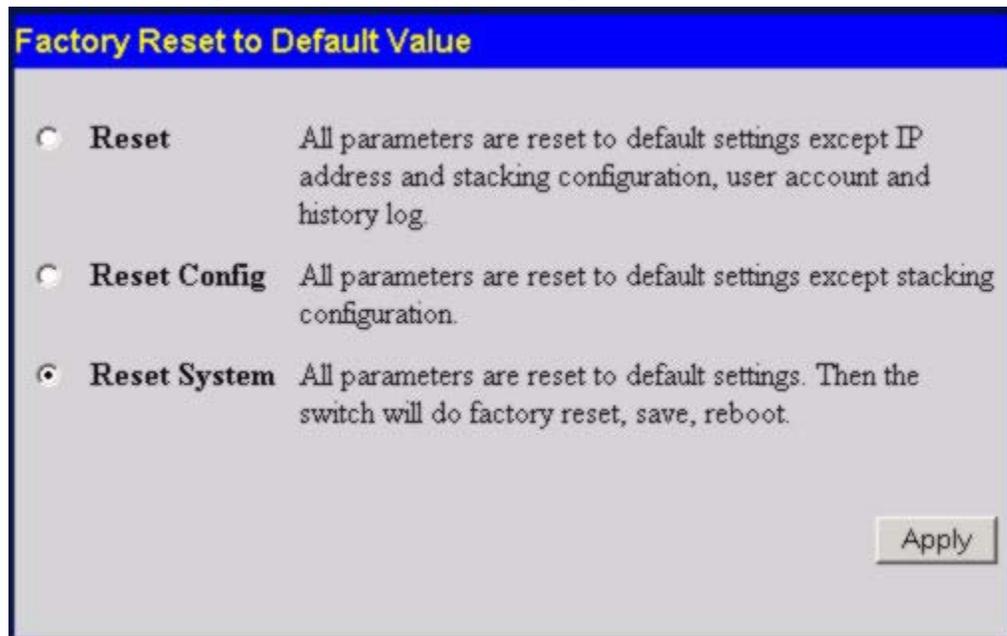


Figure 8-7. Factory Reset to Default Value window

## Restart System

The following window is used to restart the Switch.

Clicking the **Yes** click-box will instruct the Switch to save the current configuration to non-volatile RAM before restarting the Switch.

Clicking the **No** click-box instructs the Switch not to save the current configuration before restarting the Switch. All of the configuration information entered from the last time **Save Changes** was executed will be lost.

Click the **Restart** button to restart the Switch.

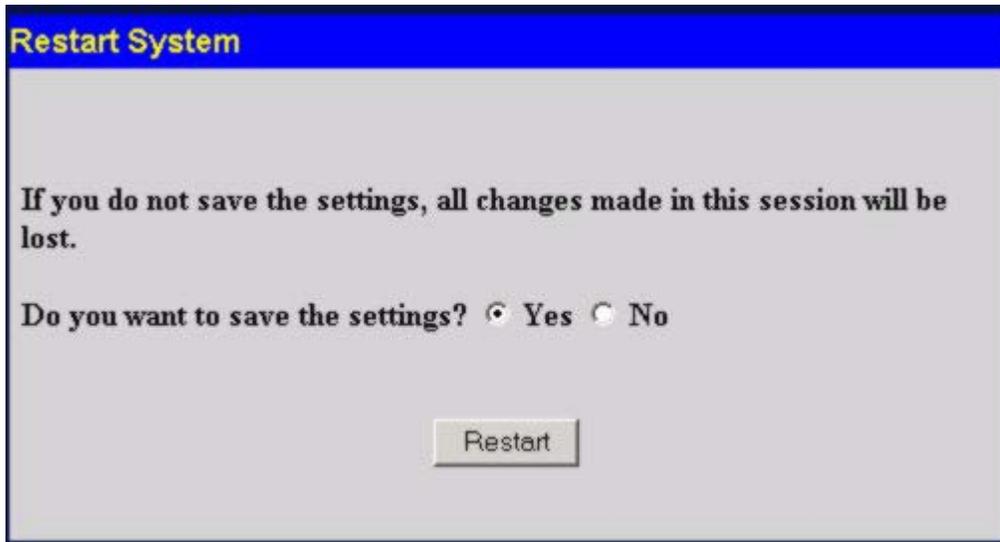


Figure 8- 8. Restart System window

## Logout

Use this window to logout of the Switch's Web-based management agent by clicking on the **Log Out** button.

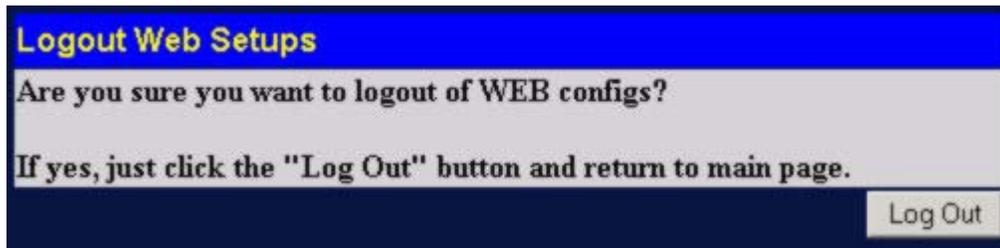


Figure 8- 9. Logout Web Setups window

## Appendix A

### Technical Specifications

General	
<b>Standard</b>	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1 P/Q VLAN IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation
<b>Protocols</b>	CSMA/CD
<b>Data Transfer Rates:</b>	Half-duplex      Full-duplex
<b>Ethernet</b>	10 Mbps          20Mbps
<b>Fast Ethernet</b>	100Mbps          200Mbps
<b>Gigabit Ethernet</b>	N/A                2000Mbps
<b>Fiber Optic</b>	IEC 793-2:1992 Type A1a - 50/125um multimode Type A1b - 62.5/125um multimode Both types use LC optical connector
<b>Topology</b>	Star
<b>Network Cables</b>	UTP Cat. 5 for 100Mbps UTP Cat. 3, 4, 5 for 10Mbps EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)

Performance	
<b>Transmission Method:</b>	Store-and-forward
<b>RAM Buffer:</b>	1 MB per device
<b>Filtering Address Table:</b>	16 K MAC address per device
<b>Packet Filtering/ Forwarding Rate:</b>	Full-wire speed for all connections. 148,800 pps per port (for 100Mbps) 1,488,000 pps per port (for 1000Mbps)
<b>MAC Address Learning:</b>	Automatic update.
<b>Forwarding Table Age Time:</b>	Max age: 10 - 1000000 seconds. Default = 300.

Physical & Environmental	
<b>AC inputs:</b>	100 - 240 VAC, 50/60 Hz (internal universal power supply)
<b>Power Consumption:</b>	30 watts maximum
<b>DC fans:</b>	1 built-in 75 x 75 x30 mm fan

<b>Operating Temperature:</b>	0 to 40 degrees Celsius (32 to 104 degrees Fahrenheit)
<b>Storage Temperature:</b>	-25 to 55 degrees Celsius (-13 to 131 degrees Fahrenheit)
<b>Humidity:</b>	Operating: 5% to 95% RH, non-condensing Storage: 0% to 95% RH, non-condensing
<b>Dimensions:</b>	441 mm x 309 mm x 44 mm (17.36 x 12.16 x 1.73 inches), 1UHeight, 19 inch rack-mount width
<b>Weight:</b>	4.4 kg (9.7 lbs.)
<b>EMI:</b>	FCC Class A, CE Mark, C-Tick
<b>Safety:</b>	CSA International