

**D-Link™ DGS-3312SR**

**12-Port Gigabit Layer 3 Stackable Switch**

**Release II**

***Manual***

---

Second Edition  
(June 2004)

---

**Version 0.2**

Printed In Taiwan



RECYCLABLE

---

Information in this document is subject to change without notice.

© 2004 D-Link Computer Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Computer Corporation is strictly forbidden.

Trademarks used in this text: D-Link and the D-LINK logo are trademarks of D-Link Computer Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Computer Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

June 2004 P/N 651SR3312025

# Table of Contents

About This Manual .....	viii
Intended Readers .....	viii
Typographical Conventions.....	viii
Notes, Notices, and Cautions.....	viii
Safety Instructions .....	ix
Safety Cautions.....	ix
General Precautions for Rack-Mountable Products.....	x
Protecting Against Electrostatic Discharge .....	xi
Introduction .....	1
Switch Description .....	1
Features .....	1
Front-Panel Components .....	2
LED Indicators .....	2
Stacking LED Indicators.....	3
Rear Panel Description .....	4
RPS Connector .....	4
Plug-in Modules .....	4
DEM-340T 1000BASE-T Module .....	4
DEM-340MG SFP (Mini GBIC) Module.....	5
DEM-540 IEEE 1394 Stacking Module .....	5
Switch Stacking.....	5
Management Options .....	6
Installation.....	8
Package Contents .....	8
Before You Connect to the Network .....	8
Installing the Switch without the Rack .....	8
Installing the Switch in a Rack .....	9
Mounting the Switch in a Standard 19" Rack.....	10
Connecting Stacked Switch Groups .....	10
Configuring a Switch Group for Stacking .....	12
External Redundant Power System.....	13
Connecting the Console Port .....	14
Password Protection .....	15
SNMP Settings .....	16
IP Address Assignment.....	17
Connecting Devices to the Switch .....	18
Basic Switch Management.....	19

Before You Start.....	19
General Deployment Strategy.....	19
VLAN Setup.....	20
Defining Static Routes.....	20
Web-based User Interface .....	20
Areas of the User Interface .....	20
Login to Web Manager.....	21
Web Pages and Folders.....	22
Basic Setup.....	22
Switch Information .....	22
Switch IP Settings.....	23
Security IP Management Stations Configuration.....	25
User Account Management .....	26
Admin and User Privileges .....	26
Save Changes.....	27
Factory Reset .....	27
Restart System .....	28
Advanced Settings .....	29
Switch Stack Management .....	30
Configure Stacking .....	31
Basic Configuration .....	34
Switch Information.....	35
IP Address .....	35
Advanced Settings.....	38
Port Configuration.....	39
Port Description.....	42
Port Mirroring .....	42
Traffic Control.....	43
Link Aggregation .....	44
LACP Port Settings .....	46
Port Access Entity .....	47
802.1X Authenticator Settings.....	49
PAE System Control.....	51
RADIUS Server.....	51
IGMP.....	52
IGMP Snooping.....	53
Static Router Ports .....	54
Spanning Tree .....	55
STP Switch Settings .....	56
STP Port Settings.....	58



Forwarding & Filtering .....	59
Unicast Forwarding .....	60
Multicast Forwarding .....	60
VLANs .....	61
802.1Q Static VLANs.....	65
802.1Q Port Settings.....	68
QoS.....	69
802.1p Default Priority .....	69
802.1p User Priority .....	70
QoS Output Scheduling Configuration.....	71
Traffic Segmentation .....	71
Bandwidth Control .....	72
MAC Notification.....	73
MAC Notification Global Settings .....	74
MAC Notification Port Settings .....	75
System Log Server .....	75
Port Security .....	77
SNTP Setting.....	78
Time Setting .....	78
Time Zone and DST Settings .....	79
Access Profile Table.....	80
Advanced Configuration .....	91
L3 Global Advanced Settings.....	92
IP Interface Settings .....	92
MD5 Key Settings.....	110
Route Redistribution Settings.....	111
Static/Default Route Settings .....	112
Static ARP Settings .....	113
RIP.....	113
RIP Global Setting.....	113
RIP Interface Settings.....	114
OSPF .....	115
OSPF General Setting.....	115
OSPF Area ID Settings.....	115
OSPF Interface Settings.....	117
OSPF Virtual Interface Settings .....	118
OSPF Area Aggregation Settings .....	120
OSPF Host Route Settings.....	121
DHCP/Bootp Relay .....	121
DHCP/Bootp Relay Information .....	122

DHCP/Bootp Relay Settings.....	122
DNS Relay.....	122
DNS Relay Information.....	123
DNS Relay Static Settings.....	123
VRRP.....	124
VRRP Configuration.....	124
VRRP Interface Settings.....	124
IP Multicast.....	129
IGMP Interface Settings.....	129
DVMRP.....	131
PIM.....	132
Security.....	134
Trusted Host.....	134
Secure Socket Layer (SSL).....	135
Download Certificate.....	135
Configuration.....	136
Secure Shell (SSH).....	137
SSH Configuration.....	138
SSH Algorithm.....	139
SSH User Authentication.....	141
Access Authentication Control.....	142
Policy & Parameters.....	143
Application Authentication Settings.....	144
Authentication Server Group.....	144
Authentication Server Host.....	145
Login Method Lists.....	147
Enable Method Lists.....	149
Local Enable Password.....	150
Enable Admin.....	151
Management.....	153
User Accounts.....	153
SNMPV3.....	154
SNMP User Table.....	155
SNMP View Table.....	157
SNMP Group Table.....	158
SNMP Community Table.....	159
SNMP Host Table.....	160
SNMP Engine ID.....	161
Monitoring.....	163
Stack Information.....	164

Port Utilization .....	166
CPU Utilization .....	168
Packets.....	168
Received Packets .....	169
Received Unicast/Multicast/Broadcast Packets .....	171
Transmitted Packets.....	173
Errors.....	175
Received Errors .....	175
Transmitted Errors .....	177
Size.....	179
Packet Size.....	179
MAC Address.....	181
Switch History .....	183
IGMP Snooping Table.....	184
Browser Router Port.....	184
VLAN Status .....	185
Session Table.....	186
Layer 3 Feature.....	187
Browse IP Address .....	187
Browse Routing Table.....	187
Browse ARP Table.....	188
Browse IP Multicast Forwarding Table.....	189
Browse IGMP Group Table.....	190
OSPF Monitor .....	190
Browse OSPF LSDB Table .....	190
Browse OSPF Neighbor Table .....	191
Browse OSPF Virtual Neighbor Table .....	192
DVMRP Monitor.....	192
Browse DVMRP Routing Table.....	192
Browse DVMRP Neighbor Address Table.....	193
Browse DVMRP Routing Next Hop Table .....	193
PIM Monitor.....	193
Browse PIM Neighbor Address Table.....	194
Maintenance .....	195
TFTP Services .....	195
Download Firmware .....	195
Download Configuration File.....	196
Save Settings .....	196
Save History Log.....	196
Ping Test.....	196

Save Changes .....	197
Factory Reset.....	197
Restart System.....	198
Logout .....	199
Single IP Management .....	200
SIM Settings .....	201
Topology .....	202
Tool Tips .....	205
Right-click .....	206
Group Icon.....	206
Commander Switch Icon .....	207
Member Switch Icon .....	208
Candidate Switch Icon.....	209
Menu Bar .....	210
Group.....	211
Device.....	211
View .....	211
Firmware Upgrade.....	211
Configuration File Backup/Restore .....	212
Technical Specifications .....	213
Cables and Connectors .....	216
Cable Lengths.....	217

## About This Manual

This manual is divided into two general sections:

**Basics** - Provides 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.

**Web Manager** – Describes management and configuration of Switch features, following the layout of the Switch's Web Manager. Five of the Switch's six main folders—Security, Management, Monitoring, Maintenance, and Single IP Management—have separate chapters. Configuration is divided into two chapters, Basic Configuration and Advanced Configuration.

## Intended Readers

The DGS-3312SR Manual contains information useful for setup and management and of the DGS-3312SR 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: [copy filename] 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: <b>You have mail</b> . 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.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
<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>	<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



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




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



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.
  - Only a trained service technician should service components inside these compartments.
- 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.
- 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.



**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.



**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.



**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. Completed power and safety ground wiring must be inspected by a qualified electrical inspector. An energy hazard will exist if the safety ground cable is omitted or disconnected.

## 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):

1. 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.
2. When transporting a sensitive component, first place it in an antistatic container or packaging.
3. Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads and an antistatic grounding strap.





<h1>Section 1</h1>
--------------------

## 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 DGS-3312SR 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 DES-3226S 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.

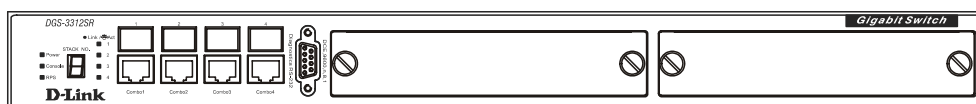
## Features

- 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.
- Star topology Switch stacking configuration for up to 12 additional DES-3226S 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
- Supports 802.3ad LACP Link Aggregation
- Supports port mirroring
- 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)
- 802.1x (port-based and MAC-based) access control and RADIUS Client support
- Administrator-definable port security
- 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
- Supports Web-based management.

- Supports CLI management.
- Supports BOOTP/DHCP/DNS Relay
- Supports TFTP upgrade
- Supports System Log
- Fully configurable either in-band or out-of-band control via RS-232 console serial connection.
- Telnet remote control console
- Traffic Segmentation
- Simple Network Time Protocol
- MAC address update notification
- Web GUI Traffic Monitoring
- Supports RIP v1, v2
- Supports OSPF
- Supports PIM-DM
- Supports DVMRP
- Supports IGMP
- Supports VRRP
- Supports floating static route
- Supports SSL
- Supports SSH
- Supports Single IP Management v.1.0
- Supports RADIUS Authentication
- Supports TACACS, TACACS+, and XTACACS

## 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 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 DES-3226S Switches.

## 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.

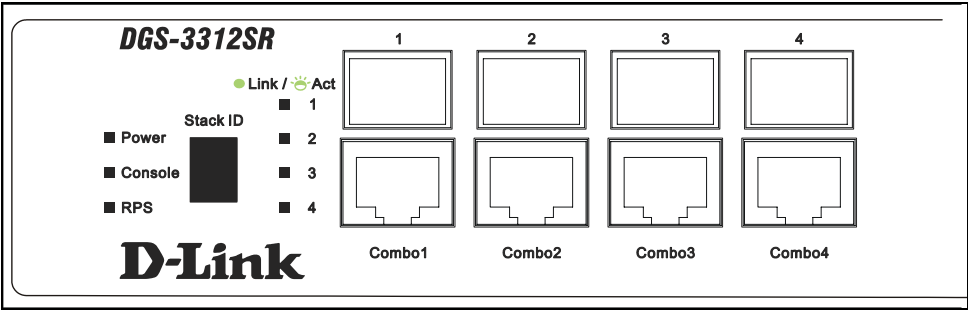


Figure 1- 2. LED Indicators

Power	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.
Console	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.
RPS	This indicator will light steady amber when an external power supply is supplying power. This indicates the internal power supply has failed.
Link/Act	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.



**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).

### 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 DEM-540 stacking module.



**NOTICE:** The four build-in combination ports on the front panel of the DGS-3312SR 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.

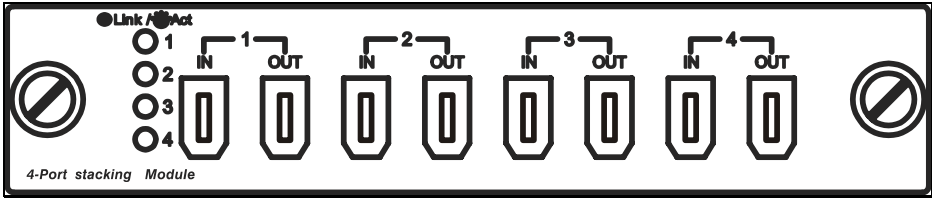


Figure 1- 3. Front panel of DEM-540 IEEE 1394 stacking module

Link/Act	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 DGS-3312SR/DES-3226S 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 DGS-3312SR/DES-3226S 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.

## RPS Connector

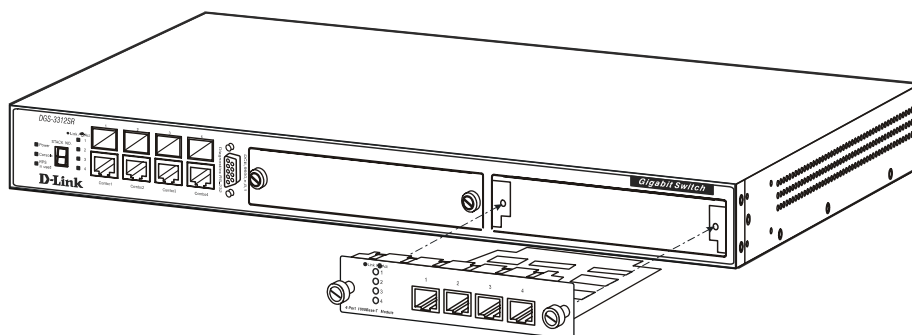
Connect the optional external redundant power supply to the RPS connector. If the Switch’s internal power unit fails, the redundant power system automatically supplies power to the Switch for uninterrupted operation.

The Switch supports the D-Link RPS-200 or RPS-500 redundant power supply units.

## Plug-in Modules

The DGS-3312SR 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.

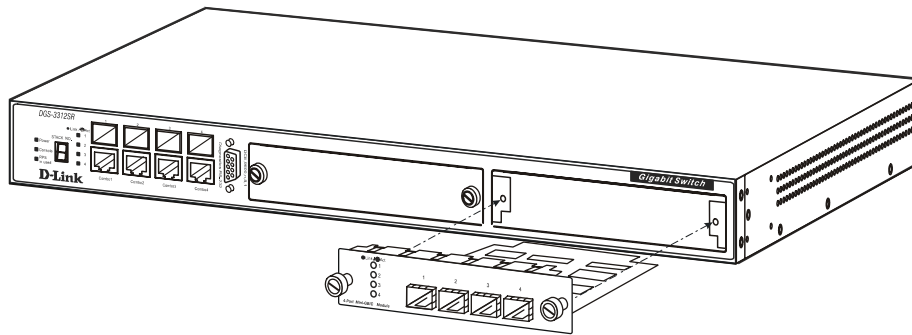
### DEM-340T 1000BASE-T Module



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

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

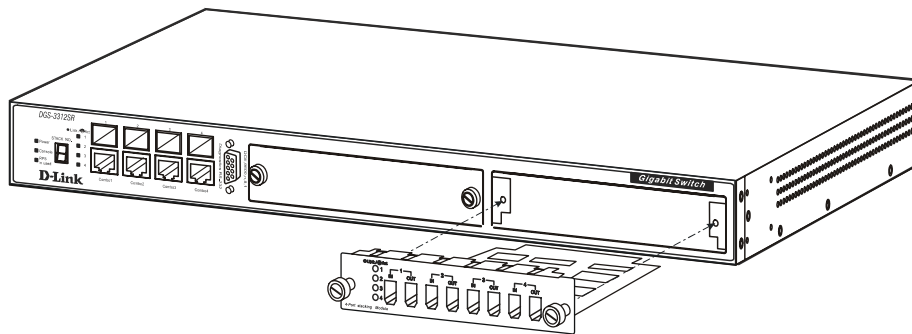
## DEM-340MG SFP (Mini GBIC) Module



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

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

## DEM-540 IEEE 1394 Stacking Module



**Figure 1- 7. DEM-540 IEEE 1394 Stacking module**

- Front-panel module
- Connect to four DES-3226S 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 DGS-3312SR can be stacked with a DES-3226S, functioning as a Master of the stack. There are two connection options available for stacking. One option is to use the built-in combination ports (1000BASE-T/SFP). The other possibility is to install one or two DEM-540 stacking modules and complete the stacking connection through the IEEE 1394 stacking ports. With two stacking modules installed, the DGS-3312SR can be stacked with as many as twelve slave units.

Each optional stacking module allows up to four DES-3226S Switches to be interconnected in a stack with the DGS-3312SR. Two stacking modules may be used to form a nine-Switch stack consisting of one Master and eight Slaves, managed through the DGS-3312SR 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 DGS-3312SR. The stacking modules connect to the slaves using IEEE 1394 serial cable (Firewire) in a star topology for DES-3226S groups (see illustration on page 8).

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 DGS-3312SR 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 (at the time of the writing of this manual), the slaves must be all DES-3226S Switches. The slave unit types cannot be mixed within a single stacked group.
- DES-3226S slave Switches must have firmware Release IV or later loaded to operate properly with the DGS-3312SR Master.
- The DGS-3312SR is automatically started as the Master Switch in a Switch stack.
- It is necessary 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.



**NOTICE:** The CLI stacking command set for the DGS-3312SR is slightly different from the CLI stacking command set for the DES-3226S. Please refer to the CLI Reference Manual for each Switch for details or read the instructions starting on page 12 below.

## 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
- D-Link Enterprise MIB



## SECTION 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:

- One DGS-3312SR Layer 3 Switch
- Mounting kit: 2 mounting brackets and screws
- Four rubber feet with adhesive backing
- One AC power cord
- This Manual
- CLI Reference

## 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).

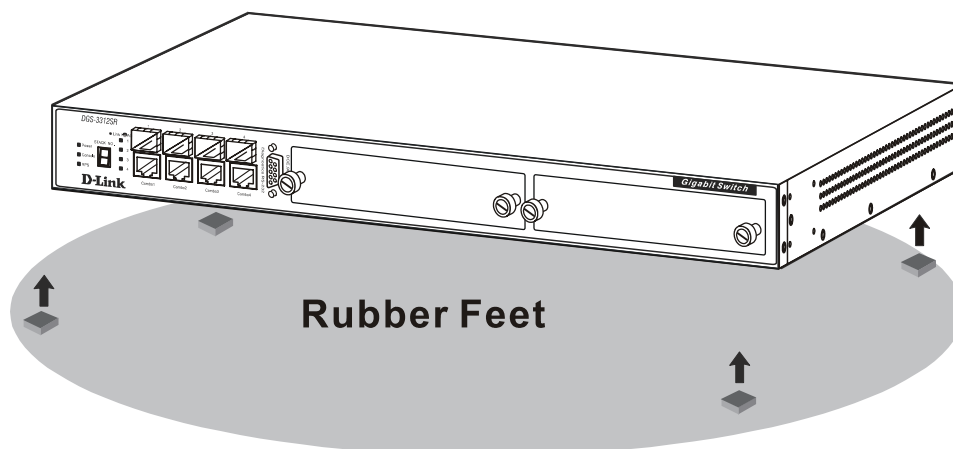
## Installing the Switch without the Rack

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.

1. 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.

2. 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.
3. 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.

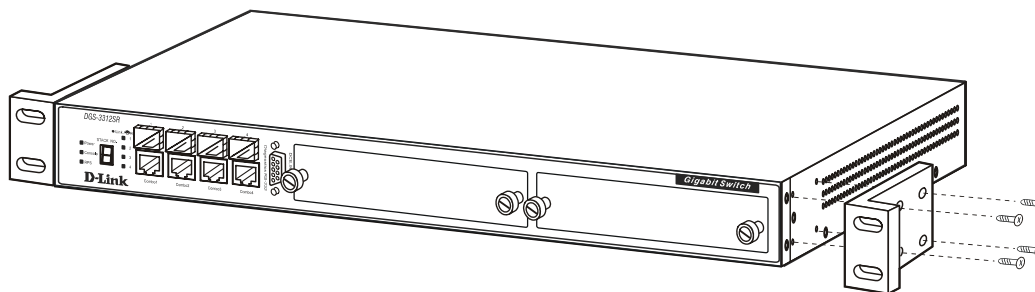


**Figure 2- 1. Install rubber feet for installations with or without a rack**

## 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.

1. Use the supplied screws to attach a mounting bracket to each side of the Switch.
2. Align the holes in the mounting bracket with the holes in the rack.
3. Insert and tighten two screws through each of the mounting brackets.



**Figure 2- 2. Attach mounting brackets to Switch**

Fasten the mounting brackets to the Switch using the screws provided. With the brackets attached securely, you can mount the Switch in a standard rack as shown in Figure 2-3 on the following page.

## Mounting the Switch in a Standard 19" Rack

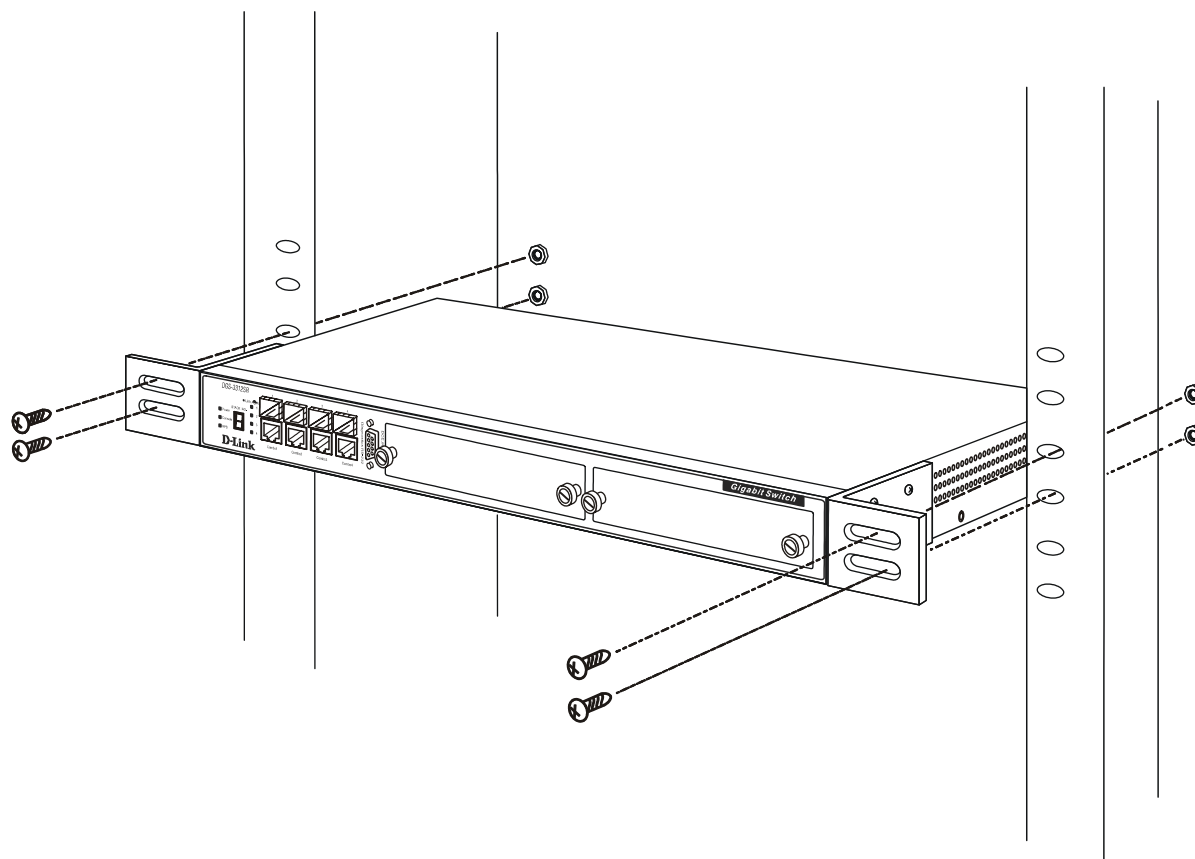


Figure 2-3. Install Switch in equipment rack

## Connecting Stacked Switch Groups

The DGS-3312SR may be configured to function as the Master of a stacked group of DES-3226S Switches (see Restrictions for Stacking on page 6). A stacked group of DES-3226S Switches are connected using a star topology. The instructions below, Configuring a Switch Group for Stacking, tell you how to configure the DGS-3312SR to function as a Master, as well as how to configure the DES-3226S 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.



11

## Configuring a Switch Group for Stacking

Follow the instructions below to first configure the slave units, and then to configure the DGS-3312SR as the designated Master.



**NOTICE:** The DGS-3312SR can be used to manage a Switch stack consisting of only DES-3226S Switches.

For the DES-3226S the stacking configuration as a Master or Slave Switch is no longer necessary. The DGS-3312SR can communicate with a DES-3226S regardless of its stacking configuration. It is recommended that you configure all DES-3226S Switches in a Switch stack in the auto stacking mode to reduce the potential for problems. The default stacking mode configuration for the DES-3226S is auto.

To configure the DES-3226S to function in a stacked group as a slave, do the following:

1. At the CLI login prompt, enter **config stacking mode enable auto** and press the **Enter** key.
2. You will be prompted to save the stacking mode configuration. Press the Y key (yes) to save the stacking mode configuration.
3. 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 DES-3226S.

```
DES-3226S: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.

DES-3226S:4#.....
```

The default settings for the DGS-3312SR 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 DGS-3312SR, do the following:

1. At the CLI login prompt, enter **config stacking mode enable** and press the **Enter** key.
2. 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.
3. Press the Y key (yes) to save the stacking mode configuration and restart the switch.

```
DGS-3312SR: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.**

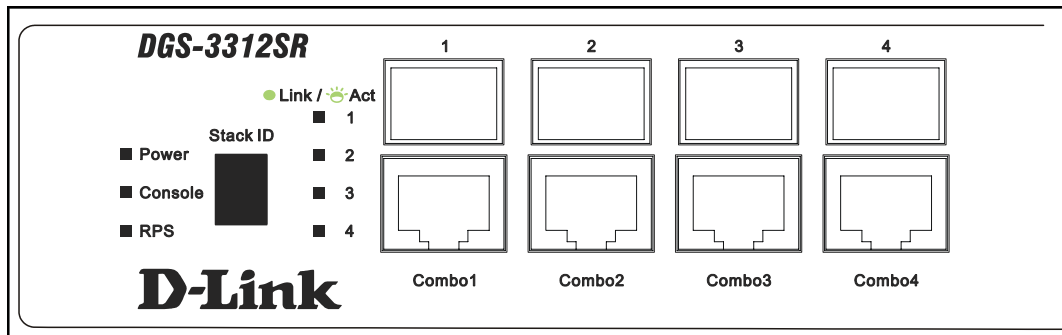
**If you do not save the changes now, they will be lost.**

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

Changing the stacking mode in the DGS-3312SR will automatically save the settings and restart the system. It will take a few minutes to complete the process.

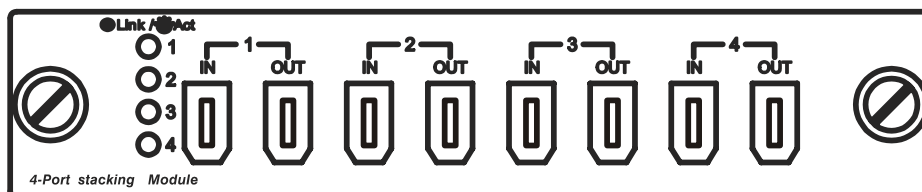
### Unit ID Display for Switches in a Switch Stack

The Stack ID 7-segment LED (as shown below) on the front panel of the DGS-3312SR will always display F (15 in hex). An F will also be displayed in the Stack ID LED even if the DGS-3312SR is in standalone mode.



**Figure 2-5. DGS-3312SR Front Panel**

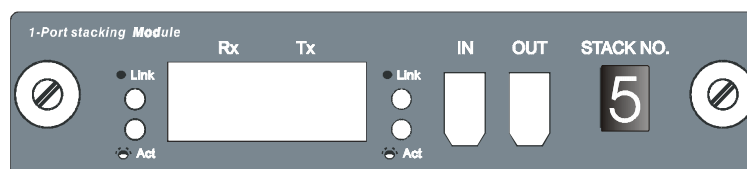
The Unit ID of individual DES-3226S Switches in a Switch stack is determined by the port number of the port on the DGS-3312SR that the Switch is connected to. The ports on the DGS-3312SR are numbered starting with port 1 from left to right along the front panel of the Switch. For example, the four combination 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 DGS-3312SR, then the stacking ports on the second module will be numbered 9 through 12.



**Figure 2-6. DEM-540 Stacking Module Front Panel**

If the a stacking module is installed in the DGS-3312SR's first module slot, then the first IN/OUT pair in the figure above will be port 5. If a DES-3226S in a Switch stack is connected to the first stacking port (port number 5 on the DGS-3312SR), then the Unit ID of the DES-3226S will be 5.

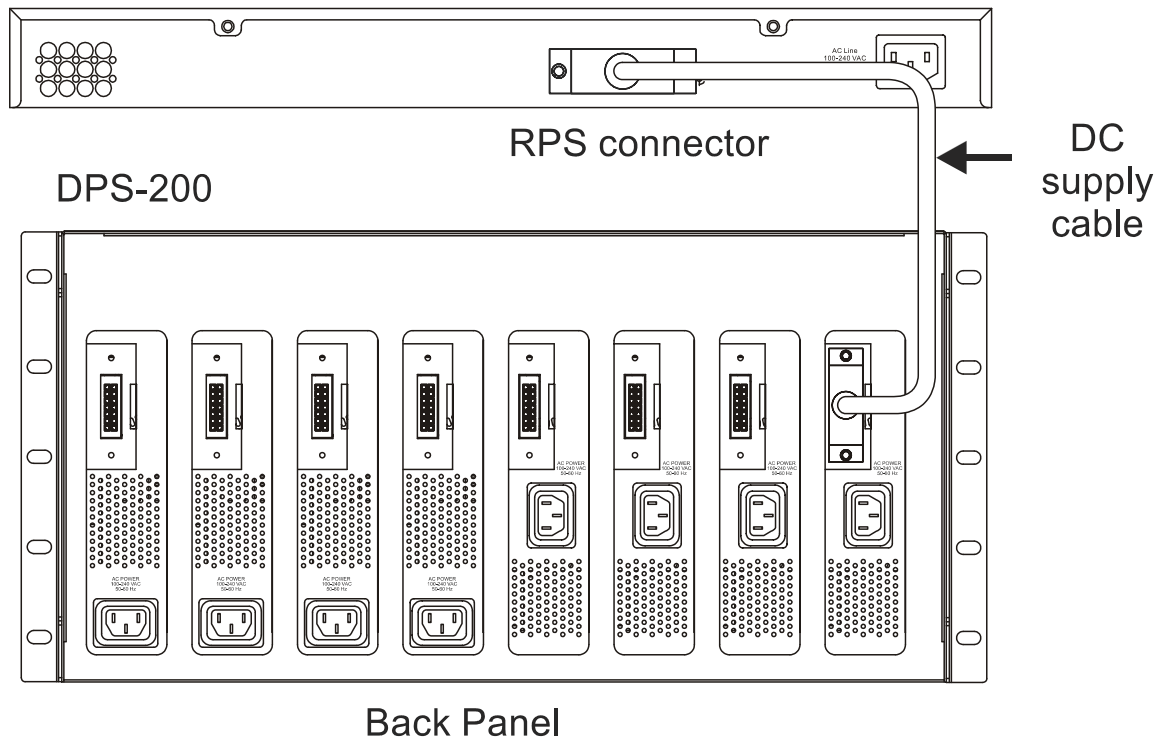
The Unit ID of the DES-3226S will be displayed in the STACK NO. LED on the front panel of the DES-3226S's stacking module, as shown below.



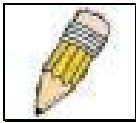
**Figure 2-7. DES-3226S Stacking Module Front Panel**

### External Redundant Power System

The Switch supports an external redundant power system.



**Figure 2-8. DPS-200 with DGS-3312SR**



**NOTE:** See the DPS-200 documentation for more information.



**CAUTION:** Do not use the Switch with any redundant power system other than the DPS-200 or DPS-500.

## 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:

1. Connect the female connector of the RS-232 cable directly to the console port on the Switch, and tighten the captive retaining screws.
2. 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:
  - a. Select the appropriate serial port (COM port 1 or COM port 2).
  - b. Set the data rate to 9600 baud.
  - c. Set the data format to 8 data bits, 1 stop bit, and no parity.

- d. Set flow control to **none**.
- e. Under **Properties**, select **VT100 for Emulation** mode.
- f. 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.

- g. 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.
- h. After the boot sequence completes, the console login screen displays.
- i. 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.
- j. 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.
- k. When you have completed your tasks, exit the session with the **logout** command or close the emulator program.

## Password Protection

The DGS-3312SR 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:

1. At the CLI login prompt, enter **create account admin** followed by the <user name> and press the **Enter** key.
2. You will be asked to provide a password. Type the <password> used for the administrator account being created and press the **Enter** key.
3. You will be prompted to enter the same password again to verify it. Type the same password and press the **Enter** key.
4. 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.



**NOTE:** Passwords are case sensitive.

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



```
DGS-3312SR:4#create account admin newmanager
Command: create account admin newmanager

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

DGS-3312SR: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 DGS-3312SR 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.

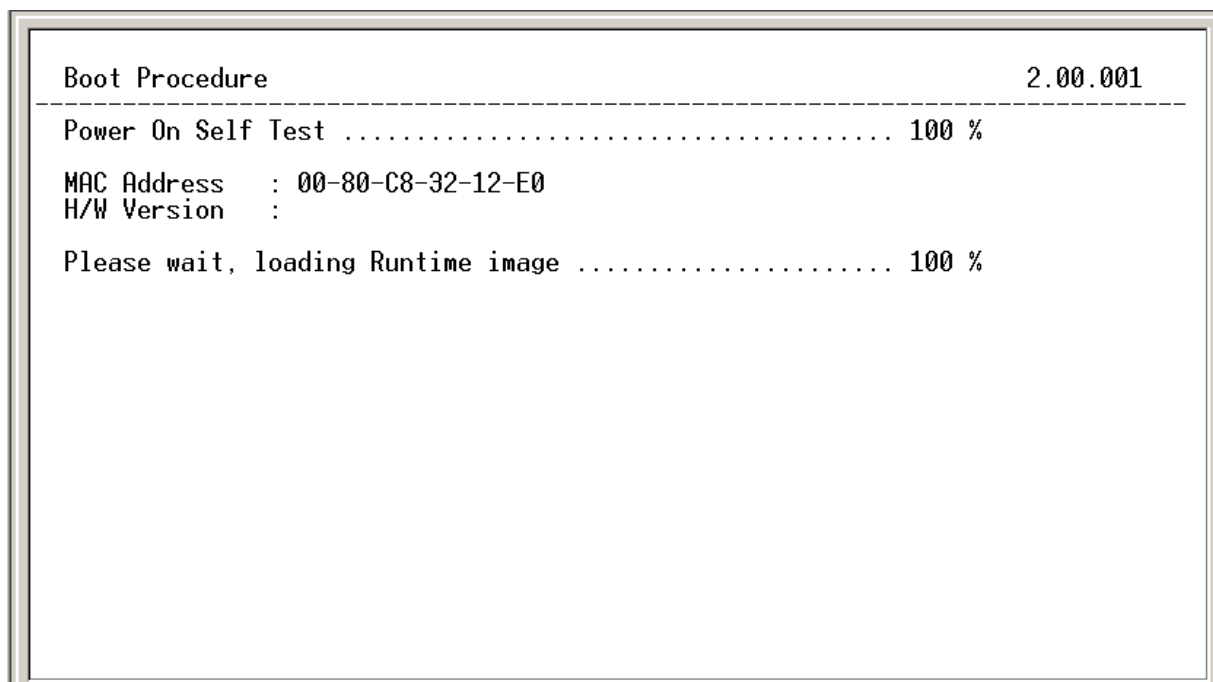
## MIBs

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.



```

Boot Procedure                                     2.00.001
-----
Power On Self Test ..... 100 %

MAC Address   : 00-80-C8-32-12-E0
H/W Version   :

Please wait, loading Runtime image ..... 100 %
  
```

**Figure 2-9. 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:

1. 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.

```
DGS-3312SR Gigabit Ethernet Switch Command Line Interface
                          Firmware: Build 2.00-B17
Copyright(C) 2000-2003 D-Link Corporation. All rights reserved.
UserName:
Password:

DGS-3312SR:4#config ipif System ipaddress 10.24.22.9/255.0.0.0
Command: config ipif System ipaddress 10.24.22.9/8

Success.
DGS-3312SR:4#
```

**Figure 2-10. Assigning the Switch an IP Address**

In the above example, the Switch was assigned an IP address of 10.22.24.9 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.

<h2>Section 3</h2>
--------------------

# Basic Switch Management

## *Before You Start*

### *General Deployment Strategy*

### *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 DGS-3312SR 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 DGS-3312SR Layer 3 Switch supports a wide array of functions and gives great flexibility and increased network performance by eliminating the routing bottleneck between the WAN or Internet and the Intranet. Its function in a network can be thought of as a new generation of router that performs routing functions in hardware, rather than software. It is in effect, a router that also has numerous independent Ethernet collision domains – each of which can be assigned an IP subnet.

This flexibility and rich feature set requires a bit of thought to arrive at a deployment strategy that will maximize the potential of the DGS-3312SR Layer 3 Switch. Please read the portions of this manual pertaining to the functions you wish to perform with the Switch. It is especially important to map out VLANs and configuration of IP interfaces, and OSPF configuration in advance of actual configuration. For this reason, these subjects are presented in greater detail in the final two parts of this manual.

## General Deployment Strategy

1. Determine how the network would be best segmented. This is probably done using VLANs in an existing layer 2 Switched network.
2. Develop an IP addressing scheme. This involves allocating a block of IP addresses to each network segment. Each network subnet is then assigned a network address and a subnet mask. Background information regarding IP addresses is presented in Part IV of this guide.
3. Determine which network resources must be shared by the subnets. Shared resources may be connected directly to Layer 3 Switches. Static routes to each of the shared resources should be determined.

4. Determine how each subnet will communicate with the WAN or Internet. Again, static routes should be determined and default gateways identified.
5. Develop a security scheme. Some subnets on the network need more security or should be isolated from the other subnets. IP or MAC filtering can be used. Also, one or more VLANs on the Layer 3 Switch can be configured without an IP subnet – in which case, these VLANs will function as a layer 2 VLAN and would require an external router to connect to the rest of the network.
6. Develop a policy scheme. Some subnets will have a greater need for multicasting bandwidth, for example. A policy is a mechanism to alter the normal packet forwarding in a network device, and can be used to intelligently allocate bandwidth to time-critical applications such as the integration of voice, video, and data on the network.
7. Develop a redundancy scheme. Planning redundant links and routes to network critical resources can save valuable time in case of a link or device failure. The DGS-3312SR Spanning Tree function can be used to block the redundant link until it is needed.

## **VLAN Setup**

VLANs setup in Layer 3 Switching is more complicated than in conventional Layer 2 Switching environments. Be sure to carefully plan the VLAN/IP interface arrangement for the network before configuring the VLANs and IP interface associations.

VLANs configuration and concepts are provided in Part III.

## **Defining Static Routes**

Routes between the IP interfaces and a default gateway or other router with a WAN connection should be determined beforehand and entered into the static/default routing table on the DGS-3312SR.

Configuration of static routes and other uses of routing protocols are presented in Part IV.

## **Web-based User Interface**

The user interface provides access to various Switch configuration and management screens, 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.

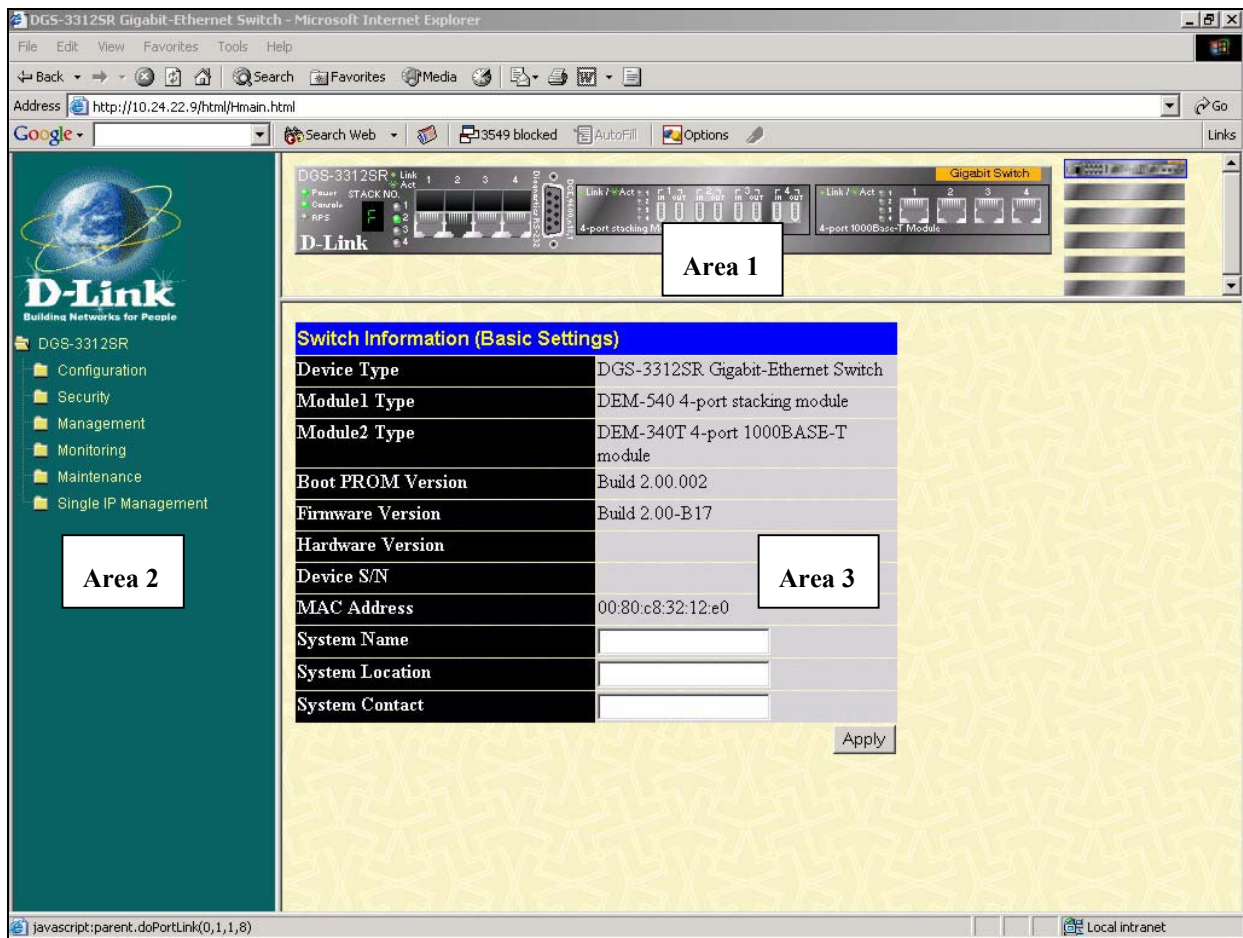


Figure 3-1. Main Web-Manager window

Area	Function
1	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.  Click on the ports in the front panel to manage the port's configuration or view data for the port.
2	Select the window to be displayed. The folder icons can be opened to display the hyperlinked window buttons and sub-folders contained within them.
3	Presents the information selected for configuration or display.

## 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 including Layer 3 functions.

**Security:** This folder contains SSL, SSH, and Access Authentication Control sub-folders are also located here. 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:** This folder includes stack information and data tables for performance statistics, application, and protocol status, including Layer 3 functions.

**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.

## Basic Setup

The subsections below describe how to change some of the basic settings for the Switch such as changing IP settings and assigning user names and passwords for management access privileges, as well as how to save the changes and restart the Switch.

## 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	DGS-3312SR Gigabit-Ethernet Switch
Module1 Type	DEM-540 4-port stacking module
Module2 Type	DEM-340T 4-port 1000BASE-T module
Boot PROM Version	Build 2.00.002
Firmware Version	Build 2.00-B17
Hardware Version	
Device S/N	
MAC Address	00:80:c8:32:12:e0
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
Apply	

**Figure 3-2. Switch Information (Basic Settings) window**

This window displays general information about the Switch including its MAC Address, Hardware Boot PROM and Firmware versions, and 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 <input type="button" value="v"/>
IP Address	<input type="text" value="10.24.22.9"/>
Subnet Mask	<input type="text" value="255.0.0.0"/>
Default Gateway	<input type="text" value="0.0.0.0"/>
VID	<input type="text" value="1"/>
Apply	

**Figure 3-3. Switch IP Settings window**





**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:**

- Select *Manual* from the Get IP From drop-down menu.
- 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 25) 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.

The screenshot shows a web-based configuration window titled "Security IP Management". It has a blue header bar with the title in yellow. Below the header, there are three rows, each with a label on the left and an input field on the right. The labels are "IP1 Access to Switch", "IP2 Access to Switch", and "IP3 Access to Switch". Each input field contains the text "0.0.0.0". To the right of these input fields is a large grey button labeled "Apply". Below the input fields, there is a note in blue text: "Note : Create a list of IP addresses that can access the switch. Your local host IP address must be one of the IP addresses to avoid disconnection."

Security IP Management	
IP1 Access to Switch	0.0.0.0
IP2 Access to Switch	0.0.0.0
IP3 Access to Switch	0.0.0.0
Apply	
<p><b>Note :</b> Create a list of IP addresses that can access the switch. Your local host IP address must be one of the IP addresses to avoid disconnection.</p>	

**Figure 3-4. Security IP Management window**

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, as shown below.

**Figure 3-5. User Account Management window**

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

**Figure 3- 6. User Account Modify Table window**

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.

**Figure 3- 7. User Account Modify Table window**

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
Configuration	Yes	Read Only
Network Monitoring	Yes	Read Only
Community Strings and Trap Stations	Yes	Read Only
Update Firmware and Configuration Files	Yes	No
System Utilities	Yes	PING Only
Factory Reset	Yes	No

---

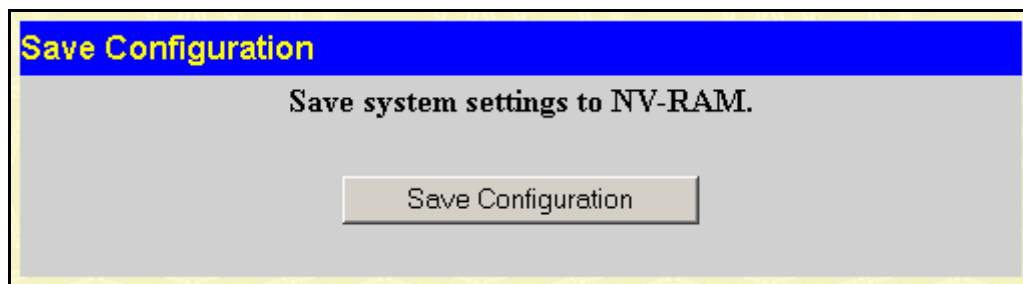
User Account Management		
Add/Update/Delete User Accounts	Yes	No
View User Accounts	Yes	No

**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.

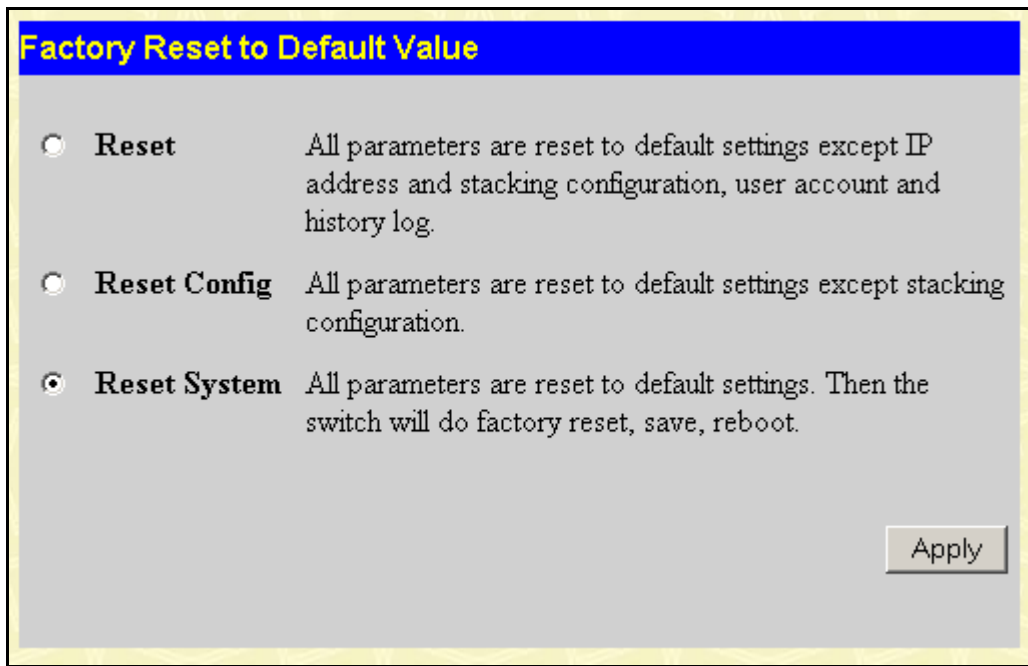
**Figure 3- 8. Save Configuration window**

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 window**

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.

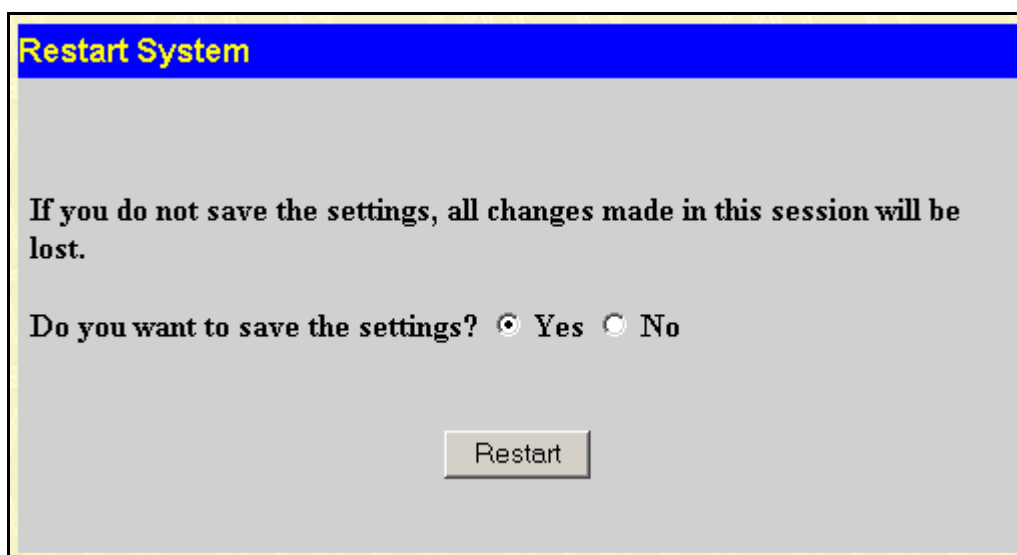


Figure 3- 10. Restart System window



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

## Advanced Settings

Switch Information (Advanced Settings)	
Serial Port Auto Logout	Never
Serial Port Baud Rate	9600
MAC Address Aging Time (10-1000000)	300
IGMP Snooping	Disabled
Multicast router Only	Disabled
Telnet Status	Enabled
Telnet TCP Port Number(1-65535)	23
Web Status	Enabled
Web TCP Port Number(1-65535)	80
RMON Status	Disabled
GVRP	Disabled
Link Aggregation Algorithm	IP Source
Switch 802.1x	Disabled
Syslog state	Disabled

Apply

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

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</i> , and <i>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.

## Switch Stack Management

The DGS-3312SR 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 DEM-540 Stacking modules must be installed in order to use the Switch in a stacked configuration. Read page 6 in Chapter 1 and page 10 in Chapter 2 for more information about stacking the DGS-3312SR Switch.



- Slave Switch units in a stacked Switch group must be uniform in type and model, furthermore they must be one of the Switch models intended for use with the DGS-3312SR, namely DES-3226S Switches.

One stacking module can be installed to stack up to four additional slave Switch units or two modules can be installed to stack up to eight additional slave Switch units. Please read the relevant information in Sections 1 and 2 for more information.

## Configure Stacking

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.

Stack Mode Setup												
Stack Topology	Disable											
Setting	STANDALONE											
Current	STANDALONE											
Stack Mode State	Disable ▾											
Stack Port	1	2	3	4	5	6	7	8	9	10	11	12
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Apply												
Total Entries : 1												
Stack Information Table												
ID	MAC Address	Port Range	Mode	Version	RPS Status	Model Name						
15	00-80-c8-32-12-e0	1-12	STANDALONE	2.00-B17	Present	DGS-3312SR						

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

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

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

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

- Select *Enabled* from the Stack Mode State drop-down menu.
- Select the Stack Port by clicking to check a corresponding selection box (Port 1- Port 4).

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 DGS-3312SR will always display an F (15 in hex), regardless of whether the DGS-3312SR 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 Port 1.



Stack Mode Setup												
Stack Topology	Auto Detect											
Setting	MASTER											
Current	MASTER											
Stack Mode State	Enable ▾											
Stack Port	1	2	3	4	5	6	7	8	9	10	11	12
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Apply												
Total Entries : 2												
Stack Information Table												
ID	MAC Address	Port Range	Mode	Version	RPS Status	Model Name						
15	00-80-c8-32-12-e0	1-12	MASTER	2.00-B17	Present	DGS-3312SR						
5	00-01-02-41-44-01	251-276	SLAVE	4.02-B03	Not Support	DES-3226S						

Figure 3- 13. Stack Mode Setup (stacking enabled) window

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>RPS Status</b>	Displays the status of an optional Redundant Power Supply.
<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.

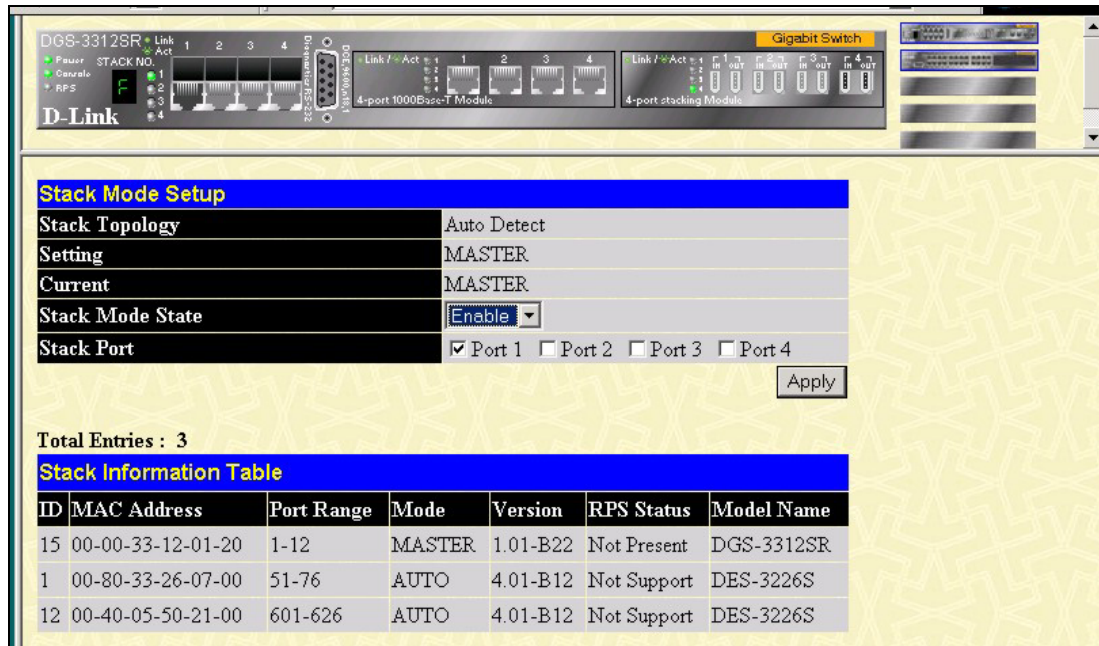


Figure 3- 14. Stack Information web page

<h2>Section 4</h2>
--------------------

## Basic Configuration

- Switch Information*
- IP Address*
- Advanced Settings*
- Port Configuration*
- Port Description*
- Port Mirroring*
- Traffic Control*
- Link Aggregation*
- LACP Port Settings*
- Port Access Entity*
- 802.1X Authenticator Settings*
- PAE System Control*
- 802.1X Capability Settings*
- RADIUS Server*
- IGMP*
- IGMP Snooping*
- Static Router Ports Entry*
- Spanning Tree*
- STP Switch Settings*
- STP Port Settings*
- Forwarding & Filtering*
- Unicast Forwarding*
- Multicast Forwarding*
- 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 DGS-3312SR'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 except those found in the **Layer 3 IP Networking** sub-folder, which are explained in the next chapter, "Advanced Configuration."

## 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	DGS-3312SR Gigabit-Ethernet Switch
Module1 Type	DEM-540 4-port stacking module
Module2 Type	DEM-340T 4-port 1000BASE-T module
Boot PROM Version	Build 2.00.002
Firmware Version	Build 2.00-B17
Hardware Version	
Device S/N	
MAC Address	00:80:c8:32:12:e0
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
Apply	

**Figure 4- 1. Switch Information (Basic Settings) window**

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

## IP Address

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.

Figure 4- 2. Switch IP Settings window



**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:**

- Select *Manual* from the Get IP From drop-down menu.
- 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 <b>Security IP Management</b> window. 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 are assigned or SNMP settings are configured to control management access.

---

### 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.

## Advanced Settings

Switch Information (Advanced Settings)	
Serial Port Auto Logout	Never
Serial Port Baud Rate	9600
MAC Address Aging Time (10-1000000)	300
IGMP Snooping	Disabled
Multicast router Only	Disabled
Telnet Status	Enabled
Telnet TCP Port Number(1-65535)	23
Web Status	Enabled
Web TCP Port Number(1-65535)	80
RMON Status	Disabled
GVRP	Disabled
Link Aggregation Algorithm	IP Source
Switch 802.1x	Disabled
Syslog state	Disabled
Apply	

Figure 4- 3. Switch Information (Advanced Settings) window

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: 2 Minutes, 5 Minutes, 10 Minutes, 15 Minutes or Never.
<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: 9600, 19200, 38400 or 115200.
<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 10 and 1,000,000 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</i> , <i>MAC Destination</i> , <i>MAC Src &amp; Dest</i> , <i>IP Source</i> , <i>IP Destination</i> , and <i>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 functions on the Switch

---

## 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:



Port Configuration				
From	To	State	Speed/Duplex	Apply
Port 1 ▾	Port 1 ▾	Disabled ▾	Auto ▾	<input type="button" value="Apply"/>

The Port Information Table			
Port	State	Speed/Duplex	Connection
1	Enabled	Auto	Link Down
2	Enabled	Auto	Link Down
3	Enabled	Auto	Link Down
4	Enabled	Auto	Link Down
5	Enabled	Auto	100M/Full
6	Enabled	Auto	Link Down
7	Enabled	Auto	Link Down
8	Enabled	Auto	Link Down
9	Enabled	Auto	Link Down
10	Enabled	Auto	Link Down
11	Enabled	Auto	100M/Full
12	Enabled	Auto	Link Down
13	Enabled	Auto	Link Down
14	Enabled	Auto	Link Down
15	Enabled	Auto	Link Down
16	Enabled	Auto	Link Down
17	Enabled	Auto	Link Down
18	Enabled	Auto	Link Down
19	Enabled	Auto	Link Down
20	Enabled	Auto	Link Down
21	Enabled	Auto	Link Down
22	Enabled	Auto	Link Down
23	Enabled	Auto	Link Down
24	Enabled	Auto	Link Down
25	Enabled	Auto	Link Down
26	Enabled	Auto	Link Down
27	Enabled	Auto	Link Down
28	Enabled	Auto	Link Down
29	Enabled	Auto	Link Down
30	Enabled	Auto	Link Down
31	Enabled	Auto	Link Down

32	Enabled	Auto	Link Down
33	Enabled	Auto	Link Down
34	Enabled	Auto	Link Down
35	Enabled	Auto	Link Down
36	Enabled	Auto	Link Down
37	Enabled	Auto	Link Down
38	Enabled	Auto	Link Down
39	Enabled	Auto	Link Down
40	Enabled	Auto	Link Down
41	Enabled	Auto	Link Down
42	Enabled	Auto	Link Down
43	Enabled	Auto	Link Down
44	Enabled	Auto	Link Down
45	Enabled	Auto	Link Down
46	Enabled	Auto	Link Down
47	Enabled	Auto	Link Down
48	Enabled	Auto	Link Down
49	Enabled	Auto	Link Down
50	Enabled	Auto	Link Down

**Figure 4- 4. Port Configuration window**

To configure Switch ports:

Choose the **Unit** from the pull-down menu.

Choose the port or sequential range of ports using the **From...To...** port pull-down menus.

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
<b>State</b> <Enabled>	Toggle the State field to either enable or disable a given port.
<b>Speed/Duplex</b> <Auto>	Toggle the Speed/Duplex field to either select the speed and duplex/half-duplex state of the port. <i>Auto</i> – 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 <i>1000M/Full</i> , <i>1000M/Half</i> , <i>100M/Full</i> , <i>100M/Half</i> , <i>10M/Full</i> , and <i>10M/Half</i> . There is no automatic adjustment of port settings with any option other than <i>Auto</i> .
<b>Flow Control</b>	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 <i>Disabled</i> .
<b>Learning</b>	Enable or disable MAC address learning for the selected ports. When <i>Enabled</i> , destination and source MAC addresses are automatically listed in the forwarding table. When learning is <i>Disabled</i> , MAC addresses must be manually entered into the forwarding table. This is sometimes done for reasons of security or efficiency.

## Port Description

The Switch supports a port description feature where the user may name various ports on the Switch. To assign names to various ports, click **Port Description** on the **Configuration** folder:

Port Description Setting			
Unit	From	To	Description
15	Port 1	Port 1	

Port Description Table	
Port	Description
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

**Figure 4- 5. Port Description Setting window**

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 DGS-3312SR Switch in standalone mode.
<b>From/To</b>	A consecutive group of ports may be configured starting with the selected port.
<b>Description</b>	Enter a description of the port or ports.

## 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 Port**

Port Number	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"/>
Ingress	<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 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"/>
Both	<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"/>

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.

Figure 4- 6. Setup Port Mirroring window

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.

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- 7. Traffic Control Setting window

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

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	t1	Modify	X
2	t2	Modify	X
3	cpu1	Modify	X
4	cpu2	Modify	X

Figure 4- 8. Port Trunking group window

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.

Port Trunking Configuration																									
Group ID	<input type="text"/>																								
State	Disabled																								
Type	Static																								
Master Port	15 Port 1																								
Member Unit	15																								
Port Map	<table border="1"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td> </tr> <tr> <td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10	11	12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	2	3	4	5	6	7	8	9	10	11	12														
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>														
Flooding Port	None																								
Active Port																									
<input type="button" value="Apply"/>																									
<p><b>Note:</b> It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.</p> <p><a href="#">Show All Port Trunking Group Entries</a></p>																									

Figure 4- 9. Port Trunking Configuration window

The user-changeable parameters are as follows:

Parameter	Description
Group ID	Select an ID number for the group.
State	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 windows 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.

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

LACP Port Mode Table	
Port	Mode
1	Stackig Link Port
2	Passive
3	Passive
4	Passive
5	Stackig Link Port
6	Stackig Link Port
7	Stackig Link Port
8	Stackig Link Port
9	Passive
10	Passive
11	Passive
12	Passive

**Figure 4- 10. LACP Port Mode Table window**

The user may set the following parameters:

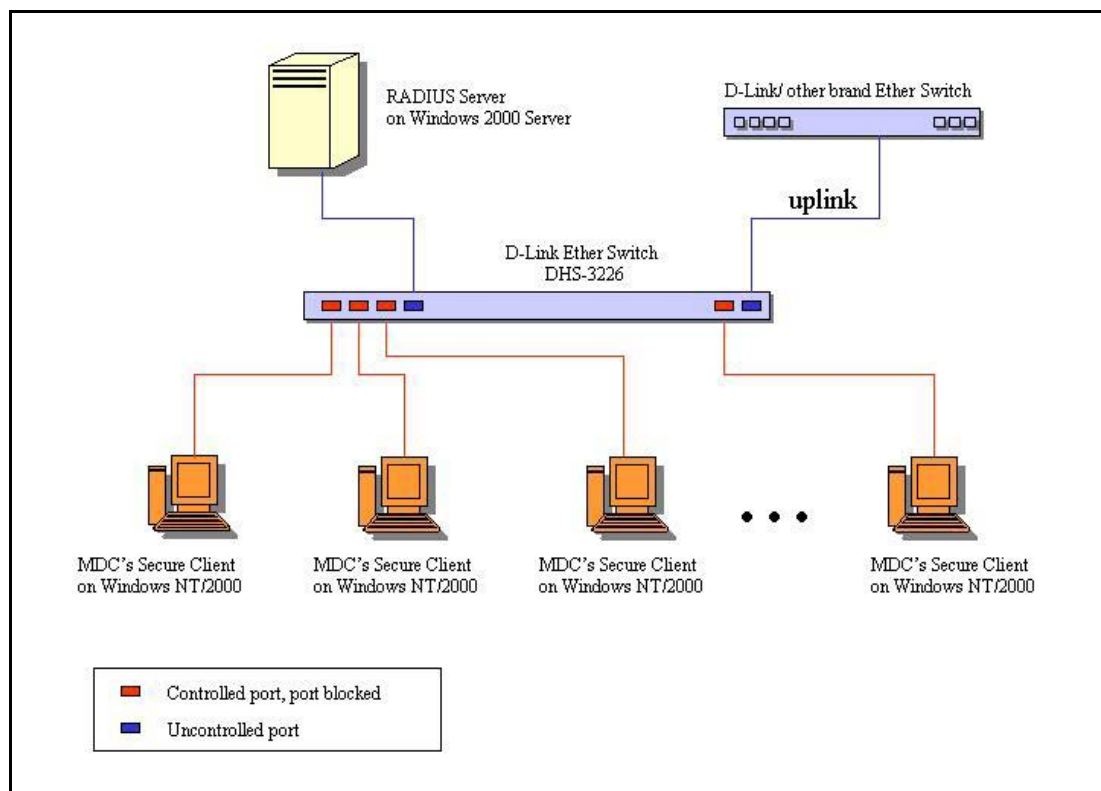


Parameter	Description
<b>Unit</b>	This is the Unit ID of a Switch in a Switch stack. The number 15 indicates a DGS-3312SR Switch in standalone mode.
<b>From/To</b>	A consecutive group of ports may be configured starting with the selected port.
<b>Mode</b>	<p><i>Active</i> – Active LACP ports are capable 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 connection must have “active” LACP ports (see above).</p>

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.

## Port Access Entity

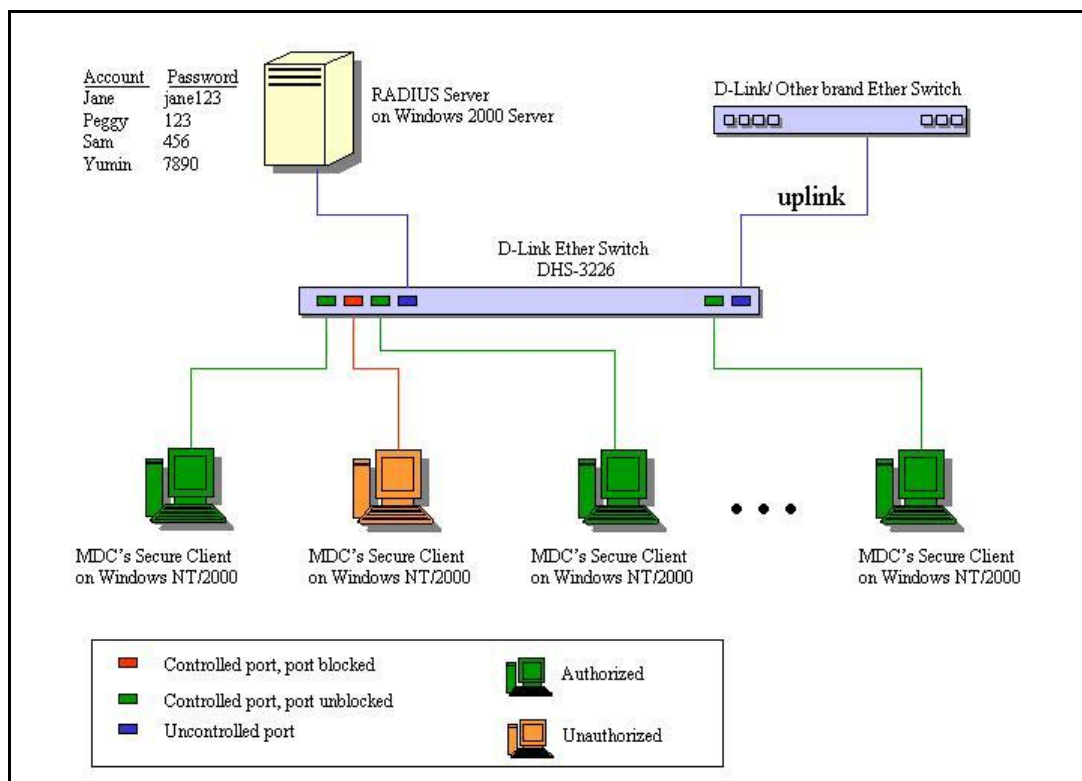
The Switch is an implementation of the server side of IEEE 802.1X-Port Based Network Access Control. Through this mechanism, users have to be authorized before being able to access the network. See the following figure:



**Figure 4- 11. Typical 802.1X Configuration Prior to User Authentication**

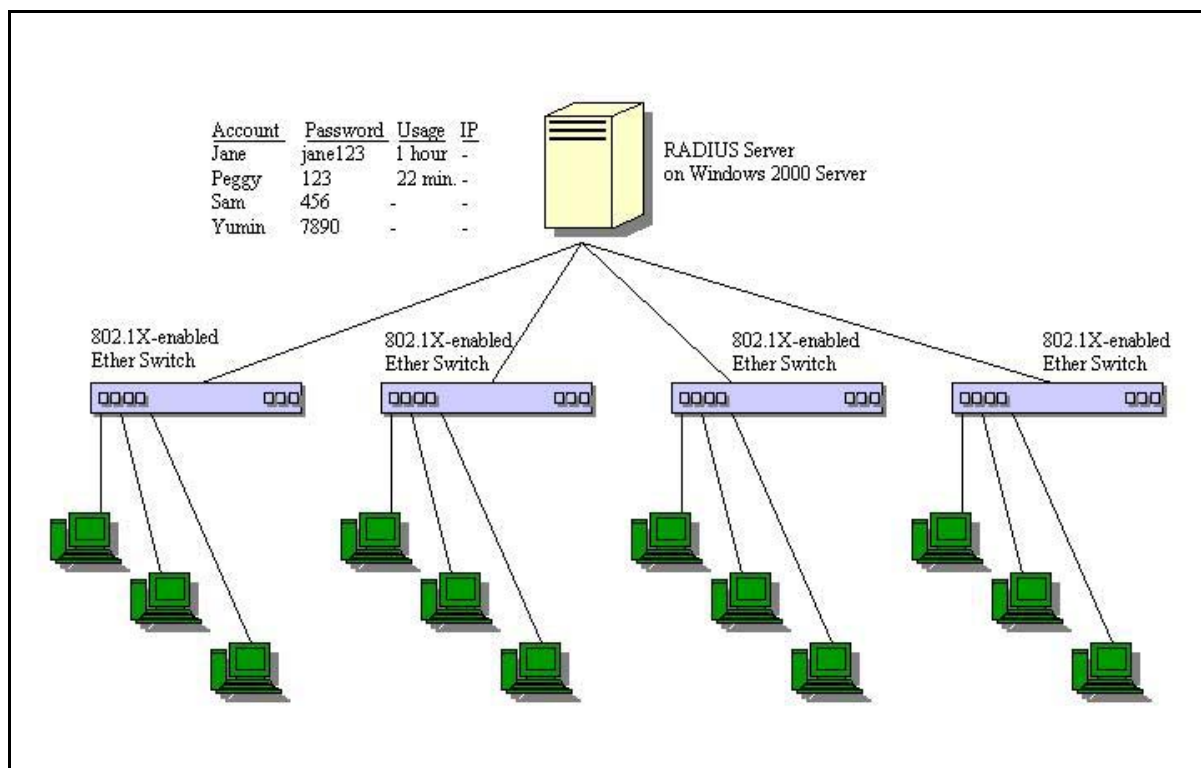
Once the user is authenticated, the Switch unblocks the port that is connected to the user as shown in the next figure.





**Figure 4- 12. 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- 13. 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- 1. Conformance to IEEE 802.1X Standards

## 802.1X Authenticator Settings

To display the current 802.1X Authenticator Settings on the Switch, open the **Port Access Entity** folder and 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- 14. 1<sup>st</sup> 802.1X Authenticator Settings window

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 1
To	Port 1
AdmDir	both
PortControl	Auto
TxPeriod	30
QuietPeriod	60
SuppTimeout	30
ServerTimeout	30
MaxReq	2
ReAuthPeriod	3600
ReAuth	Disabled

[Show Authenticators Setting for Unit 15](#)

Apply

Figure 4- 15. 2<sup>nd</sup> 802.1X Authenticator Settings window

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.
<b>PortControl</b>	This allows you to control the port authorization state.
	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.
<b>TxPeriod</b>	The default setting is <i>Auto</i> .
	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 **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	None	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- 16. 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.

## 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**.

Succession	Radius Server	Auth UDP Port	Acct UDP Port	Status
First				
Second				
Third				

**Figure 4- 17. 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.
<b>Status</b>	This drop-down menu allows you to select <i>Valid</i> or <i>Invalid</i> .

## 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.

Current IGMP Snooping Group Entries				
VLAN ID	VLAN Name	State	Querier State	Modify
1	default	Disabled	Non-Querier	<a href="#">Modify</a>
2	v2	Disabled	Non-Querier	<a href="#">Modify</a>
3	v3	Disabled	Non-Querier	<a href="#">Modify</a>

**Figure 4- 18. Current IGMP Snooping Group Entries window**

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

IGMP Snooping Settings	
VLAN ID	<input type="text" value="1"/>
VLAN Name	<input type="text" value="default"/>
Query Interval	<input type="text" value="125"/>
Max Response Time	<input type="text" value="10"/>
Robustness Value	<input type="text" value="2"/>
Last Member Query Interval	<input type="text" value="1"/>
Host Timeout	<input type="text" value="260"/>
Route Timeout	<input type="text" value="260"/>
Leave Timer	<input type="text" value="2"/>
Querier State	<input type="text" value="Disabled"/>
State	<input type="text" value="Disabled"/>
<input type="button" value="Apply"/>	
<a href="#">Show All IGMP Group Entries</a>	

**Figure 4- 19. IGMP Snooping Settings window**

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.

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

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:

- 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 then 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

Figure 4- 20. Current Static Router Port Entries window



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.

Static Router Ports Settings												
VID	1											
VLAN Name	default											
Unit	15											
Member Ports												
1	2	3	4	5	6	7	8	9	10	11	12	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="button" value="Apply"/> <a href="#">Show All Static Router Ports Entries</a>												

**Figure 4- 21. Static Router Ports Settings window**

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 D-Link managed Ethernet Switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1d 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 IEEE 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, each link 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
Forwarding	Forwarding	Yes	Yes

**Table 4- 2. 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, 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.

## STP Switch 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: <math>2 * (\text{Forward Delay} - 1) \geq \text{Max Age}</math>,  <math>\text{Max Age} \geq 2 * (\text{Hello Time} + 1)</math></i></p>	

Figure 4- 22. Switch Spanning Tree Settings window

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.

**Bridge Forward Delay (4 - 30 sec)**  
<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.

**Bridge Priority (0 - 61440)** <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.

**STP Version**<rstp >

Choose *rstp* (default) or *Stp Compatibility*. Both versions use STP parameters in the same way. RSTP is fully compatible with IEEE 802.1d STP and will function with legacy equipment.

**Tx Hold Count(1-10)**  
<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.

**Forwarding BPDU**  
<Enabled >

This can be *Enabled* or *Disabled*. When it is *Enabled* it allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is *Enabled*.



**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  $\leq 2 \times$  (Forward Delay - 1 second)

Max. Age  $\geq 2 \times$  (Hello Time + 1 second)

## STP Port Settings

Unit	From	To	State	Cost	Priority	Migration	Edge	P2P	Apply
15	Port 1	Port 1	Disabled	0	0	No	No	No	Apply

The STP Port Information									
Port	Designated Bridge	State	Cost	Priority	Edge	P2P	STP Status	Role	
1	N/A		*200000	Stacking Link Port					
2	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled	
3	N/A	Yes	*200000	128	No	Yes	Forwarding	NonStp	
4	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled	
5	N/A		*200000	Stacking Link Port					
6	N/A		*200000	Stacking Link Port					
7	N/A		*200000	Stacking Link Port					
8	N/A		*200000	Stacking Link Port					
9	N/A	Yes	*200000	128	No	Yes	Forwarding	NonStp	
10	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled	
11	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled	
12	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled	

Figure 4- 23. STP Port Settings window

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 DGS-3312SR 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.

Figure 4- 24. Setup Static Unicast Forwarding Table window

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 figure and table describe 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:

Figure 4- 25. Static Multicast Forwarding Settings window

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.

Setup Static Multicast Forwarding Table													
Unit	VID	Multicast MAC Address											
15	0	00-00-00-00-00-00											
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 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"/>
Apply													
<a href="#">Show All Multicast Forwarding Entries</a>													

Figure 4- 26. Setup Static Multicast Forwarding Table window

The following parameters can be set:

Parameter	Description
<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.

## 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.

VLANs can function somewhat differently in a Layer 3 Switch, that is when the VLANs are Layer 3-based, than if they are strictly based on Layer 2 information. Since IP Switching among VLANs may be unfamiliar to users who are otherwise well acquainted with conventional VLANs used in standard Ethernet Switches, some explanation of VLANs used in Layer 3 Switching is presented below. It is essential to fully grasp this difference to take advantage of the improved efficiency of Layer 3 Switching.

### VLANs in Layer 2

In normal 802.1Q VLAN implementation, packets cannot cross VLANs in a Switch that is limited to Layer 2 functions. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

### Layer 3-Based VLANs

Layer 3-based VLANs use network-layer addresses (subnet address for TCP/IP) to determine VLAN membership. These VLANs are based on layer 3 information, however this does not constitute a 'routing' function.

The DGS-3312SR and associated DGS-3312SR series Switches allow an IP subnet to be configured for each 802.1Q VLAN that exists on the Switch. That is, a VLAN can be associated or attached to an IP subnet. This represents an improvement in performance since it bypasses any routing functions, packets transferred between subnets are reduced to a "hardware" decision.

Even though a Switch inspects a packet's IP address to determine VLAN membership, no route calculation is performed, the RIP protocol is not employed, and packets traversing the Switch are bridged using the Spanning Tree algorithm.

A Switch that implements layer 3 (or ‘subnet’) VLANs without performing any routing function between these VLANs is referred to as performing ‘IP Switching’.

## Planning VLAN Layout

VLANs on the DGS-3312SR and DES-3226S series Switches have considerably more functions and are more complex than on a traditional layer 2 Switch, and must therefore be laid-out and configured with a bit more forethought. VLANs with an IP interface assigned to them could be thought of as network links – not just as a collection of associated end users. Further, VLANs assigned an IP network address and subnet mask enables IP routing between them.

VLANs must be configured on the Switch before they can be assigned IP subnets. Furthermore, the static VLAN configuration is specified on a per port basis. On the DGS-3312SR, a VLAN can consist of end-nodes – just like a traditional layer 2 Switch, but a VLAN can also consist of one or more Switches – each of which is connected to multiple end-nodes or network resources.

So, the IP subnets for a network must be determined first, and the VLANs configured on the Switch to accommodate the IP subnets. Finally, the IP subnets can be assigned to the VLANs.

## Assigning IP Network Addresses and Subnet Masks to VLANs

The DGS-3312SR allows the assignment of IP subnets to individual VLANs. This is the fundamental advantage of VLANs in IP Switching.

Developing an IP addressing scheme is a complex subject, but it is sufficient here to mention that the total number of anticipated end nodes – for each IP interface – must be accommodated with a unique IP address. It should be noted that the Switch regards a VLAN with an IP network address and corresponding subnet mask assigned as an IP interface.

## 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 DGS-3312SR 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.

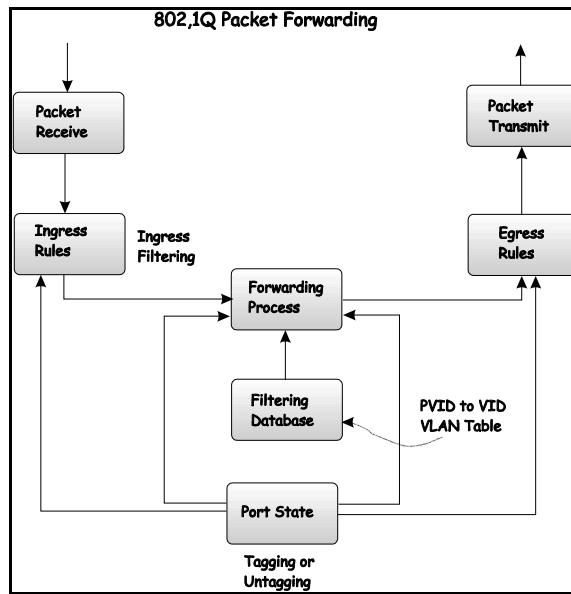


Figure 4- 27. 802.1Q Packet Forwarding

## 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.

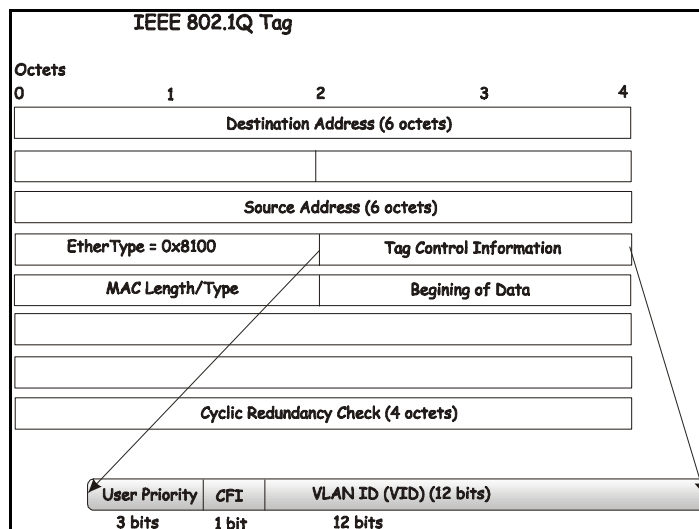


Figure 4- 28. IEEE 802.1Q Tag

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.



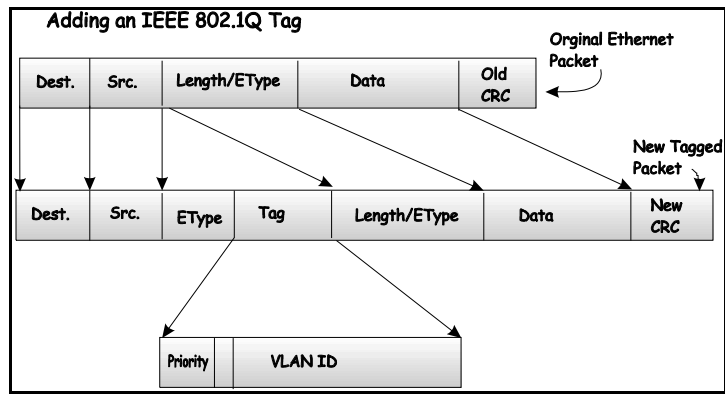


Figure 4- 29. Adding an IEEE 802.1Q Tag

## 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

Figure 4- 30. 1<sup>st</sup> 802.1Q Static VLANs window

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.

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

[Show All Static VLAN Entries](#) Apply

Figure 4- 31. 2<sup>nd</sup> 802.1Q Static VLANs window

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.
<b>Egress</b>	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.
<b>Forbidden</b>	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.

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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" 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"/>	<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"/>	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Apply												
<a href="#">Show All Static VLAN Entries</a>												

Figure 4- 32. Add New Static VLAN Example window

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.

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	<input checked="" type="checkbox"/>
11	engineering	Modify	<input checked="" type="checkbox"/>

Figure 4- 33. 802.1Q Static VLANs With Added VLAN window

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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<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"/>	<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"/>	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Apply												

Figure 4- 34. 802.1Q Static VLANs – Modify window

## 802.1Q Port Settings

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.

**802.1Q Port Settings**

Unit	From	To	Ingress Check	Frame Type	PVID	GVRP	Apply
15 ▾	Port 1 ▾	Port 1 ▾	Disabled ▾	Admit_all ▾	1	Disabled ▾	Apply

**802.1Q Port Table**

Port	PVID	Ingress	Frame Type	GVRP
1	0	Disabled	All frames	Enabled
2	1	Enabled	All frames	Disabled
3	1	Enabled	All frames	Disabled
4	1	Enabled	All frames	Disabled
5	0	Disabled	All frames	Disabled
6	0	Disabled	All frames	Disabled
7	0	Disabled	All frames	Disabled
8	0	Disabled	All frames	Disabled
9	1	Enabled	All frames	Disabled
10	1	Enabled	All frames	Disabled
11	1	Enabled	All frames	Disabled
12	1	Enabled	All frames	Disabled

**Figure 4- 35. 802.1Q Port Settings window**

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>	<p>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.</p>
<b>Frame Type</b>	<p>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.</p>

**PVID**

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 eight hardware queues. Therefore, the Switch must have a means of mapping the eight levels specified in the IEEE 802.1p standard to the eight 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:

Port Default Priority assignment				
Unit	From	To	Priority(0~7)	Apply
15	Port 1	Port 1	0	Apply

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

Figure 4- 36. Port Default Priority assignment window

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 DGS-3312SR 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- 37. User Priority Configuration window

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- 38. QoS Output Scheduling Configuration window**

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.



Traffic Segmentation Setting				
Unit	Port	Portlist	Configuration	Apply
15 ▾	Port 1 ▾	<input type="text"/>	<input type="button" value="View"/>	<input type="button" value="Apply"/>

Current Traffic Segmentation Table	
Unit	Forward Portlist
15	1-12
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

Figure 4- 39. Traffic Segmentation Setting window

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.

## Bandwidth Control

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

Bandwidth Settings						
Unit	From	To	Type	no_limit	Rate	Apply
15	Port 1	Port 1	RX	Disabled	1	Apply

Port Bandwidth Table		
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- 40. Bandwidth Settings window

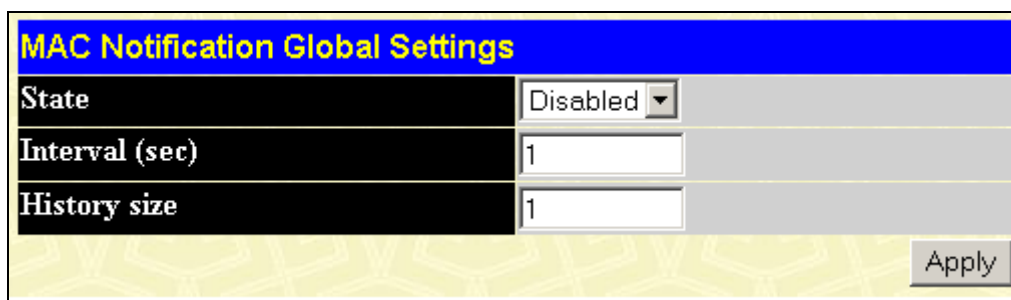
The following parameters can be set or are displayed:

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.

## MAC Notification Global Settings



MAC Notification Global Settings	
State	Disabled
Interval (sec)	1
History size	1
<input type="button" value="Apply"/>	

**Figure 4- 41. MAC Notification Global Settings window**

The following parameters can be set:

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

## MAC Notification 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- 42. MAC Notification Port Settings window**

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.

Index	Server IP	Severity	Facility	UDP Port	Status	Delete
-------	-----------	----------	----------	----------	--------	--------

Figure 4- 43. System Log Servers window

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.

Index	0
Server IP	0.0.0.0
Severity	Warning
Facility	Local0
UDP Port	0
Status	Disabled

[Show All System Log Servers](#)

Figure 4- 44. System Log Server – Add window

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>	<table> <tr> <th>Numerical Code</th><th>Facility</th></tr> <tr> <td>0</td><td>kernel messages</td></tr> <tr> <td>1</td><td>user-level messages</td></tr> <tr> <td>2</td><td>mail system</td></tr> <tr> <td>3</td><td>system daemons</td></tr> <tr> <td>4</td><td>security/authorization messages</td></tr> <tr> <td>5</td><td>messages generated internally by syslog line printer subsystem</td></tr> <tr> <td>7</td><td>network news subsystem</td></tr> </table>	Numerical Code	Facility	0	kernel messages	1	user-level messages	2	mail system	3	system daemons	4	security/authorization messages	5	messages generated internally by syslog line printer subsystem	7	network news subsystem
Numerical Code	Facility																
0	kernel messages																
1	user-level messages																
2	mail system																
3	system daemons																
4	security/authorization messages																
5	messages generated internally by syslog line printer subsystem																
7	network news subsystem																

- 8 UUCP subsystem
- 9 clock daemon
- 10 security/authorization messages
- 11 FTP daemon
- 12 NTP subsystem
- 13 log audit
- 14 log alert
- 15 clock daemon
- 16 **local use 0 (local0)**
- 17 **local use 1 (local1)**
- 18 **local use 2 (local2)**
- 19 **local use 3 (local3)**
- 20 **local use 4 (local4)**
- 21 **local use 5 (local5)**
- 22 **local use 6 (local6)**
- 23 **local use 7 (local7)**

**UDP Port** Type the UDP port number used for sending Syslog messages. The default is 514.

**Status** Choose *Enabled* or *Disabled* 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- 45. Port Security Settings window**

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.
<b>Lock Address Mode</b>	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 <i>Permanent</i> , <i>DeleteOnReset</i> , and <i>DeleteOnTimeout</i> .

## SNTP Setting

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

### Time Setting

The screenshot displays a web-based configuration interface for a switch. It is divided into three main sections, each with a blue header bar:

- Current Time: Status**: This section shows the current system time as '0 days 20:00:14' and the time source as 'System Clock'.
- Current Time: SNTP Settings**: This section contains four rows of configuration options:
  - SNTP State**: A dropdown menu currently set to 'Disabled'.
  - SNTP Primary Server**: A text input field containing '0.0.0.0'.
  - SNTP Secondary Server**: A text input field containing '0.0.0.0'.
  - SNTP Poll Interval in Seconds**: A text input field containing '720'.
 An 'Apply' button is located at the bottom right of this section.
- Current Time: Set Current Time**: This section allows manual time setting with four rows of dropdown menus:
  - Year**: A dropdown menu.
  - Month**: A dropdown menu.
  - Day**: A dropdown menu.
  - Time in HH MM SS**: Three separate dropdown menus for hours, minutes, and seconds.
 An 'Apply' button is located at the bottom right of this section.

Figure 4- 46. Current Time: Status window

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 in Seconds</b>	This is the interval between requests for updated SNTP information.
<b>Year</b>	Enter the current year, if you want to update the system clock.
<b>Month</b>	Enter the current month, if you want to update the system clock.
<b>Day</b>	Enter the current day, if you want to update the system clock.
<b>Time in HH MM SS</b>	Enter the current time in hours, minutes, and seconds, if you want to update the system clock.

## Time Zone and DST 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- 47. Time Zone and DST Settings window**

The following parameters can set:



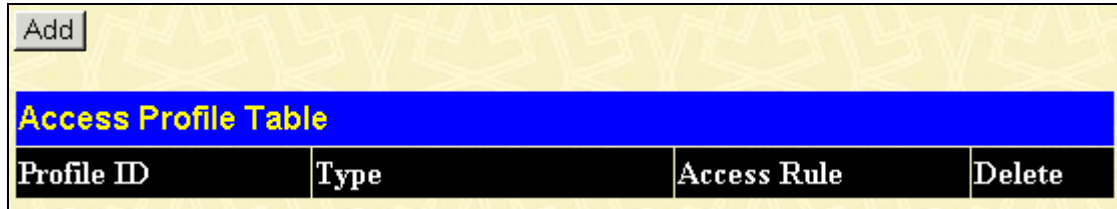
Parameter	Description
<b>Daylight Saving Time State</b>	Use this pull-down menu to enable or disable the DST Settings.
<b>Daylight Saving Time Offset in Minutes</b>	Use this pull-down menu to specify the amount of time that will constitute your local DST offset – 30, 60, 90, or 120 minutes.
<b>Time Zone 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.
<b>To: What Time</b>	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.

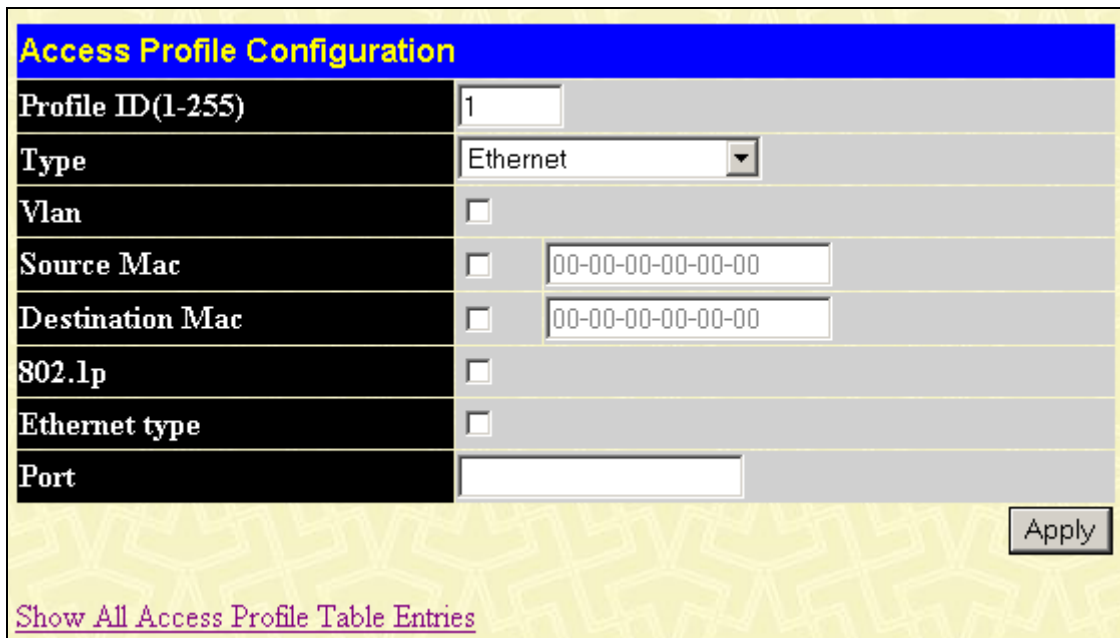


The image shows a web interface window titled 'Access Profile Table'. At the top left is an 'Add' button. Below the title bar is a table with four columns: 'Profile ID', 'Type', 'Access Rule', and 'Delete'.

Profile ID	Type	Access Rule	Delete
------------	------	-------------	--------

**Figure 4- 48. 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 three **Access Profile Configuration** windows – one for Ethernet (or MAC address-based) profile configuration, one for IP address-based profile configuration, and one for Packet Content Mask-based profile configuration. You can Switch among the three **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.



The image shows a web interface window titled 'Access Profile Configuration'. It contains several fields for configuring an Ethernet-based profile:

- Profile ID(1-255)**: Text input field with '1' entered.
- Type**: Drop-down menu with 'Ethernet' selected.
- Vlan**: Check box (unchecked).
- Source Mac**: Check box (unchecked) and text input field with '00-00-00-00-00-00'.
- Destination Mac**: Check box (unchecked) and text input field with '00-00-00-00-00-00'.
- 802.1p**: Check box (unchecked).
- Ethernet type**: Check box (unchecked).
- Port**: Text input field.

At the bottom right is an 'Apply' button. At the bottom left is a link: [Show All Access Profile Table Entries](#).

**Figure 4- 49. Access Profile Configuration (Ethernet) 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), IP address or packet content mask. 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. Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet 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>Port</b>	The user may set the <b>Access Profile Table</b> window on a per-port basis by entering a port number in this field. Entering "all" will denote all ports on the Switch.

The page shown below is the **Access Profile Configuration** window for IP:

Access Profile Configuration			
Profile ID(1-255)	<input type="text" value="1"/>		
Type	IP <input type="button" value="v"/>		
Vlan	<input type="checkbox"/>		
Source IP Mask	<input type="checkbox"/>	<input type="text"/>	
Destination IP Mask	<input type="checkbox"/>	<input type="text"/>	
Dscp	<input type="checkbox"/>		
Protocol	<input type="checkbox"/>	<input checked="" type="radio"/> ICMP <input type="checkbox"/> type <input type="checkbox"/> code	
		<input type="radio"/> IGMP <input type="checkbox"/> type	
		<input 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="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="radio"/> protocol id           user mask <input type="text" value="00000000"/>	
Port	<input type="text"/>		
<input type="button" value="Apply"/>			
<a href="#">Show All Access Profile Table Entries</a>			

**Figure 4- 50. 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), IP address or packet content mask. 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. Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet 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>	<p>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.</p> <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 <i>ICMP</i> to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.</p> <ul style="list-style-type: none"> <li>Select <i>type</i> 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.</li> </ul> <p>Select <i>IGMP</i> to instruct the Switch to examine the Internet Group Management Protocol (ICMP) field in each frame's header.</p> <ul style="list-style-type: none"> <li>Select <i>type</i> to further specify that the access profile will apply an IGMP type value</li> </ul> <p>Select <i>TCP</i> 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> <ul style="list-style-type: none"> <li><i>src port mask</i> – Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff).</li> <li><i>dest port mask</i> – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff).</li> <li><i>flag bit</i> – Specify a flag bite in the TCP header.</li> </ul> <p>Select <i>UDP</i> 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> <ul style="list-style-type: none"> <li><i>src port mask</i> – Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff).</li> <li><i>dest port mask</i> – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff).</li> </ul> <p>protocol id – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffffffff).</p>
<b>Protocol</b>	

**Port**

The user may set the Access Profile Table window on a per-port basis by entering a port number in this field. Entering "all" will denote all ports on the Switch.

The window shown below is the **Access Profile Configuration** window for Packet Content Mask.

Access Profile Configuration			
Profile ID(1-255)	1		
Type	Packet Content Mask		
Offset	<input type="checkbox"/> value(0-15)	mask	00000000
		mask	00000000
		mask	00000000
		mask	00000000
	<input type="checkbox"/> value(16-31)	mask	00000000
		mask	00000000
		mask	00000000
		mask	00000000
	<input type="checkbox"/> value(32-47)	mask	00000000
		mask	00000000
		mask	00000000
		mask	00000000
	<input type="checkbox"/> value(48-63)	mask	00000000
		mask	00000000
		mask	00000000
		mask	00000000
	<input type="checkbox"/> value(64-79)	mask	00000000
		mask	00000000
		mask	00000000
		mask	00000000
Port			
Apply			
<a href="#">Show All Access Profile Table Entries</a>			

**Figure 4- 51. Access Profile Configuration (Packet Content Mask) window**

This window will aid the user in configuring the Switch to mask packet headers beginning with the offset value specified. The following fields are used to configure the Packet Content Masks:

The following parameters can be set:

Parameter	Description
Profile ID(1-255)	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.

Select profile based on *Ethernet* (MAC Address), *IP* address or *packet content mask*. This will change the menu according to the requirements for the type of profile.

### Type

- Select *Ethernet* to instruct the Switch to examine the layer 2 part of each packet header.
- Select *IP* to instruct the Switch to examine the IP address in each frame's header.
- Select *Packet Content Mask* to specify a mask to hide the content of the packet header.

This field will instruct the switch to mask the packet header beginning with the offset value specified:

### Offset

- *value(0-15)* - Enter a value in hex form to mask the packet from the beginning of the packet to the 16th byte.
- *value(16-31)* - Enter a value in hex form to mask the packet from byte 16 to byte 31.
- *value(32-47)* - Enter a value in hex form to mask the packet from byte 32 to byte 47.
- *value(48-63)* - Enter a value in hex form to mask the packet from byte 48 to byte 63.
- *value(64-79)* - Enter a value in hex form to mask the packet from byte 64 to byte 79.

### Port

The user may set the Access Profile Table window on a per-port basis by entering a port number in this field. Entering "all" will denote all ports on the Switch.

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- 52. Access Rule Table window**

To create a new rule set for the access profile, click the **Add** button. A new window is displayed. To remove a previously created rule, select it and click the **Delete** button.

Access Rule Configuration	
Profile ID	10
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Access ID	1
Type	Ethernet
Priority(0-7)	<input type="checkbox"/> 0 <input type="checkbox"/> replace priority
Replace Dscp(0-63)	<input type="checkbox"/> 0
Vlan Name	
Source Mac	00-00-00-00-00-00
Destination Mac	00-00-00-00-00-00
802.1p(0-7)	0
Ethernet Type	0000
<input type="button" value="Apply"/>	
<a href="#">Show All Access Rule Entries</a>	

**Figure 4- 53. Access Rule Configuration (Ethernet) 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>Mode</b>	<p>Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).</p> <p>Select <i>Deny</i> to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.</p>
<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>	<p>Select profile based on Ethernet (MAC Address), IP address or packet content mask. This will change the menu according to the requirements for the type of profile.</p> <ul style="list-style-type: none"> <li>Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header.</li> <li>Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header.</li> <li>Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header.</li> </ul>
<b>Priority(0-7)</b>	Specify the priority tag, located in the packet header that will be identified by the Switch.
<b>Replace Priority(0-7)</b>	This parameter is specified if you want to change the 802.1p user priority of a packet that meets the specified criteria. Otherwise, a packet will have its incoming 802.1p

user priority re-written to its original value before being transmitted from 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.

Access Rule Configuration	
Profile ID	15
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Access ID	1
Type	IP
Priority(0-7)	<input type="checkbox"/> 0 <input type="checkbox"/> replace priority
Replace Dscp(0-63)	<input type="checkbox"/> 0
Vlan Name	
Source IP	0.0.0.0
Destination IP	0.0.0.0
Dscp(0-63)	0
Protocol	Protocol id 00
	user define 00000000
<input type="button" value="Apply"/>	
<a href="#">Show All Access Rule Entries</a>	

**Figure 4- 54. 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>Mode</b>	<p>Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).</p> <p>Select <i>Deny</i> to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.</p>
<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>	<p>Select profile based on Ethernet (MAC Address), IP address or packet content mask. This will change the menu according to the requirements for the type of profile.</p> <ul style="list-style-type: none"><li>• Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header.</li><li>• Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header.</li><li>• Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header.</li></ul>
<b>Priority(0-7)</b>	Specify the priority tag, located in the packet header that will be identified by the Switch.
<b>Replace Dscp with(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>	<p>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.</p>
<b>Protocol</b>	<p>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.</p>

---

Access Rule Configuration			
Profile ID	1		
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Deny		
Access ID	1		
Type	Packet Content Mask		
Priority(0-7)	<input type="checkbox"/> <input type="text"/> <input type="checkbox"/> replace priority		
Replace Dscp(0-63)	<input type="checkbox"/> <input type="text"/>		
Offset	<input type="checkbox"/> value(0-15)	mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
	<input type="checkbox"/> value(16-31)	mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
	<input type="checkbox"/> value(32-47)	mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
	<input type="checkbox"/> value(48-63)	mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
	<input type="checkbox"/> value(64-79)	mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
		mask	<input type="text" value="00000000"/>
			<input type="button" value="Apply"/>
<a href="#">Show All Access Rule Entries</a>			

**Figure 4- 55. Access Rule Configuration (Package Content Mask) window**

Configure the Access Rule Configuration settings on the window above.

The following parameters can be set:

Parameter	Description
Profile ID	This is the identifier number for this profile set.

<b>Mode</b>	<p>Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).</p> <p>Select <i>Deny</i> to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.</p>
<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>	<p>Select profile based on Ethernet (MAC Address), IP address or packet content mask. This will change the menu according to the requirements for the type of profile.</p> <ul style="list-style-type: none"><li>• Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header.</li><li>• Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header.</li><li>• Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header.</li></ul>
<b>Priority(0-7)</b>	Specify the priority tag, located in the packet header that will be identified by the Switch.
<b>Replace Dscp with(0-63)</b>	<p>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.</p> <p>This field will instruct the switch to match the packet header beginning with the offset value specified:</p> <ul style="list-style-type: none"><li>• <i>value(0-15)</i> - Enter a value in hex form to match the packet from the beginning of the packet to the 16<sup>th</sup> byte.</li><li>• <i>value(16-31)</i> - Enter a value in hex form to match the packet from byte 16 to byte 31.</li><li>• <i>value(32-47)</i> - Enter a value in hex form to match the packet from byte 32 to byte 47.</li><li>• <i>value(48-63)</i> - Enter a value in hex form to match the packet from byte 48 to byte 63.</li><li>• <i>value(64-79)</i> - Enter a value in hex form to match the packet from byte 64 to byte 79.</li></ul>
<b>Offset</b>	

---

<h2>Section 5</h2>
--------------------

## Advanced Configuration

*L3 Global Advanced Settings*

*IP Interface Settings*

*MD5 Key Settings*

*Route Redistribution Settings*

*Static/Default Route Settings*

*Static ARP Settings*

*RIP*

*RIP Global Setting*

*RIP Interface Settings*

*OSPF*

*OSPF General Setting*

*OSPF Area ID Settings*

*OSPF Interface Settings*

*OSPF Virtual Interface Settings*

*OSPF Area Aggregation Settings*

*OSPF Host Route Settings*

*DHCP/BOOTP Relay*

*DHCP/BOOTP Relay Information*

*DHCP/BOOTP Relay Settings*

*DNS Relay*

*DNS Relay Information*

*DNS Relay Static Settings*

*VRRP*

*VRRP Configuration*

*VRRP Interface Settings*

*IP Multicast*

*IGMP Interface Settings*

*DVMRP*

*DVMRP Global Setting*

*DVMRP Interface Settings*

*PIM*

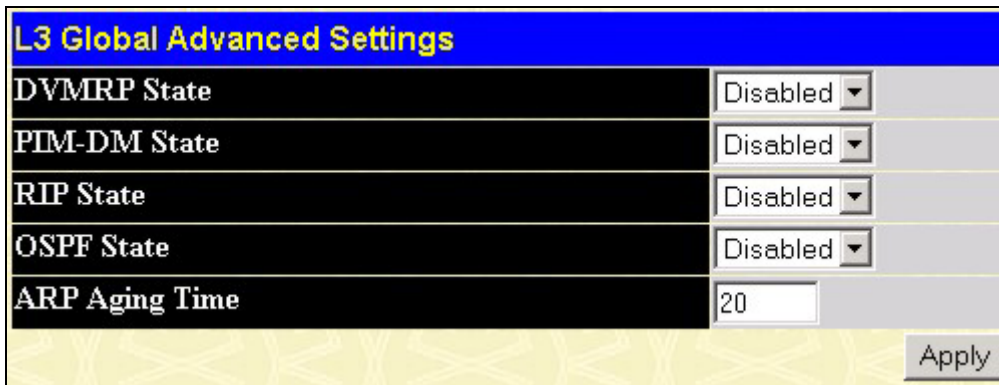
*PIM-DM Global Setting*

*PIM-DM Interface Settings*

## L3 Global Advanced Settings

In order to use DVMRP, PIM-DM, RIP, or OSPF, the Switch must first be globally enabled. To enable or disable these Layer 3 protocols as well as configure ARP Aging Time, access the **L3 Global Advanced Settings** window.

To enable DVMRP, PIM-DM, RIP or OSPF for the Switch, select *Enabled* for the global setting and click the **Apply** button. You may later select *Disabled* for any of these to disable the protocol without changing any of the settings that may have been configured for them.



**Figure 5- 1. L3 Global Advanced Settings window**

ARP aging timeout is the time in seconds that an entry is allowed to remain in the ARP dynamic entry table. To setup permanent entries for ARP, use the **Static ARP Settings** window (described later in this chapter).

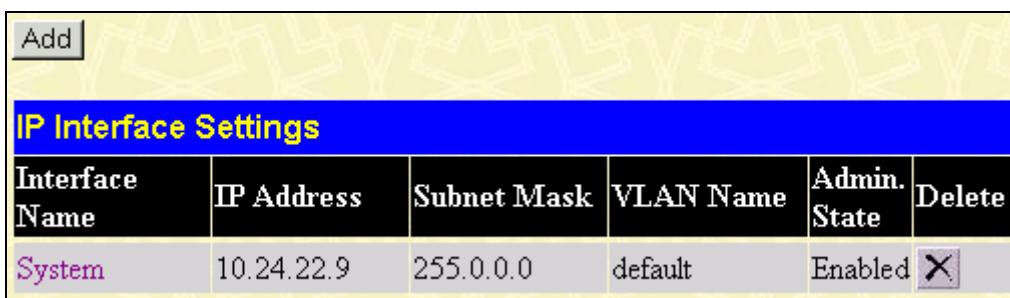


**NOTE:** PIM, RIP, OSPF, and DVMRP may also be globally enabled or disabled using a separate global settings window for each protocol. The links for the individual global settings windows are located in their respective subfolders.

## IP Interface Settings

Each VLAN must be configured prior to setting up the VLAN's corresponding IP interface.

To set up IP interfaces, open the **Layer 3 IP Networking** sub-folder in the **Configuration** folder and then click **IP Interfaces Settings** to open the following window:



Interface Name	IP Address	Subnet Mask	VLAN Name	Admin. State	Delete
<a href="#">System</a>	10.24.22.9	255.0.0.0	default	Enabled	X

**Figure 5- 2. 1<sup>st</sup> IP Interface Settings window**

Click the **Add** button to configure settings for a new IP interface. If you want to change an existing IP interface, click on the hyperlinked Interface Name in the list.

Figure 5- 3. 2<sup>nd</sup> IP Interface Settings window

Enter the desired IP interface settings and click the **Apply** button. A message should appear informing you if the settings have been successfully applied. For convenience, you may want to use the same name for the IP interface and the VLAN. To return to the first **IP Interface Settings** window, click the [Show ALL IP Interface Entries](#) link. The example pictured below follows the example IP interface setup discussed on the previous window.

Figure 5- 4. Example IP Interface Settings window

Choose a name for the interface to be added and enter it in the Interface Name field (if you are editing an IP Interface, the Interface Name will already be in the top field as seen in the window above). Enter the interface's IP address and subnet mask in the corresponding fields. Pull the Admin. State pull-down menu to *Enabled* and click **Apply** to enter to make the IP interface effective. Use **Save Changes** in the **Maintenance** folder to enter the changes into NV-RAM.

The following fields can be set:

Parameter	Description
<b>Interface Name</b>	This field displays the name for the IP interface. The default IP interface is named "System".
<b>IP Address</b>	Enter an IP address to be assigned to this IP interface.
<b>Subnet Mask</b>	Enter a subnet mask to be applied to this IP interface.
<b>VLAN Name</b>	Enter the VLAN Name for the VLAN the IP interface belongs to. The VLAN name

must match the existing

<b>Admin. State</b>	Select <i>Enabled</i> or <i>Disabled</i> to activate or deactivate the interface.
<b>Port/Member</b>	Specify which of the ports on the Switch will be a member of this VLAN.

---

## Introduction to OSPF

The Open Shortest Path First (OSPF) routing protocol that uses a *link-state* algorithm to determine routes to network destinations. A “link” is an interface on a router and the “state” is a description of that interface and its relationship to neighboring routers. The state contains information such as the IP address, subnet mask, type of network the interface is attached to, other routers attached to the network, etc. The collection of link-states are then collected in a link-state database that is maintained by routers running OSPF.

OSPF specifies how routers will communicate to maintain their link-state database and defines several concepts about the topology of networks that use OSPF.

To limit the extent of link-state update traffic between routers, OSPF defines the concept of *Area*. All routers within an area share the exact same link-state database, and a change to this database on one router triggers an update to the link-state database of all other routers in that area. Routers that have interfaces connected to more than one area are called *Border Routers* and take the responsibility of distributing routing information between areas.

One area is defined as *Area 0* or the *Backbone*. This area is central to the rest of the network in that all other areas have a connection (through a router) to the backbone. Only routers have connections to the backbone and OSPF is structured such that routing information changes in other areas will be introduced into the backbone, and then propagated to the rest of the network.

When constructing a network to use OSPF, it is generally advisable to begin with the backbone (area 0) and work outward.

## Link-State Algorithm

An OSPF router uses a link-state algorithm to build a shortest path tree to all destinations known to the router. The following is a simplified description of the algorithm’s steps:

1. When OSPF is started, or when a change in the routing information changes, the router generates a link-state advertisement. This advertisement is a specially formatted packet that contains information about all the link-states on the router.
2. This link-state advertisement is flooded to all router in the area. Each router that receives the link-state advertisement will store the advertisement and then forward a copy to other routers.
3. When the link-state database of each router is updated, the individual routers will calculate a Shortest Path Tree to all destinations – with the individual router as the root. The IP routing table will then be made up of the destination address, associated cost, and the address of the next hop to reach each destination.
4. Once the link-state databases are updated, Shortest Path Trees calculated, and the IP routing tables written – if there are no subsequent changes in the OSPF network (such as a network link going down) there is very little OSPF traffic.

## Shortest Path Algorithm

The Shortest Path to a destination is calculated using the Dijkstra algorithm. Each router is places at the root of a tree and then calculates the shortest path to each destination based on the cumulative cost to reach that destination over multiple possible routes. Each router will then have its own Shortest Path Tree (from the perspective of its location in the network area) even though every router in the area will have and use the exact same link-state database.

The following sections describe the information used to build the Shortest Path Tree.

## OSPF Cost

Each OSPF interface has an associated cost (also called “metric”) that is representative of the overhead required to send packets over that interface. This cost is inversely proportional to the bandwidth of the interface (i.e. a higher bandwidth interface has a lower cost). There is then a higher cost (and longer time delays) in sending packets over a 56 Kbps dial-up connection than over a 10 Mbps Ethernet connection. The formula used to calculate the OSPF cost is as follows:

$$\text{Cost} = 100,000,000 / \text{bandwidth in bps}$$

As an example, the cost of a 10 Mbps Ethernet line will be 10 and the cost to cross a 1.544 Mbps T1 line will be 64.

### Shortest Path Tree

To build Router A's shortest path tree for the network diagramed below, Router A is put at the root of the tree and the smallest cost link to each destination network is calculated.

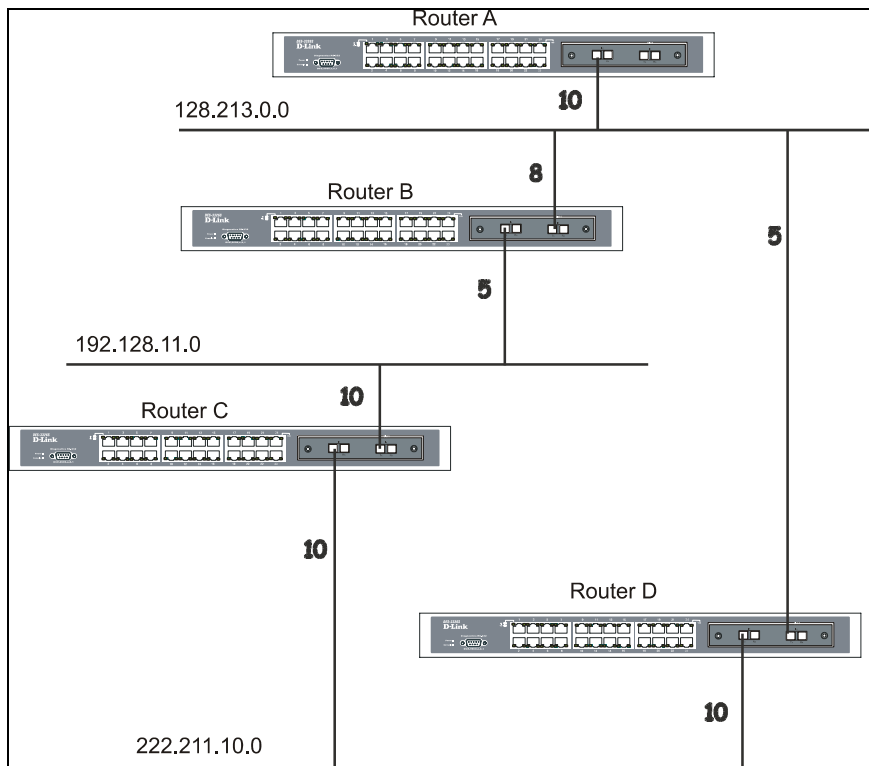


Figure 5- 5. Constructing a Shortest Path Tree

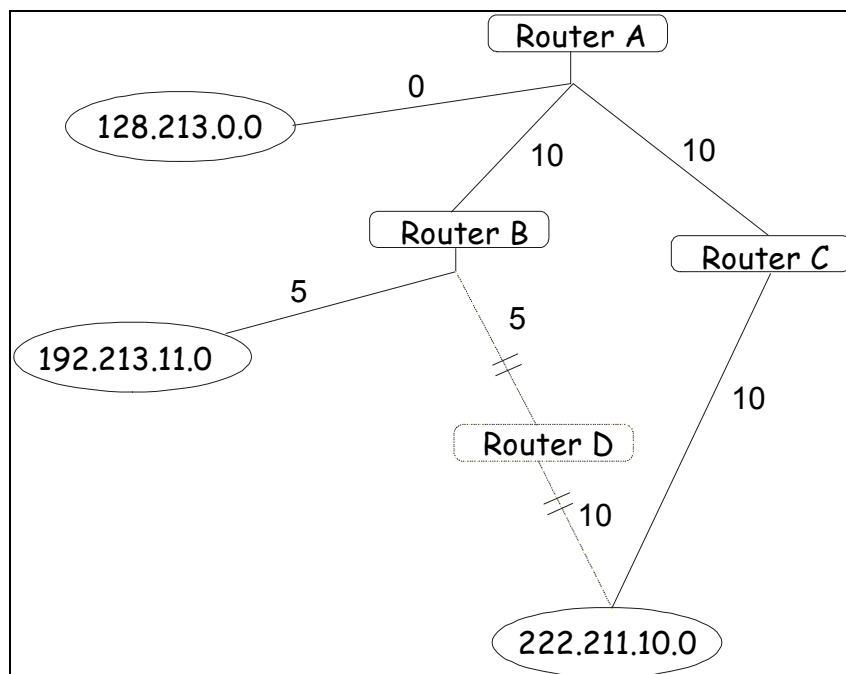
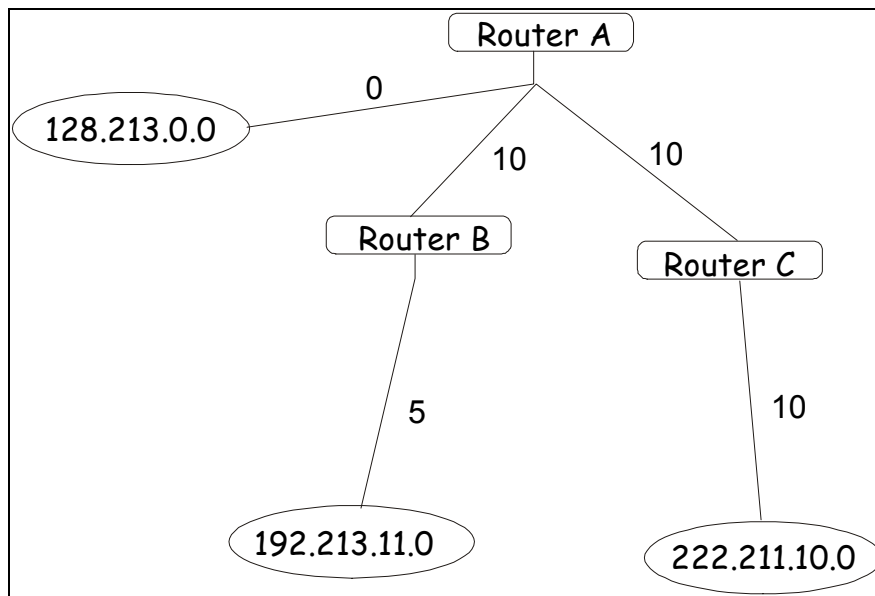


Figure 5- 6. Constructing a Shortest Path Tree

The diagram above shows the network from the viewpoint of Router A. Router A can reach 192.213.11.0 through Router B with a cost of  $10+5=15$ . Router A can reach 222.211.10.0 through Router C with a cost of  $10+10=20$ . Router A can also reach 222.211.10.0 through Router B and Router D with a cost of  $10+5+10=25$ , but the cost is higher than the route



through Router C. This higher-cost route will not be included in the Router A's shortest path tree. The resulting tree will look like this:



**Figure 5- 7. Constructing a Shortest Path Tree - Completed**

Note that this shortest path tree is only from the viewpoint of Router A. The cost of the link from Router B to Router A, for instance is not important to constructing Router A's shortest path tree, but is very important when Router B is constructing its shortest path tree.

Note also that directly connected networks are reached at a cost of 0, while other networks are reached at the cost calculated in the shortest path tree.

Router A can now build its routing table using the network addresses and costs calculated in building the above shortest path tree.

## Areas and Border Routers

OSPF link-state updates are forwarded to other routers by flooding to all routers on the network. OSPF uses the concept of areas to define where on the network routers that need to receive particular link-state updates are located. This helps ensure that routing updates are not flooded throughout the entire network and to reduce the amount of bandwidth consumed by updating the various router's routing tables.

Areas establish boundaries beyond which link-state updates do not need to be flooded. So the exchange of link-state updates and the calculation of the shortest path tree are limited to the area that the router is connected to.

Routers that have connections to more than one area are called Border Routers (BR). The Border Routers have the responsibility of distributing necessary routing information and changes between areas.

Areas are specific to the router interface. A router that has all of its interfaces in the same area is called an Internal Router. A router that has interfaces in multiple areas is called a Border Router. Routers that act as gateways to other networks (possibly using other routing protocols) are called Autonomous System Border Routers (ASBRs).

## Link-State Packets

There are different types of link-state packets, four are illustrated below:

- Router Link-State Updates – these describe a router's links to destinations within an area.
- Summary Link-State Updates – issued by Border Routers and describe links to networks outside the area but within the Autonomous System (AS).
- Network Link-State Updates – issued by multi-access areas that have more than one attached router. One router is elected as the Designated Router (DR) and this router issues the network link-state updates describing every router on the segment.
- External Link-State Updates – issued by an Autonomous System Border Router and describes routes to destinations outside the AS or a default route to the outside AS.

The format of these link-state updates is described in more detail below.

Router link-state updates are flooded to all routers in the current area. These updates describe the destinations reachable through all of the router's interfaces.

Summary link-state updates are generated by Border Routers to distribute routing information about other networks within the AS. Normally, all Summary link-state updates are forwarded to the backbone (area 0) and are then forwarded to all other areas in the network. Border Routers also have the responsibility of distributing routing information from the Autonomous System Border Router in order for routers in the network to get and maintain routes to other Autonomous Systems.

Network link-state updates are generated by a router elected as the Designated Router on a multi-access segment (with more than one attached router). These updates describe all of the routers on the segment and their network connections.

External link-state updates carry routing information to networks outside the Autonomous System. The Autonomous System Border Router is responsible for generating and distributing these updates.

## **OSPF Authentication**

OSPF packets can be authenticated as coming from trusted routers by the use of predefined passwords. The default for routers is to use not authentication.

There are two other authentication methods – simple password authentication (key) and Message Digest authentication (MD-5).

### **Message Digest Authentication (MD-5)**

MD-5 authentication is a cryptographic method. A key and a key-ID are configured on each router. The router then uses an algorithm to generate a mathematical “message digest” that is derived from the OSPF packet, the key and the key-ID. This message digest (a number) is then appended to the packet. The key is not exchanged over the wire and a non-decreasing sequence number is included to prevent replay attacks.

### **Simple Password Authentication**

A password (or key) can be configured on a per-area basis. Routers in the same area that participate in the routing domain must be configured with the same key. This method is possibly vulnerable to passive attacks where a link analyzer is used to obtain the password.

## **Backbone and Area 0**

OSPF limits the number of link-state updates required between routers by defining areas within which a given router operates. When more than one area is configured, one area is designated as area 0 – also called the backbone.

The backbone is at the center of all other areas – all areas of the network have a physical (or virtual) connection to the backbone through a router. OSPF allows routing information to be distributed by forwarding it into area 0, from which the information can be forwarded to all other areas (and all other routers) on the network.

In situations where an area is required, but is not possible to provide a physical connection to the backbone, a virtual link can be configured.

## **Virtual Links**

Virtual links accomplish two purposes:

1. Linking an area that does not have a physical connection to the backbone.
2. Patching the backbone in case there is a discontinuity in area 0.

### **Areas Not Physically Connected to Area 0**

All areas of an OSPF network should have a physical connection to the backbone, but in some cases it is not possible to physically connect a remote area to the backbone. In these cases, a virtual link is configured to connect the remote area to the backbone. A virtual path is a logical path between two border routers that have a common area, with one border router connected to the backbone.

## **Partitioning the Backbone**

OSPF also allows virtual links to be configured to connect the parts of the backbone that are discontinuous. This is the equivalent to linking different area 0s together using a logical path between each area 0. Virtual links can also be added for

redundancy to protect against a router failure. A virtual link is configured between two border routers that both have a connection to their respective area 0s.

## Neighbors

Routers that are connected to the same area or segment become neighbors in that area. Neighbors are elected via the Hello protocol. IP multicast is used to send out Hello packets to other routers on the segment. Routers become neighbors when they see themselves listed in a Hello packet sent by another router on the same segment. In this way, two-way communication is guaranteed to be possible between any two neighbor routers.

Any two routers must meet the following conditions before they become neighbors:

- **Area ID** – Two routers having a common segment – their interfaces have to belong to the same area on that segment. Of course, the interfaces should belong to the same subnet and have the same subnet mask.
- **Authentication** – OSPF allows for the configuration of a password for a specific area. Two routers on the same segment and belonging to the same area must also have the same OSPF password before they can become neighbors.
- **Hello and Dead Intervals** – The Hello interval specifies the length of time, in seconds, between the hello packets that a router sends on an OSPF interface. The dead interval is the number of seconds that a router's Hello packets have not been seen before its neighbors declare the OSPF router down. OSPF routers exchange Hello packets on each segment in order to acknowledge each other's existence on a segment and to elect a Designated Router on multi-access segments. OSPF requires these intervals to be exactly the same between any two neighbors. If any of these intervals are different, these routers will not become neighbors on a particular segment.
- **Stub Area Flag** – any two routers also have to have the same stub area flag in their Hello packets in order to become neighbors.

## Adjacencies

Adjacent routers go beyond the simple Hello exchange and participate in the link-state database exchange process. OSPF elects one router as the Designated Router (DR) and a second router as the Backup Designated Router (BDR) on each multi-access segment (the BDR is a backup in case of a DR failure). All other routers on the segment will then contact the DR for link-state database updates and exchanges. This limits the bandwidth required for link-state database updates.

## Designated Router Election

The election of the DR and BDR is accomplished using the Hello protocol. The router with the highest OSPF priority on a given multi-access segment will become the DR for that segment. In case of a tie, the router with the highest Router ID wins. The default OSPF priority is 1. A priority of zero indicates a router that cannot be elected as the DR.

## Building Adjacency

Two routers undergo a multi-step process in building the adjacency relationship. The following is a simplified description of the steps required:

- **Down** – No information has been received from any router on the segment.
- **Attempt** – On non-broadcast multi-access networks (such as Frame Relay or X.25), this state indicates that no recent information has been received from the neighbor. An effort should be made to contact the neighbor by sending Hello packets at the reduced rate set by the Poll Interval.
- **Init** – The interface has detected a Hello packet coming from a neighbor but bi-directional communication has not yet been established.
- **Two-way** – Bi-directional communication with a neighbor has been established. The router has seen its address in the Hello packets coming from a neighbor. At the end of this stage the DR and BDR election would have been done. At the end of the Two-way stage, routers will decide whether to proceed in building an adjacency or not. The decision is based on whether one of the routers is a DR or a BDR or the link is a point-to-point or virtual link.
- **Exstart** – (Exchange Start) Routers establish the initial sequence number that is going to be used in the information exchange packets. The sequence number insures that routers always get the most recent information. One router will become the primary and the other will become secondary. The primary router will poll the secondary for information.

- **Exchange** – Routers will describe their entire link-state database by sending database description packets.
- **Loading** – The routers are finalizing the information exchange. Routers have link-state request list and a link-state retransmission list. Any information that looks incomplete or outdated will be put on the request list. Any update that is sent will be put on the retransmission list until it gets acknowledged.
- **Full** – The adjacency is now complete. The neighboring routers are fully adjacent. Adjacent routers will have the same link-state database.

## Adjacencies on Point-to-Point Interfaces

OSPF Routers that are linked using point-to-point interfaces (such as serial links) will always form adjacencies. The concepts of DR and BDR are unnecessary.

## OSPF Packet Formats

All OSPF packet types begin with a standard 24-byte header and there are five packet types. The header is described first, and each packet type is described in a subsequent section.

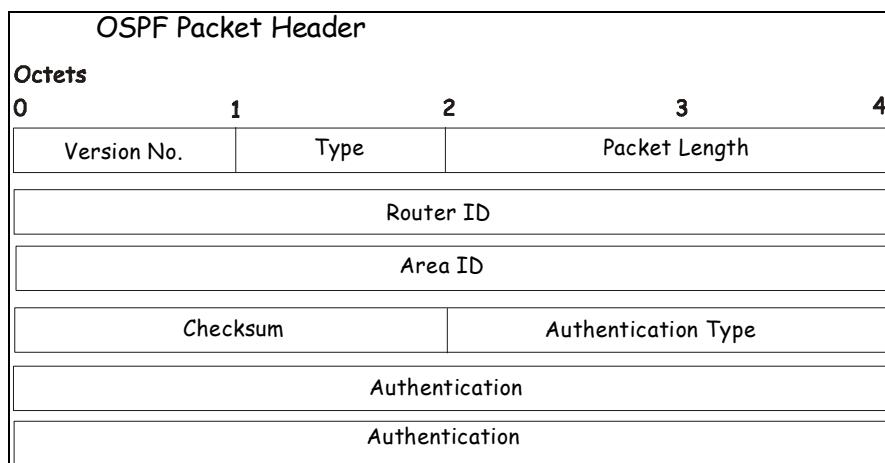
All OSPF packets (except for Hello packets) forward link-state advertisements. Link-State Update packets, for example, flood advertisements throughout the OSPF routing domain.

- OSPF packet header
- Hello packet
- Database Description packet
- Link-State Request packet
- The Link-State Update packet
- Link-State Acknowledgment packet

## OSPF Packet Header

Every OSPF packet is preceded by a common 24-byte header. This header contains the information necessary for a receiving router to determine if the packet should be accepted for further processing.

The format of the OSPF packet header is shown below:



**Figure 5- 8. OSPF Packet Header**

Field	Description
<b>Version No.</b>	The OSPF version number
<b>Type</b>	The OSPF packet type. The OSPF packet types are as follows: Type    Description

	Hello
	Database Description
	Link-State Request
	Link-State Update
	Link-State Acknowledgment
<b>Packet Length</b>	The length of the packet in bytes. This length includes the 24-byte header.
<b>Router ID</b>	The Router ID of the packet's source.
<b>Area ID</b>	A 32-bit number identifying the area that this packet belongs to. All OSPF packets are associated with a single area. Packets traversing a virtual link are assigned the backbone Area ID of 0.0.0.0
<b>Checksum</b>	A standard IP checksum that includes all of the packet's contents except for the 64-bit authentication field.
<b>Authentication Type</b>	The type of authentication to be used for the packet.
<b>Authentication</b>	A 64-bit field used by the authentication scheme.

## Hello Packet

Hello packets are OSPF packet type 1. They are sent periodically on all interfaces, including virtual links, in order to establish and maintain neighbor relationships. In addition, Hello Packets are multicast on those physical networks having a multicast or broadcast capability, enabling dynamic discovery of neighboring routers.

All routers connected to a common network must agree on certain parameters such as the Network Mask, the Hello Interval, and the Router Dead Interval. These parameters are included in hello packets, so that differences can inhibit the forming of neighbor relationships. A detailed explanation of the receive processing for Hello packets, so that differences can inhibit the forming of neighbor relationships.

The format of the Hello packet is shown below:

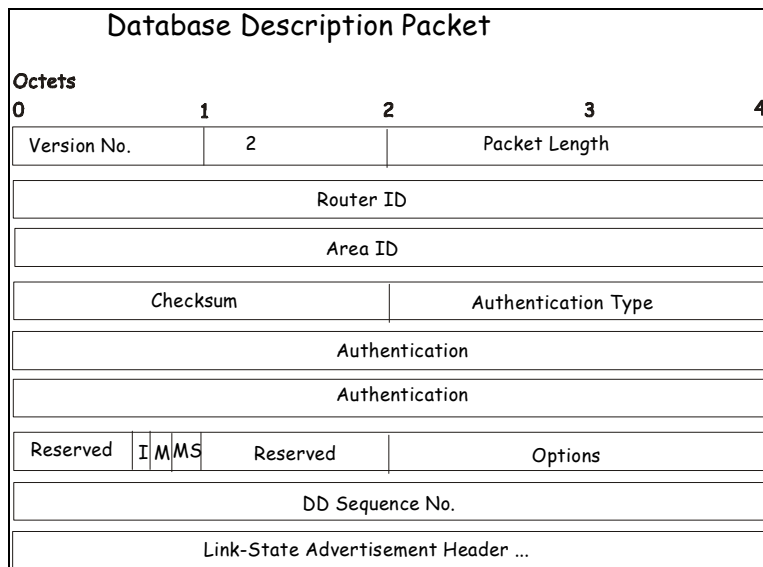
Hello Packet				
Octets				
0	1	2	3	4
Version No.		1	Packet Length	
Router ID				
Area ID				
Checksum		Authentication Type		
Authentication				
Authentication				
Network Mask				
Hello Interval		Options	Router Priority	
Router Dead Interval				
Designated Router				
Backup Designated Router				
Neighbor				

**Figure 5- 9. Hello Packet**

Field	Description
<b>Network Mask</b>	The network mask associated with this interface.
<b>Options</b>	The optional capabilities supported by the router.
<b>Hello Interval</b>	The number of seconds between this router's Hello packets.
<b>Router Priority</b>	This router's Router Priority. The Router Priority is used in the election of the DR and BDR. If this field is set to 0, the router is ineligible become the DR or the BDR.
<b>Router Dead Interval</b>	The number of seconds that must pass before declaring a silent router as down.
<b>Designated Router</b>	The identity of the DR for this network, in the view of the advertising router. The DR is identified here by its IP interface address on the network.
<b>Backup Designated Router</b>	The identity of the Backup Designated Router (BDR) for this network. The BDR is identified here by its IP interface address on the network. This field is set to 0.0.0.0 if there is no BDR.
<b>Field</b>	<b>Description</b>
<b>Neighbor</b>	The Router Ids of each router from whom valid Hello packets have been seen within the Router Dead Interval on the network.

## Database Description Packet

Database Description packets are OSPF packet type 2. These packets are exchanged when an adjacency is being initialized. They describe the contents of the topological database. Multiple packets may be used to describe the database. For this purpose a poll-response procedure is used. One of the routers is designated to be master, the other a slave. The master sends Database Description packets (polls) that are acknowledged by Database Description packets sent by the slave (responses). The responses are linked to the polls via the packets' DD sequence numbers.

**Figure 5- 10. Database Description Packet**

Field	Description
<b>Options</b>	The optional capabilities supported by the router.
<b>I – bit</b>	The Initial bit. When set to 1, this packet is the first in the sequence of Database Description packets.
<b>M – bit</b>	The More bit. When set to 1, this indicates that more Database Description packets will follow.
<b>MS – bit</b>	The Master Slave bit. When set to 1, this indicates that the router is the master during the Database Exchange process. A zero indicates the opposite.
<b>DD Sequence Number</b>	User to sequence the collection of Database Description Packets. The initial value (indicated by the Initial bit being set) should be unique. The DD sequence number then increments until the complete database description has been sent.

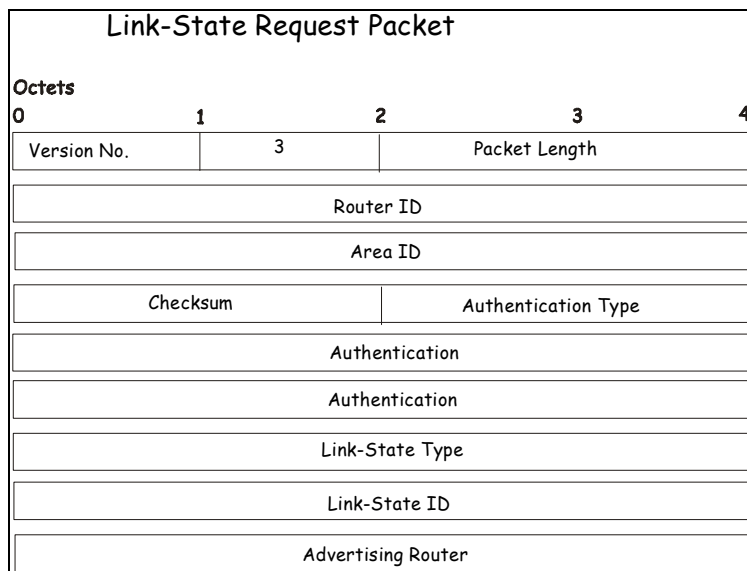
The rest of the packet consists of a list of the topological database's pieces. Each link state advertisement in the database is described by its link state advertisement header.

### Link-State Request Packet

Link-State Request packets are OSPF packet type 3. After exchanging Database Description packets with a neighboring router, a router may find that parts of its topological database are out of date. The Link-State Request packet is used to request the pieces of the neighbor's database that are more up to date. Multiple Link-State Request packets may need to be used. The sending of Link-State Request packets is the last step in bringing up an adjacency.

A router that sends a Link-State Request packet has in mind the precise instance of the database pieces it is requesting, defined by LS sequence number, LS checksum, and LS age, although these fields are not specified in the Link-State Request packet itself. The router may receive even more recent instances in response.

The format of the Link-State Request packet is shown below:



**Figure 5- 11. Link-State Request Packet**

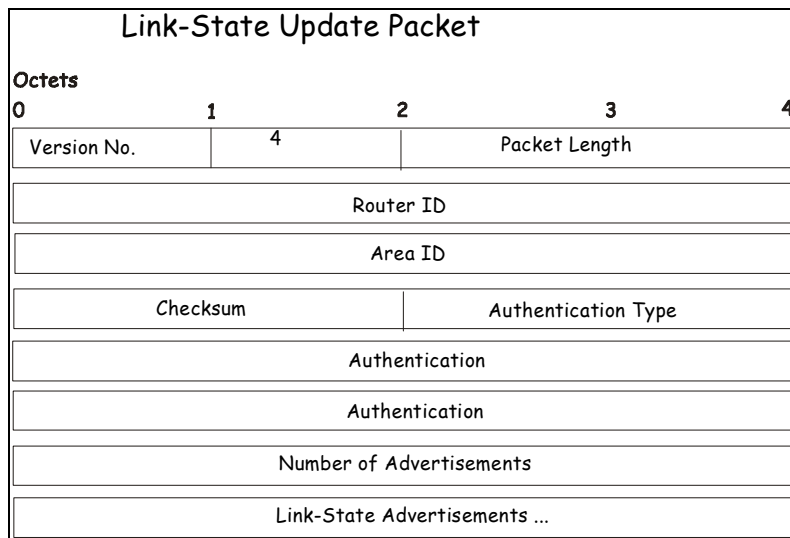
Each advertisement requested is specified by its Link-State Type, Link-State ID, and Advertising Router. This uniquely identifies the advertisement, but not its instance. Link-State Request packets are understood to be requests for the most recent instance.

## Link-State Update Packet

Link-State Update packets are OSPF packet type 4. These packets implement the flooding of link-state advertisements. Each Link-State Update packet carries a collection of link-state advertisements one hop further from its origin. Several link-state advertisements may be included in a single packet.

Link-State Update packets are multicast on those physical networks that support multicast/broadcast. In order to make the flooding procedure reliable, flooded advertisements are acknowledged in Link-State Acknowledgment packets. If retransmission of certain advertisements is necessary, the retransmitted advertisements are always carried by unicast Link-State Update packets.

The format of the Link-State Update packet is shown below:



**Figure 5- 12. Link-State Update Packet**

The body of the Link-State Update packet consists of a list of link-state advertisements. Each advertisement begins with a common 20-byte header, the link-state advertisement header. Otherwise, the format of each of the five types of link-state advertisements is different.

## Link-State Acknowledgment Packet

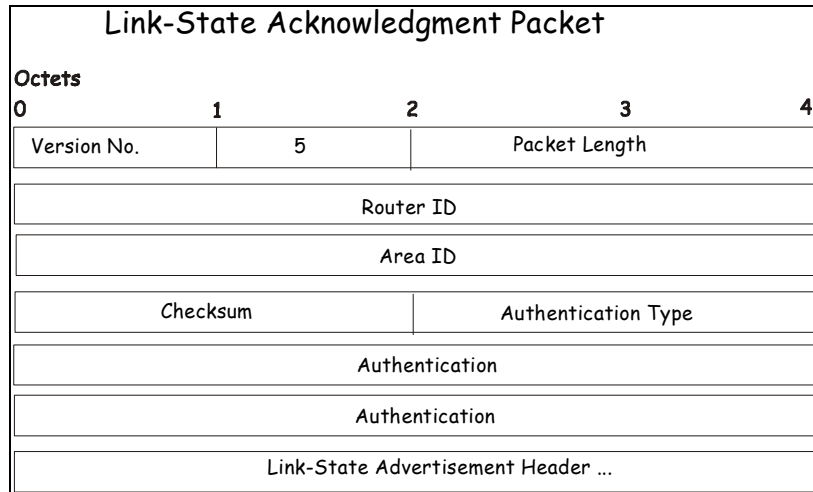
Link-State Acknowledgment packets are OSPF packet type 5. To make the flooding of link-state advertisements reliable, flooded advertisements are explicitly acknowledged. This acknowledgment is accomplished through the sending and receiving of Link-State Acknowledgment packets. Multiple link-state advertisements can be acknowledged in a single Link-State Acknowledgment packet.

Depending on the state of the sending interface and the source of the advertisements being acknowledged, a Link-State Acknowledgment packet is sent either to the multicast address AllSPFRouters, to the multicast address AllDRouters, or as a unicast packet.

The format of this packet is similar to that of the Data Description packet. The body of both packets is simply a list of link-state advertisement headers.

The format of the Link-State Acknowledgment packet is shown below:





**Figure 5- 13. Link-State Acknowledgment Packet**

Each acknowledged link-state advertisement is described by its link-state advertisement header. It contains all the information required to uniquely identify both the advertisement and the advertisement's current instance.

## Link-State Advertisement Formats

There are five distinct types of link-state advertisements. Each link-state advertisement begins with a standard 20-byte link-state advertisement header. Succeeding sections then diagram the separate link-state advertisement types.

Each link-state advertisement describes a piece of the OSPF routing domain. Every router originates a router links advertisement. In addition, whenever the router is elected as the Designated Router, it originates a network links advertisement. Other types of link-state advertisements may also be originated. The flooding algorithm is reliable, ensuring that all routers have the same collection of link-state advertisements. The collection of advertisements is called the link-state (or topological) database.

From the link-state database, each router constructs a shortest path tree with itself as root. This yields a routing table.

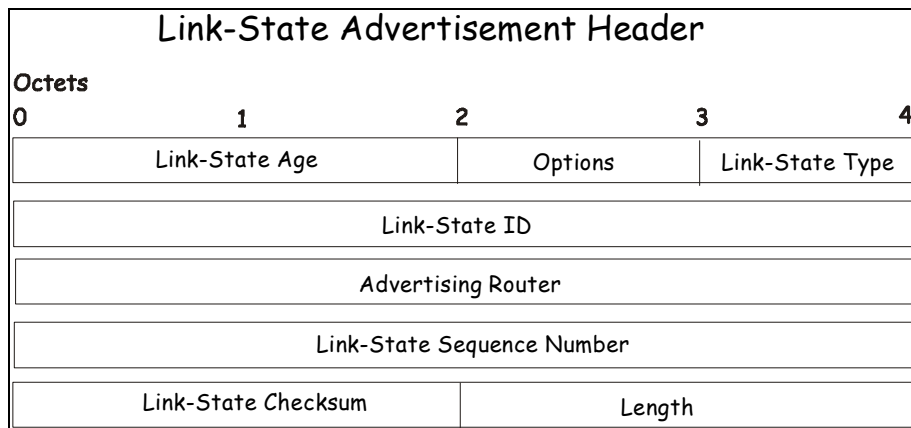
There are four types of link state advertisements, each using a common link state header. These are:

- Router Links Advertisements
- Network Links Advertisements
- Summary Link Advertisements
- Autonomous System Link Advertisements

## Link State Advertisement Header

All link state advertisements begin with a common 20-byte header. This header contains enough information to uniquely identify the advertisements (Link State Type, Link State ID, and Advertising Router). Multiple instances of the link state advertisement may exist in the routing domain at the same time. It is then necessary to determine which instance is more recent. This is accomplished by examining the link state age, link state sequence number and link state checksum fields that are also contained in the link state advertisement header.

The format of the Link State Advertisement Header is shown below:

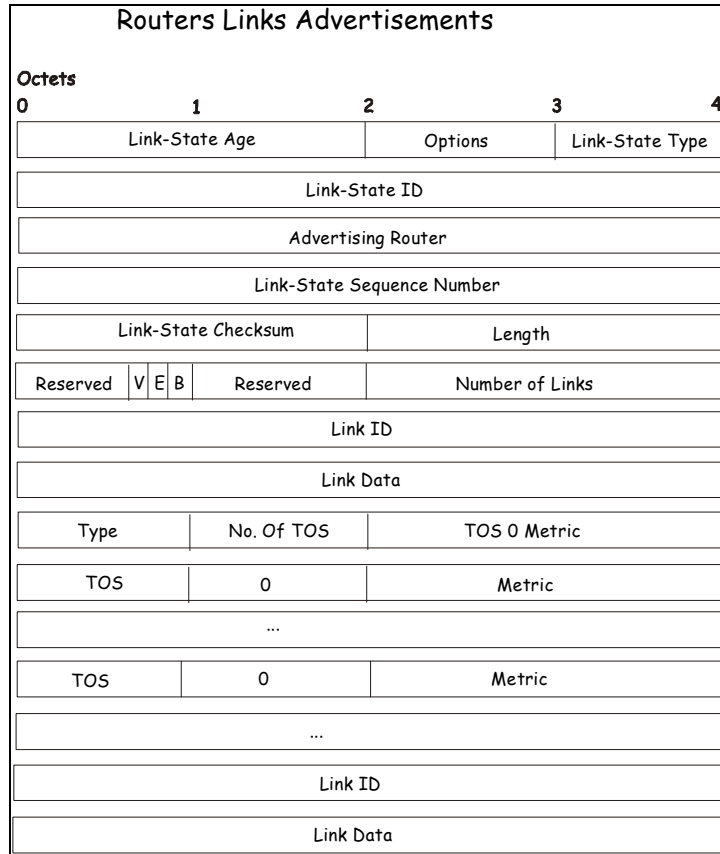
**Figure 5- 14. Link-State Advertisement Header**

Field	Description												
<b>Link State Age</b>	The time in seconds since the link state advertisement was originated.												
<b>Options</b>	The optional capabilities supported by the described portion of the routing domain.												
<b>Link State Type</b>	<p>The type of the link state advertisement. Each link state type has a separate advertisement format. The link state types are as follows:</p> <table> <tr> <th>Type</th><th>Description</th></tr> <tr> <td>1</td><td>Router Links</td></tr> <tr> <td></td><td>Network Links</td></tr> <tr> <td></td><td>Summary Link (IP Network)</td></tr> <tr> <td></td><td>Summary Link (ASBR)</td></tr> <tr> <td></td><td>AS External Link</td></tr> </table>	Type	Description	1	Router Links		Network Links		Summary Link (IP Network)		Summary Link (ASBR)		AS External Link
Type	Description												
1	Router Links												
	Network Links												
	Summary Link (IP Network)												
	Summary Link (ASBR)												
	AS External Link												
<b>Link State ID</b>	This field identifies the portion of the internet environment that is being described by the advertisement. The contents of this field depend on the advertisement's Link State Type.												
<b>Advertising Router</b>	The Router ID of the router that originated the Link State Advertisement. For example, in network links advertisements this field is set to the Router ID of the network's Designated Router.												
<b>Link State Sequence Number</b>	Detects old or duplicate link state advertisements. Successive instances of a link state advertisement are given successive Link State Sequence numbers.												
<b>Link State Checksum</b>	The Fletcher checksum of the complete contents of the link state advertisement, including the link state advertisement header by excepting the Link State Age field.												
<b>Length</b>	The length in bytes of the link state advertisement. This includes the 20-byte link state advertisement header.												

## Router Links Advertisements

Router links advertisements are type 1 link state advertisements. Each router in an area originates a routers links advertisement. The advertisement describes the state and cost of the router's links to the area. All of the router's links to the area must be described in a single router links advertisement.

The format of the Router Links Advertisement is shown below:



**Figure 5- 15. Routers Links Advertisement**

In router links advertisements, the Link State ID field is set to the router's OSPF Router ID. The T – bit is set in the advertisement's Option field if and only if the router is able to calculate a separate set of routes for each IP Type of Service (TOS). Router links advertisements are flooded throughout a single area only.

Field	Description
<b>V – bit</b>	When set, the router is an endpoint of an active virtual link that is using the described area as a Transit area (V is for Virtual link endpoint).
<b>E – bit</b>	When set, the router is an Autonomous System (AS) boundary router (E is for External).
<b>B – bit</b>	When set, the router is an area border router (B is for Border).
<b>Number of Links</b>	The number of router links described by this advertisement. This must be the total collection of router links to the area.

The following fields are used to describe each router link. Each router link is typed. The Type field indicates the kind of link being described. It may be a link to a transit network, to another router or to a stub network. The values of all the other fields describing a router link depend on the link's Type. For example, each link has an associated 32-bit data field. For links to stub networks this field specifies the network's IP address mask. For other link types the Link Data specifies the router's associated IP interface address.

Field	Description
<b>Type</b>	A quick classification of the router link. One of the following:
	Type    Description
	Point-to-point connection to another router.
	Connection to a transit network.
	Connection to a stub network.
<b>Link ID</b>	Virtual link.
	Identifies the object that this router link connects to. Value depends on the link's Type. When connecting to an object that also originates a link state advertisement (i.e. another router or a transit network) the Link ID is equal to the neighboring advertisement's Link State ID. This provides the key for looking up an advertisement in the link state database.
	Type    Link ID
	Neighboring router's Router ID.
	IP address of Designated Router.
<b>Link Data</b>	IP network/subnet number.
	Neighboring router's Router ID
	Contents again depend on the link's Type field. For connections to stub networks, it specifies the network's IP address mask. For unnumbered point-to-point connection, it specifies the interface's MIB-II ifIndex value. For other link types it specifies the router's associated IP interface address. This latter piece of information is needed during the routing table build process, when calculating the IP address of the next hop.
<b>No. of TOS</b>	The number of different Type of Service (TOS) metrics given for this link, not counting the required metric for TOS 0. If no additional TOS metrics are given, this field should be set to 0.
<b>TOS 0 Metric</b>	The cost of using this router link for TOS 0.
<b>Field</b>	<b>Description</b>
<b>TOS</b>	IP Type of Service that this metric refers to.
<b>Metric</b>	The cost of using this outbound router link, for traffic of the specified TOS.

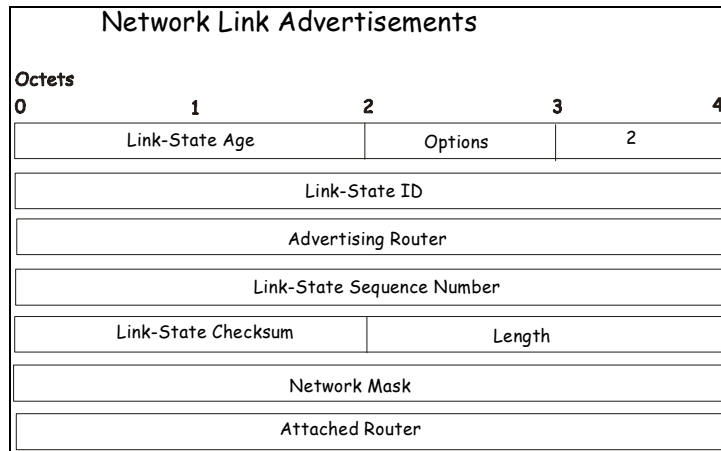
For each link, separate metrics may be specified for each Type of Service (TOS). The metric for TOS 0 must always be included, and was discussed above. Metrics for non-zero TOS are described below. Note that the cost for non-zero TOS values that are not specified defaults to the TOS 0 cost. Metrics must be listed in order of increasing TOS encoding. For example, the metric for TOS 16 must always follow the metric for TOS 8 when both are specified.

## Network Links Advertisements

Network links advertisements are Type 2 link state advertisements. A network links advertisement is originated for each transit network in the area. A transit network is a multi-access network that has more than one attached router. The network links advertisement is originated by the network's Designated router. The advertisement describes all routers attached to the network, including the Designated Router itself. The advertisement's Link State ID field lists the IP interface address of the Designated Router.

The distance from the network to all attached routers is zero, for all TOS. This is why the TOS and metric fields need not be specified in the network links advertisement.

The format of the Network Links Advertisement is shown below:



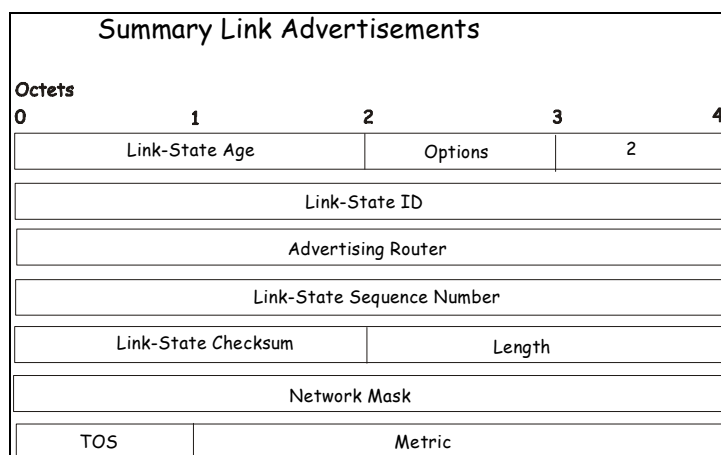
**Figure 5- 16. Network Link Advertisements**

Field	Description
<b>Network Mask</b>	The IP address mask for the network.
<b>Attached Router</b>	The Router Ids of each of the routers attached to the network. Only those routers that are fully adjacent to the Designated Router (DR) are listed. The DR includes itself in this list.

## Summary Link Advertisements

Summary link advertisements are Type 3 and 4 link state advertisements. These advertisements are originated by Area Border routers. A separate summary link advertisement is made for each destination known to the router, that belongs to the Autonomous System (AS), yet is outside the area.

Type 3 link state advertisements are used when the destination is an IP network. In this case the advertisement's Link State ID field is an IP network number. When the destination is an AS boundary router, a Type 4 advertisement is used, and the Link State ID field is the AS boundary router's OSPF Router ID. Other than the difference in the Link State ID field, the format of Type 3 and 4 link state advertisements is identical.



**Figure 5- 17. Summary Link Advertisements**

For stub area, Type 3 summary link advertisements can also be used to describe a default route on a per-area basis. Default summary routes are used in stub area instead of flooding a complete set of external routes. When describing a default summary route, the advertisement's Link State ID is always set to the Default Destination – 0.0.0.0, and the Network Mask is set to 0.0.0.0.

Separate costs may be advertised for each IP Type of Service. Note that the cost for TOS 0 must be included, and is always listed first. If the T-bit is reset in the advertisement's Option field, only a route for TOS 0 is described by the advertisement. Otherwise, routes for the other TOS values are also described. If a cost for a certain TOS is not included, its cost defaults to that specified for TOS 0.

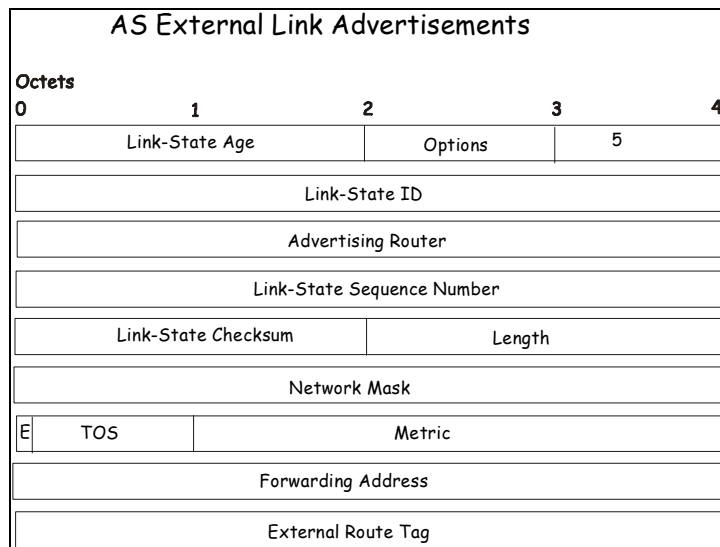
Field	Description
<b>Network Mask</b>	For Type 3 link state advertisements, this indicates the destination network's IP address mask. For example, when advertising the location of a class A network the value 0xff000000
<b>TOS</b>	The Type of Service that the following cost is relevant to.
<b>Metric</b>	The cost of this route. Expressed in the same units as the interface costs in the router links advertisements.

## Autonomous Systems External Link Advertisements

Autonomous Systems (AS) link advertisements are Type 5 link state advertisements. These advertisements are originated by AS boundary routers. A separate advertisement is made for each destination known to the router, that is external to the AS.

AS external link advertisements usually describe a particular external destination. For these advertisements the Link State ID field specifies an IP network number. AS external link advertisements are also used to describe a default route. Default routes are used when no specific route exists to the destination. When describing a default route, the Link Stat ID is always set the Default Destination address (0.0.0.0) and the Network Mask is set to 0.0.0.0.

The format of the AS External Link Advertisement is shown below:



**Figure 5- 18. AS External Link Advertisements**

Field	Description
<b>Network Mask</b>	The IP address mask for the advertised destination.
<b>E – bit</b>	The type of external metric. If the E – bit is set, the metric specified is a Type 2 external metric. This means the metric is considered larger than any link state path. If the E – bit is zero, the specified metric is a Type 1 external metric. This means that is comparable directly to the link state metric.
<b>Forwarding Address</b>	Data traffic for the advertised destination will be forwarded to this address. If the Forwarding Address is set to 0.0.0.0, data traffic will

	be forwarded instead to the advertisement's originator.
<b>TOS</b>	The Type of Service that the following cost is relevant to.
<b>Metric</b>	The cost of this route. The interpretation of this metric depends on the external type indication (the E – bit above).
<b>External Route Tag</b>	A 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

## MD5 Key Settings

MD5 authentication is used to identify trusted routers sending OSPF packets. By default no authentication is used for OSPF so it is not necessary to configure any MD5 keys to use OSPF. MD5 authentication can be set up at any time, before or after you have configured OSPF settings.

The **MD5 Key Setting** window allows the entry of a 16-character Message Digest – version 5 (MD5) key that can be used to authenticate every packet exchanged between OSPF routers. It is used as a security mechanism to limit the exchange of network topology information to the OSPF routing domain.

MD5 Keys created here are entered in when setting up OSPF interfaces. Please read the description in the section below about OSPF Interface Settings.

To configure an MD5 Key, click the **MD5 Key Settings** link in the **Layer 3 IP Networking** folder to open the following window:

MD5 Key Setting	
Key ID	Key
1	

Add/Modify

MD5 Key Table		
Key ID	Key	Delete

**Figure 5- 19. MD5 Key Setting window**

To add an MD5 key to the table, type a unique Key ID (Key Identifier) and provide a Key in the fields provided. Click the **Add/Modify** button to add the key to the MD5 Key Table.

To remove a key, simply click the **X** in the **Delete** column for the Key you wish to remove.

To change an existing key in the list, type the Key ID for that key in the Key ID field, change the Key as desired and click the **Add/Modify** button. The modified key will appear in the new list.

**MD5 Key Setting**

Key ID	Key
1	

Add/Modify

**MD5 Key Table**

Key ID	Key	Delete
1	hedo	X
2	peja	X
3	vlade	X

Figure 5- 20. Newly Created MD5 Key List window

The MD5 key settings must satisfy the requirements listed here:

Parameter	Description
<b>Key ID</b>	A number from 1 to 255 used to identify the MD5 Key.
<b>Key</b>	A alphanumeric string of between 1 and 16 case-sensitive characters used to generate the Message Digest which is in turn, used to authenticate OSPF packets within the OSPF routing domain.

## Route Redistribution Settings

Route redistribution allows routers on the network – that are running different routing protocols – to exchange routing information. This is accomplished by comparing the routes stored in the various routers' routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual routers current routing protocol. The DGS-3312SR can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local DGS-3312SRs Switch is also redistributed.

**Route Redistribution Settings**

Dest Protocol	Src Protocol	Type	Metric
RIP	RIP	All	

Add/Modify

**Route Redistribution Table**

Src Protocol	Dest Protocol	Type	Metric	Delete
OSPF	RIP	All	1	X
STATIC	RIP	All	1	X

Figure 5- 21. Route Redistribution Settings window

To create a new route redistribution criteria, select the Dest Protocol (destination protocol) and Src Protocol (source protocol) from the drop-down menus, choose the metric Type and enter a Metric value. Click on the **Add/Modify** button



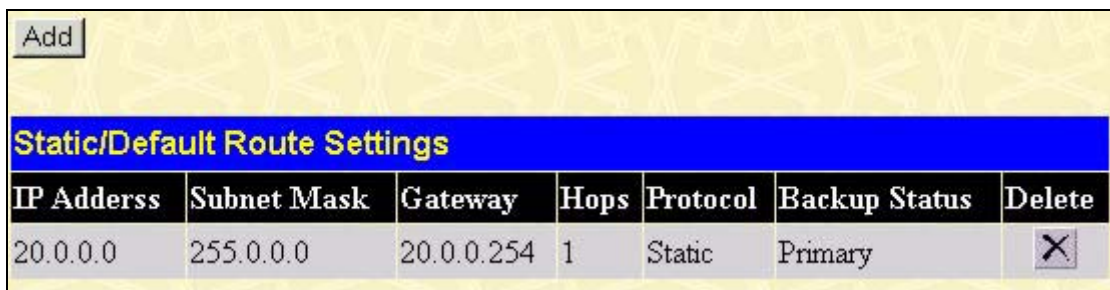
and the new redistribution setting appears listed in the table. To eliminate an existing redistribution configuration, click the **X** in the Delete column for the configuration being removed.

Refer to the table below for descriptions of the **Router Redistribution Settings** window settings:

Parameter	Description
<b>Dest Protocol</b>	Allows the selection of the protocol of the destination device. Available choices are <i>RIP</i> and <i>OSPF</i> .
<b>Src Protocol</b>	Allows the selection of the protocol of the source device. Available choices are <i>RIP</i> , <i>OSPF</i> , <i>Static</i> , or <i>Local</i> .
<b>Type</b>	Allows the selection of one of two methods for calculating the metric value. <i>Type-1</i> calculates the metric (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. <i>Type-2</i> uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF.
<b>Metric</b>	Allows the entry of an interface cost.

## Static/Default Route Settings

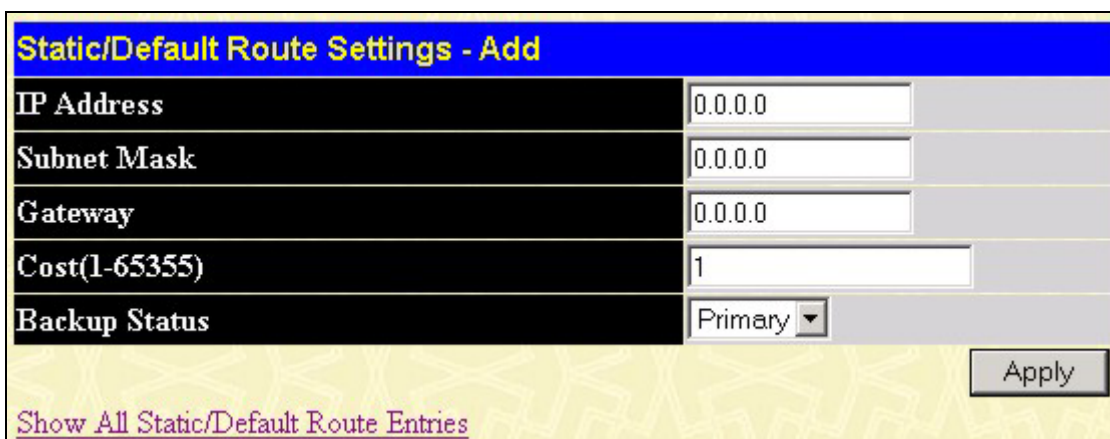
Static routes that have been previously configured appear in the Static/Default Route Settings table. To add a new route, click on the **Add** button, a new window appears. To remove an existing route, click the **X** button in the Delete column for the route you want to eliminate.



Static/Default Route Settings						
IP Address	Subnet Mask	Gateway	Hops	Protocol	Backup Status	Delete
20.0.0.0	255.0.0.0	20.0.0.254	1	Static	Primary	X

Figure 5- 22. Static/Default Route Settings window

Use the **Static/Default Route Settings – Add** window to configure IP settings and Metric cost for the new route.



Static/Default Route Settings - Add	
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
Cost(1-65535)	1
Backup Status	Primary

[Show All Static/Default Route Entries](#) Apply

Figure 5- 23. Static/Default Route Settings – Add window

Configure the IP settings for the new static route and click the **Apply** button to create the static route. The new route will appear in the previous window. To view the new route and any other static routes configured for the Switch click the [Show All Static/Default Route Entries](#) link.

The following fields can be set:

Parameter	Description
<b>IP Address &lt;0.0.0.0&gt;</b>	Allows the entry of an IP address that will be a static entry into the Switch's Routing Table.
<b>Subnet Mask &lt;0.0.0.0&gt;</b>	Allows the entry of a subnet mask corresponding to the IP address above.
<b>Gateway IP &lt;0.0.0.0&gt;</b>	Allows the entry of an IP address of a gateway for the IP address above.
<b>Cost (1-65355) &lt;1&gt;</b>	Allows the entry of a routing protocol metric representing the number of routers between the Switch and the IP address above.
<b>Backup Status</b>	Specify the route as <i>Primary</i> or <i>Backup</i> . If a single IP route is used, it is unnecessary to change this. Designate a backup route if an alternate route is desired. A backup IP route is sometimes called a "floating static route."

## Static ARP Settings

Use the **Static ARP Settings** window to create permanent entries in the ARP table for different IP interfaces. Static ARP entries that have been configured appear in the Static ARP Settings table in this window. To add a new static ARP entry, click on the **Add** button, a new window appears (see below). To remove an existing entry, click the **X** button in the Delete column for the entry you want to eliminate. To delete all static ARP entries, click the **Clear All** button.

Static ARP Settings					
Interface Name	IP Address	MAC Address	Type	Modify	Delete

Figure 5- 24. Static ARP Settings window

Clicking the **Add** button allows you to add a new entry using the window below.

Static ARP Table - Add a New Entry	
IP Address	0.0.0.0
MAC Address	00-00-00-00-00-00
<input type="button" value="Apply"/>	
<a href="#">Show All Static ARP Entries</a>	

Figure 5- 25. Static ARP Table – Add a New Entry window

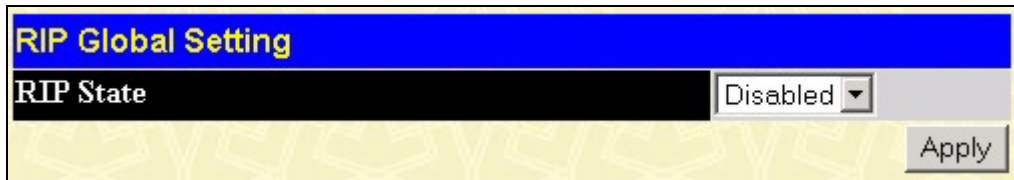
Enter the IP address and the MAC address of the device you want to map with ARP and click the **Apply** button. The new entry will appear in the **Static ARP Settings** window. Click the [Show All Static ARP Entries](#) link to see the **Static ARP Settings** window.

## RIP

The Switch supports the Routing Information Protocol (RIP).

### RIP Global Setting

To setup Routing Information Protocol (RIP) for the IP interfaces configured in the Switch, open the **RIP** folder and click on the **RIP Global Setting** link. Use the **RIP Global Setting** window to first enable RIP and then configure RIP settings for the individual IP interfaces. To enable RIP, select *Enabled* from the drop-down RIP State menu and click the **Apply** button. RIP can be disabled or enabled without changing any of the RIP IP interfaces settings using this window.



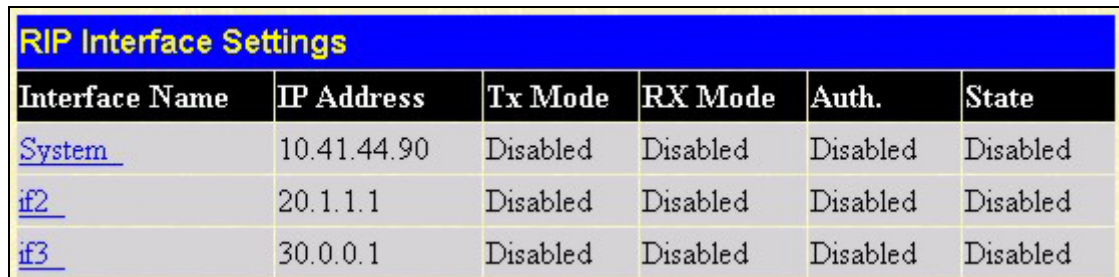
**RIP Global Setting**

RIP State Disabled

Figure 5- 26. RIP Global Setting window

## RIP Interface Settings

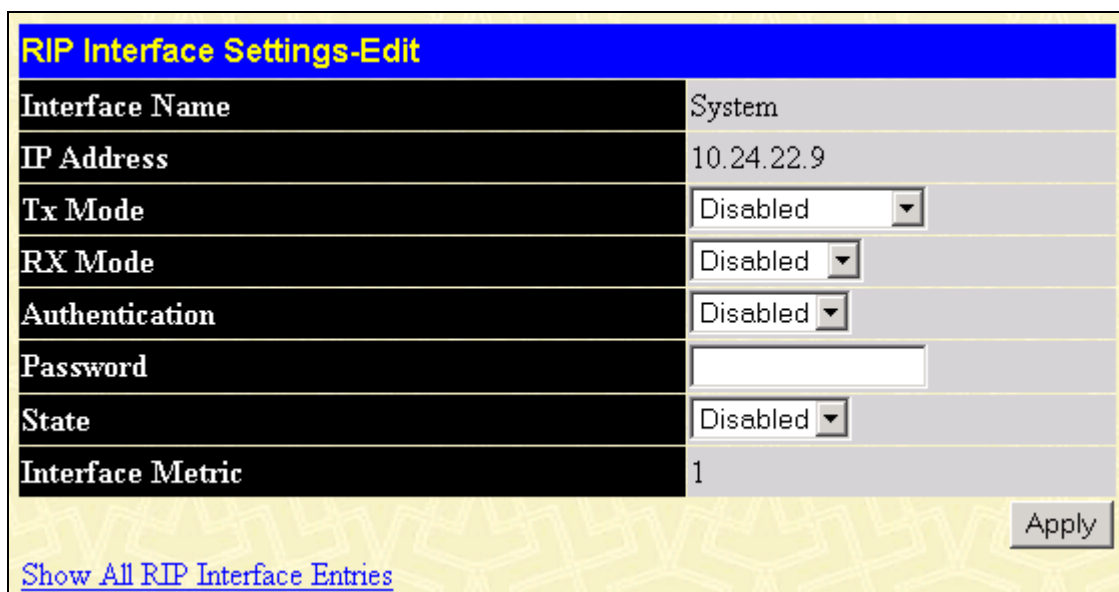
RIP settings are configured for each IP interface on the Switch. Click the **RIP Interface Settings** link in the **RIP** sub-folder. The window appears in table form listing settings for IP interfaces currently on the Switch. To configure RIP settings for an individual interface, click on the hyperlinked name of the interface.



RIP Interface Settings					
Interface Name	IP Address	Tx Mode	RX Mode	Auth.	State
<a href="#">System</a>	10.41.44.90	Disabled	Disabled	Disabled	Disabled
<a href="#">if2</a>	20.1.1.1	Disabled	Disabled	Disabled	Disabled
<a href="#">if3</a>	30.0.0.1	Disabled	Disabled	Disabled	Disabled

Figure 5- 27. RIP Interface Settings window

Click the name of the interface you want to setup for RIP to the following window:



**RIP Interface Settings-Edit**

Interface Name	System
IP Address	10.24.22.9
Tx Mode	<span>Disabled</span>
RX Mode	<span>Disabled</span>
Authentication	<span>Disabled</span>
Password	<input type="text"/>
State	<span>Disabled</span>
Interface Metric	1

[Show All RIP Interface Entries](#)

Figure 5- 28. RIP Interface Settings – Edit window

Refer to the table below for a description of the available parameters for RIP interface settings. To return to the RIP Interface Settings table, click the [Show All RIP Interface Settings](#) link.

The following RIP settings can be applied to each IP interface:

Parameter	Description
<b>Interface Name</b>	The name of the IP interface on which RIP is to be setup. This interface must be previously configured on the Switch.
<b>TX Mode &lt;Disabled&gt;</b>	Toggle among <i>Disabled</i> , <i>V1 Only</i> , <i>V1 Compatible</i> , and <i>V2 Only</i> . This entry specifies which version of the RIP protocol will be used to transmit RIP packets. <i>Disabled</i> prevents the transmission of RIP packets.

<b>RX Mode &lt;Disabled&gt;</b>	Toggle among <i>Disabled</i> , <i>V1 Only</i> , <i>V2 Only</i> , and <i>V1 and V2</i> . This entry specifies which version of the RIP protocol will be used to interpret received RIP packets. <i>Disabled</i> prevents the reception of RIP packets.
<b>Authentication</b>	Toggle between <i>Disabled</i> and <i>Enabled</i> to specify that routers on the network should use the Password above to authenticate router table exchanges.
<b>Password</b>	A password to be used to authenticate communication between routers on the network.
<b>State</b>	Toggle between <i>Disabled</i> and <i>Enabled</i> to disable or enable this RIP interface on the Switch.

## OSPF

All the links for OSPF configuration windows are contained within the **OSPF** sub-folder of the **Layer 3 IP Networking** folder (located under **Configuration**).

### OSPF General Setting

The **OSPF General Setting** window allows OSPF to be enabled or disabled on the Switch – without changing the Switch's OSPF configuration.

From the **Layer 3 IP Networking** folder, open the **OSPF** sub-folder and click on the **OSPF General Setting** link. To enable OSPF, first supply an OSPF Route ID (see below), select *Enabled* from the State drop-down menu and click the **Apply** button.

Figure 5- 29. OSPF General Setting window

The following parameters are used for general OSPF configuration:

Parameter	Description
<b>OSPF Route ID</b>	A 32-bit number (in the same format as an IP address – xxx.xxx.xxx.xxx) that uniquely identifies the Switch in the OSPF domain. It is common to assign the highest IP address assigned to the Switch (router). In this case, it would be 10.255.255.255, but any unique 32-bit number will do. If 0.0.0.0 is entered, the highest IP address assigned to the Switch will become the OSPF Route ID.
<b>Current Route ID</b>	Displays the OSPF Route ID currently in use by the Switch. This Route ID is displayed as a convenience to the user when changing the Switch's OSPF Route ID.
<b>State</b>	Allows OSPF to be <i>Enabled</i> or <i>Disabled</i> globally on the Switch without changing the OSPF configuration.

### OSPF Area ID Settings

This window allows the configuration of OSPF Area IDs and to designate these areas as either *Normal* or *Stub*. Normal OSPF areas allow Link-State Database (LSDB) advertisements of routes to networks that are external to the area, while

stub areas do not allow the LSDB advertisement of external routes. Stub areas use a default summary external route (0.0.0.0 or Area 0) to reach external destinations.

To set up an OSPF Area configuration click the OSPF Area Settings link to open the following window:

OSPF Area Settings			
Area ID	Type	Stub Import Summary LSA	Stub Default Cost
0.0.0.0	Normal	Disabled	1

Add/Modify

OSPF Area ID Table				
Area ID	Type	Stub Import Summary LSA	Stub Default Cost	Delete
0.0.0.0	Normal	None	None	X

**Figure 5- 30. OSPF Area Settings window**

To add an OSPF Area to the table, type a unique Area ID (see below) select the Type from the drop-down menu. For a Stub type, choose *Enabled* or *Disabled* from the Stub Import Summary LSA drop-down menu and determine the Stub Default Cost. Click the **Add/Modify** button to add the Area ID set to the table.

To remove an Area ID configuration set, simply click the **X** in the **Delete** column for the configuration.

To change an existing set in the list, type the Area ID of the set you want to change, make the changes and click the **Add/Modify** button. The modified OSPF Area ID will appear in the table.

OSPF Area Settings			
Area ID	Type	Stub Import Summary LSA	Stub Default Cost
0.0.0.0	Stub	Disabled	1

Add/Modify

OSPF Area ID Table				
Area ID	Type	Stub Import Summary LSA	Stub Default Cost	Delete
0.0.0.0	Normal	None	None	X
10.0.0.128	Normal	None	None	X
10.0.0.254	Stub	Disabled	1	X

**Figure 5- 31. OSPF Area Settings window**

See the parameter descriptions below for information on the OSPF Area ID setting.

The Area ID settings are as follows:

Parameter	Description
<b>Area ID</b>	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
<b>Type</b>	This field can be toggled between <i>Normal</i> and <i>Stub</i> using the space bar. When it is toggled to <i>Stub</i> , additional fields appear – Stub Import Summary LSA, and Default Cost.
<b>Stub Import Summary LSA</b>	Displays whether or not the selected Area will allow Summary Link-State Advertisements (Summary LSAs) to be imported into the area from other areas.



**Default Cost** Displays the default cost for the route to the stub of between 0 and 65,535. The default is 0.

## OSPF Interface Settings

To set up OSPF interfaces, click the **OSPF Interface Settings** link to view OSPF settings for existing IP interfaces. If there are no IP interfaces configured (besides the default System interface), only the System interface settings will appear listed. To change settings for in IP interface, click on the hyperlinked name of the interface to see the configuration menu for that interface.

OSPF Interface Settings							
Name	IP Address	Area ID	Priority	Hello Time	Dead Time	Auth. Type	State
<a href="#">System</a>	10.24.22.9	0.0.0.0	1	10	40	None	Disabled

Figure 5- 32. OSPF Interface Settings window

OSPF Interface Settings - Edit	
Interface Name	System
IP Address	10.24.22.9(Link Up)
Network Medium Type	BROADCAST
Area ID	<input type="text" value="0.0.0.0"/>
Router Priority	<input type="text" value="1"/>
Hello Interval	<input type="text" value="10"/>
Dead Interval	<input type="text" value="40"/>
State	Disabled ▾
Auth. Type	None ▾
Auth. Key ID	<input type="text"/>
Metric	<input type="text" value="1"/>
DR State	DOWN
DR Address	0.0.0.0
Backup DR Address	0.0.0.0
transmit Delay	1
Retransmit Time	5

[Show All OSPF Interface Entries](#)

Figure 5- 33. OSPF Interface Settings - Edit window

Configure each IP interface individually using the **OSPF Interface Settings – Edit** window. Click the **Apply** button when you have entered the settings. The new configuration appears listed in the OSPF Interface Settings table. To return to the **OSPF Interface Settings** window, click the [Show All OSPF Interface Entries](#) link.

OSPF interface settings are described below.

Some OSPF interface settings require previously configured OSPF settings. Read the descriptions below for details.

Parameter	Description
<b>Interface Name</b>	Displays the of an IP interface previously configured on the Switch.
<b>Area ID</b>	Allows the entry of an OSPF Area ID configured above.
<b>Router Priority</b>	Allows the entry of a number between 0 and 255 representing the OSPF priority of the selected area. If a Router Priority of 0 is selected, the Switch cannot be elected as the Designated Router for the network.
<b>Hello Interval</b>	Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 5 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.
<b>Dead Interval</b>	Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 5 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.
<b>State</b>	Allows the OSPF interface to be disabled for the selected area without changing the configuration for that area.
<b>Auth Type</b>	This field can be toggled between <i>None</i> , <i>Simple</i> , and <i>MD5</i> using the space bar. This allows a choice of authorization schemes for OSPF packets that may be exchanged over the OSPF routing domain. <i>None</i> specifies no authorization. <i>Simple</i> uses a simple password to determine if the packets are from an authorized OSPF router. When <i>Simple</i> is selected, the Auth Key field allows the entry of an 8-character password that must be the same as a password configured on a neighbor OSPF router. <i>MD5</i> uses a cryptographic key entered in the MD5 Key Setting window. When <i>MD5</i> is selected, the Auth Key ID field allows the specification of the Key ID as defined in the MD5 configuration above. This must be the same MD5 Key as used by the neighboring router.
<b>Metric</b>	This field allows the entry of a number between 1 and 65,535 that is representative of the OSPF cost of reaching the selected OSPF interface. The default metric is 1.

## OSPF Virtual Interface Settings

Click the **OSPF Virtual Interface Settings** link to view the current OSPF virtual interface settings. There are not virtual interface settings configured by default, so the first time this table is viewed there will be not interfaces listed. To add a new OSPF virtual interface configuration set to the table, click the **Add** button. A new window appears (see below). To change an existing configuration, click on the hyperlinked Transit Area ID for the set you want to change. The window to modify an existing set is the same as the window used to add a new one. To eliminate an existing configuration, click the **X** in the Delete column for the configuration being removed.

Add								
OSPF Virtual Interface Settings								
Transit Area ID	Neighbor Router ID	Hello Interval	Dead Interval	Auth. Type	Transmit Delay	RetransInterval	Status	Delete
10.0.0.128	20.1.1.254	10	60	None	1	5	Down	X

Figure 5- 34. OSPF Virtual Interface Settings window

The status of the virtual interface appears (Up or Down) in the **Status** column.

OSPF Virtual Interface Settings - Add	
Transit Area ID	0.0.0.0
Neighbor Router ID	0.0.0.0
Hello Interval(1-65535)	10
Dead Interval(1-65535)	60
Auth Type	None
Password/Auth. Key ID	
Transmit Delay	1
RetransInterval	5

Apply

[Show All OSPF Virtual Link Entries](#)

**Figure 5- 35. OSPF Virtual Interface Settings – Add window**

Configure the following parameters if you are adding or changing an OSPF Virtual Interface:

Parameter	Description
<b>Transit Area ID</b>	Allows the entry of an OSPF Area ID – previously defined on the Switch – that allows a remote area to communicate with the backbone (area 0). A Transit Area cannot be a Stub Area or a Backbone Area.
<b>Neighbor Router ID</b>	The OSPF router ID for the remote router. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.
<b>Hello Interval(1-65535)</b>	Specify the interval between the transmission of OSPF Hello packets, in seconds. Enter a value between 1 and 65535 seconds. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should have identical settings for all routers on the same network.
<b>Dead Interval(1-65535)</b>	Specify the length of time between (receiving) Hello packets from a neighbor router before the selected area declares that router down. Again, all routers on the network should use the same setting.
<b>Auth Type</b>	If using authorization for OSPF routers, select the type being used. MD5 key authorization must be set up in the MD5 Key Settings window.
<b>Password/Auth. Key ID</b>	Enter a case-sensitive password for simple authorization or enter the MD5 key you set in the MD5 Key Settings window.



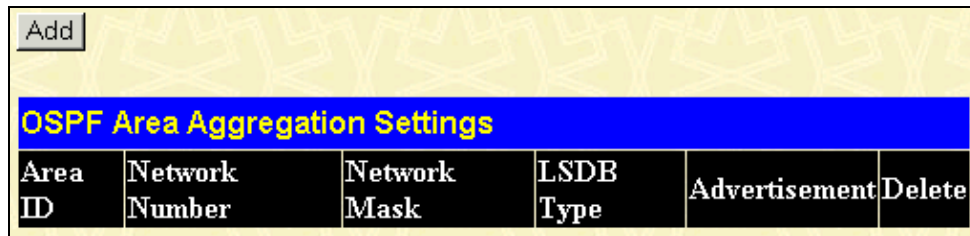
**NOTE:** For OSPF to function properly some settings should be identical on all participating OSPF devices. These settings include the Hello Interval and Dead Interval. For networks using authorization for OSPF devices, they Authorization Type and Password or Key used must likewise be identical.



## OSPF Area Aggregation Settings

Area Aggregation allows all of the routing information that may be contained within an area to be aggregated into a summary LSDB advertisement of just the network address and subnet mask. This allows for a reduction in the volume of LSDB advertisement traffic as well as a reduction in the memory overhead in the Switch used to maintain routing tables.

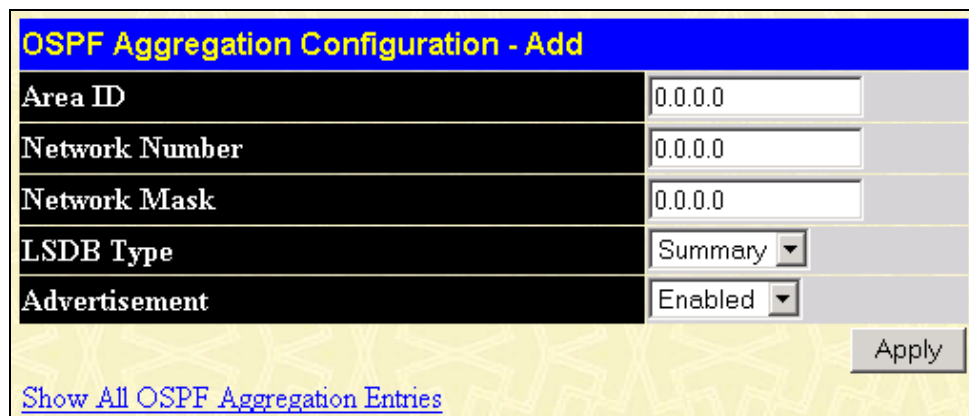
Click the **OSPF Area Aggregation Settings** link to view the current settings. There are no aggregation settings configured by default, so there will not be any listed the first accessing the window. To add a new OSPF Area Aggregation setting, click the **Add** button. A new window (pictured below) appears. To change an existing configuration, click on the hyperlinked Area ID for the set you want to change. The window to modify an existing configuration is the same as the window used to add a new one. To eliminate an existing configuration, click the **X** in the Delete column for the configuration being removed.



The screenshot shows a web interface window titled "OSPF Area Aggregation Settings". At the top left is an "Add" button. Below the title bar is a table with the following columns: "Area ID", "Network Number", "Network Mask", "LSDB Type", "Advertisement", and "Delete". The table is currently empty.

Figure 5- 36. OSPF Area Aggregation Settings window

Use the window below to change settings or add a new Area Aggregation setting.



The screenshot shows a web interface window titled "OSPF Aggregation Configuration - Add". It contains several input fields: "Area ID" (0.0.0.0), "Network Number" (0.0.0.0), "Network Mask" (0.0.0.0), "LSDB Type" (Summary), and "Advertisement" (Enabled). There is an "Apply" button at the bottom right and a link "Show All OSPF Aggregation Entries" at the bottom left.

Figure 5- 37. OSPF Aggregation Configuration – Add window

Specify the OSPF Aggregation settings and click the **Apply** button to add or change the settings. The new settings will appear listed in the **OSPF Area Aggregation Settings** window. To view the table, click the [Show All OSPF Aggregation Entries](#) link to return to the previous window.

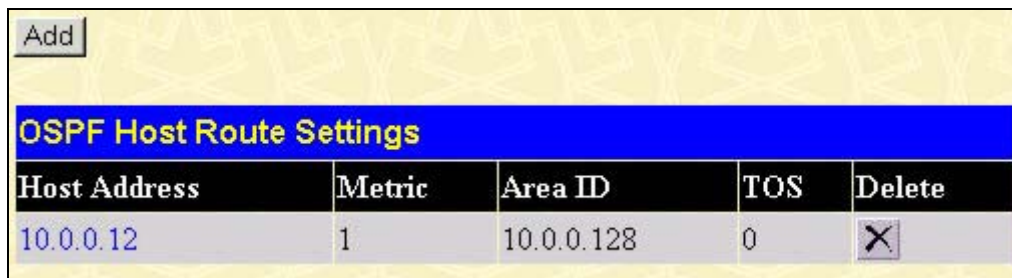
Configure the following settings for OSPF Area Aggregation:

Parameter	Description
<b>Area ID</b>	Allows the entry the OSPF Area ID for which the routing information will be aggregated. This Area ID must be previously defined on the Switch.
<b>Network Number</b>	Sometimes called the Network Address. The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area above.
<b>Network Mask</b>	The subnet mask used for the OSPF Area.
<b>LSDB Type</b>	Specify the type of address aggregation. Choose <i>Summary</i> or <i>NSSA-Ext</i> .
<b>Advertisement</b>	Select <i>Enabled</i> or <i>Disabled</i> to determine whether the selected OSPF Area will advertise its summary LSDB (Network-Number and Network-Mask).

## OSPF Host Route Settings

OSPF host routes work in a way analogous to RIP, only this is used to share OSPF information with other OSPF routers. This is used to work around problems that might prevent OSPF information sharing between routers.

To configure OSPF host routes, click the **OSPF Host Route Settings** link. To add a new OSPF Route, click the **Add** button. Configure the setting in the menu that appears. The Add and Modify windows for OSPF host route setting are nearly identical. The difference being that if you are changing an existing configuration you will be unable to change the Host Address. To change an existing configuration, click on the hyperlinked Host Address in the list for the configuration you want to change and proceed to change the metric or area ID. To eliminate an existing configuration, click the **X** in the Delete column for the configuration being removed.

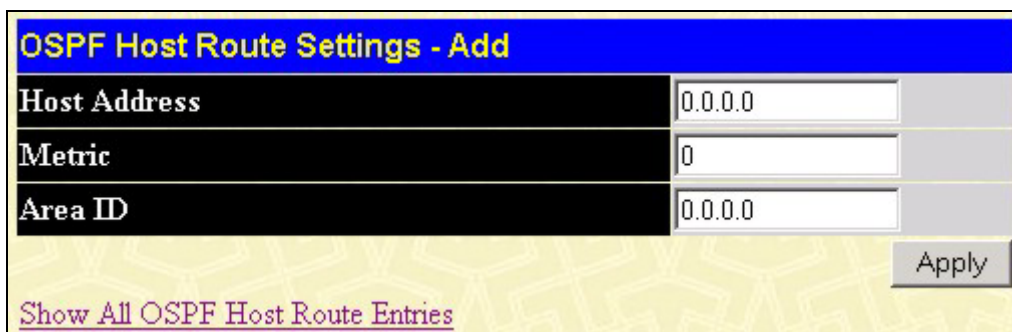


The screenshot shows a web interface window titled "OSPF Host Route Settings". At the top left is an "Add" button. Below the title bar is a table with five columns: Host Address, Metric, Area ID, TOS, and Delete. The first row of data shows Host Address as 10.0.0.12 (which is a hyperlink), Metric as 1, Area ID as 10.0.0.128, TOS as 0, and a Delete column containing an 'X' icon.

Host Address	Metric	Area ID	TOS	Delete
<a href="#">10.0.0.12</a>	1	10.0.0.128	0	X

Figure 5- 38. OSPF Host Route Settings window

Use the window below to set up OSPF host routes.



The screenshot shows a web interface window titled "OSPF Host Route Settings - Add". It contains three input fields: Host Address (with value 0.0.0.0), Metric (with value 0), and Area ID (with value 0.0.0.0). An "Apply" button is located at the bottom right. At the bottom left, there is a link that says "Show All OSPF Host Route Entries".

Figure 5- 39. OSPF Host Route Settings – Add window

Specify the host route settings and click the **Apply** button to add or change the settings. The new settings will appear listed in the **OSPF Host Route Settings** window. To view the previous window, click the [Show All OSPF Host Route Entries](#) link to return to the previous window.

The following fields are configured for OSPF host route:

Parameter	Description
<b>Host Address</b>	The IP address of the OSPF host.
<b>Metric</b>	A value between 1 and 65,535 that will be advertised for the route.
<b>Area ID</b>	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

## DHCP/Bootp Relay

Use DHCP/BOOTP configuration to allow the Switch to relay DHCP/BOOTP information packets to hosts that request them from sources outside the interface on which they reside.

## DHCP/Bootp Relay Information

Figure 5- 40. DHCP/Bootp Relay Information window

This window is used to enable BOOTP Relay and configure hops and time limit. Set the relay configuration as desired and click on the **Apply** button. These settings will be applied to all BOOTP/DHCP relays regardless of the destination or source.

Parameter	Description
<b>Bootp Relay Status</b>	Enable or disable BOOTP/DHCP Relay.
<b>Bootp Hops Count Limit (1-16)</b>	Specifies the maximum number of relay agent hops that the BOOTP packets can cross.
<b>Bootp Relay Time Threshold (0-65535)</b>	If this time is exceeded, the Switch will relay the BOOTP packet.

To configure BOOTP relay for individual IP interfaces, use the following window.

## DHCP/Bootp Relay Settings

Figure 5- 41. DHCP/Bootp Relay Settings window

To create a new relay configuration, enter the IP interface name you want to configure for DHCP relay and the IP address of the server. Click on the **Add** button to enter the relay settings. Up to four servers can be entered for each IP interface. The information listed in the window is described as follows:

Parameter	Description
<b>Interface</b>	The name of the IP interface in which BOOTP relay is to be enabled.
<b>Server IP</b>	The IP address of the BOOTP or DHCP server.

## DNS Relay

Use DNS Relay configuration to allow the Switch to relay DNS information packets to hosts that request them from sources outside the interface on which they reside.

## DNS Relay Information

DNS Relay Information	
DNS Relay Status	Disabled
Primary Name Server	0.0.0.0
Secondary Name Server	0.0.0.0
DNSR Cache Status	Disabled
DNSR Static Table Status	Disabled
Apply	

**Figure 5- 42. DNS Relay Information window**

The **DNS Relay Information** window is used to enable DNS Relay and configure IP addresses for available DNS servers. Set the relay configuration as desired and click on the **Apply** button.

Parameter	Description
<b>DNS Relay Status</b>	Enable or disable DNS Relay.
<b>Primary Name Server</b>	Indicates that the IP address below is the address of the primary DNS server.
<b>Secondary Name Server</b>	Indicates that the IP address below is the address of the secondary DNS server.
<b>DNSR Cache Status</b>	Use this to enable the DNS relay cache function. The DNS cache relay can be used to temporarily store DNS relay information for faster recall.
<b>DNSR Static Table Status</b>	Use this to enable the DNS relay static table. This table will permanently store DNS relay information in a static table. Configure the table using the window pictured below.

To configure permanent entries for the DNS Relay Static Table, use the following window.

## DNS Relay Static Settings

DNS Relay Static Settings		
Domain Name	IP Address	Apply
<input type="text"/>	0.0.0.0.0.0.60.116	Add
DNS Relay Static Table		
Domain Name	IP Address	Delete
yourcompany.com	172.98.12.4	X
		Previous

**Figure 5- 43. DNS Relay Static Settings window**

To create a new DNS Relay Static entry, enter the Domain Name and the associated IP address. Click on the **Add** button to enter the settings into the static table.

Parameter	Description
<b>Domain Name</b>	The domain name used for the static entry.
<b>IP Address</b>	The IP address associated with the domain name.

## VRRP

Virtual Routing Redundancy Protocol (VRRP) is a function on the Switch that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router that controls the IP address associated with a virtual router is called the Master, and will forward packets sent to this IP address. This will allow any Virtual Router IP address on the LAN to be used as the default first hop router by end hosts. Utilizing VRRP, the administrator can achieve a higher available default path cost without needing to configure every end host for dynamic routing or routing discovery protocols.

Statically configured default routes on the LAN are prone to a single point of failure. VRRP is designed to eliminate these failures by setting an election protocol that will assign a responsibility for a virtual router to one of the VRRP routers on the LAN. When a virtual router fails, the election protocol will select a virtual router with the highest priority to be the Master router on the LAN. This retains the link and the connection is kept alive, regardless of the point of failure.

To configure VRRP for virtual routers on the Switch, an IP interface must be present on the system and it must be a part of a VLAN. VRRP IP interfaces may be assigned to every VLAN, and therefore IP interface, on the Switch. VRRP routers within the same VRRP group must be consistent in configuration settings for this protocol to function optimally.

## VRRP Configuration

To enable VRRP globally on the Switch, click **Configuration > Layer 3 IP Networking > VRRP > VRRP Configuration**:

**Figure 5- 44. VRRP Configuration window**

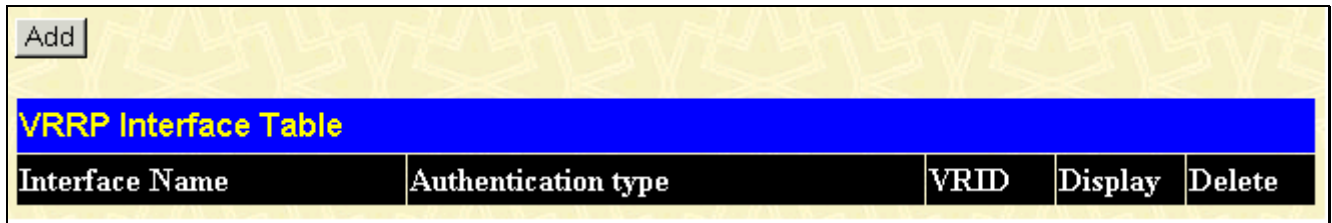
The following fields can be set:

Parameter	Description
<b>Global VRRP</b>	Use the pull-down menu to enable or disable VRRP globally on the Switch. The default is <i>Disabled</i> .
<b>Non-owner response PING</b>	Enabling this parameter will allow the virtual IP address to be PINGed from other host end nodes to verify connectivity. This will only enable the PING connectivity check function. This command is <i>Disabled</i> by default.

Click **Apply** to implement changes made.



## VRRP Interface Settings

The following window will allow the user to set the parameters for the VRRP function on the Switch. To view this window, click **Configuration > Layer 3 IP Networking > VRRP > VRRP Interface Settings**:



**Figure 5- 45. VRRP Interface Table window**

This window displays VRRP entries currently set on the Switch and holds the following information:

Parameter	Description
<b>Interface Name</b>	An IP interface name that has been enabled for VRRP. This entry must have been previously set in the <b>IP Interface Settings</b> window.
<b>Authentication type</b>	Displays the type of authentication used to compare VRRP packets received by a virtual router. Possible authentication types include:  No authentication – No authentication has been selected to compare VRRP packets received by a virtual router.  Simple Text Password – A Simple password has been selected to compare VRRP packets received by a virtual router, for authentication.  IP Authentication Header – An MD5 message digest algorithm has been selected to compare VRRP packets received by a virtual router, for authentication.
<b>VRID</b>	Displays the virtual router ID set by the user. This will uniquely identify the VRRP Interface on the network.
<b>Display</b>	Click the  button to display the settings for this particular VRRP entry.
<b>Delete</b>	Click the  to delete this VRRP entry.

Click the **Add** button to display the following window to configure a VRRP interface. Clicking a hyperlinked **Interface Name** will take you to the same window.

## VRRP Interface Settings

VRRP Interface Settings	
Interface Name	<input type="text"/>
VRID(1-255)	<input type="text" value="0"/>
IP Address	<input type="text" value="0.0.0.0"/>
Admin. State	<input type="text" value="Up"/>
Priority(1-255)	<input type="text" value="0"/>
Advertisement Interval(1-255)	<input type="text" value="0"/>
Preempt Mode	<input type="text" value="True"/>
Critical IP Address	<input type="text" value="0.0.0.0"/>
Checking Critical IP	<input type="text" value="Disabled"/>
Auth. Type	<input type="text" value="None"/>
Auth. Data	<input type="text"/>
<input type="button" value="Apply"/>	
<a href="#">Show All VRRP Interface Entries</a>	

Figure 5- 46. VRRP Interface Settings window

The following parameters may be set to configure an existing or new VRRP interface.


Parameter	Description
<b>Interface Name</b>	Enter the name of a previously configured IP interface to create a VRRP entry for. This IP interface must be assigned to a VLAN on the Switch.
<b>VRID(1-255)</b>	Enter a value between 1 and 255 to uniquely identify this VRRP group on the Switch. All routers participating in this group must be assigned the same <i>VRID</i> value. This value <b>MUST</b> be different from other VRRP groups set on the Switch.
<b>IP Address</b>	Enter the virtual IP address that will be assigned to the VRRP entry. This IP address is also the default gateway that will be statically assigned to end hosts and must be set for all routers that participate in this group.
<b>Admin. State</b>	Used to enable ( <i>Up</i> ) and disable ( <i>Down</i> ) the VRRP IP interface on the Switch.
<b>Priority(1-255)</b>	Enter a value between 1 and 255 to indicate the router priority. The VRRP Priority value may determine if a higher priority VRRP router overrides a lower priority VRRP router. A higher priority will increase the probability that this router will become the Master router of the group. A lower priority will increase the probability that this router will become the backup router. VRRP routers that are assigned the same priority value will elect the highest physical IP address as the Master router. The default value is 100.
<b>Advertisement Interval(1-255)</b>	Enter a time interval value, in seconds, for sending VRRP message packets. This value must be consistent with all routers participating within the same VRRP group and is used to troubleshoot incorrectly configured routers. The default is 1 second.
<b>Preempt Mode</b>	This entry will determine the behavior of backup routers within the VRRP group by controlling whether a higher priority backup router will preempt a lower priority Master



	router. A <i>True</i> entry, along with having the backup router's priority set higher than the masters priority, will set the backup router as the Master router. A <i>False</i> entry will disable the backup router from becoming the Master router. This setting must be consistent with all routers participating within the same VRRP group. The default setting is <i>True</i> .
<b>Critical IP Address</b>	Enter the IP address of the physical device that will provide the most direct route to the Internet or other critical network connections from this virtual router. This must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, a new Master will be elected from the backup routers participating in the VRRP group. If the connection to the backup fails, this backup router cannot assume the Master router role. Different critical IP addresses may be assigned to different routers participating in the VRRP group, and can therefore define multiple routes to the Internet or other critical network connections.
<b>Checking Critical IP</b>	Use the pull-down menu to enable or disable the Critical IP address entered above.
<b>Auth. Type</b>	Specifies the type of authentication used. The Auth. Type must be consistent with all routers participating within the VRRP group. The choices are:  <i>None</i> – Selecting this parameter indicates that VRRP protocol exchanges will not be authenticated.  <i>Simple</i> – Selecting this parameter will require the user to set a simple password in the Auth. Data field for comparing VRRP message packets received by a router. If the two passwords are not exactly the same, the packet will be dropped.  <i>IP</i> – Selecting this parameter will require the user to set a MD5 message digest for authentication in comparing VRRP messages received by the router. If the two values are inconsistent, the packet will be dropped.
<b>Auth. Data</b>	This field is only valid if the user selects <i>Simple</i> or <i>IP</i> in the Auth. Type field. <i>Simple</i> will require the user to enter an alphanumeric string of no more than eight characters to identify VRRP packets received by a router. <i>IP</i> will require the user to enter a MD5 message digest for authentication in comparing VRRP messages received by the router

Click **Apply** to implement changes made.

### VRRP Interface Entry Display

To view the settings for a particular VRRP setting, click the corresponding  in the **VRRP Interface Table** window of the entry, which will display the following:



VRRP Interface Entry Display	
Interface Name	DHT
Authentication type	IP Authentication Header
VRID	2
Virtual IP Address	11.1.1.1
Virtual MAC Address	00:00:5e:00:01:02
Virtual Router State	Initialize
Admin. State	Up
Priority	255
Master IP Address	11.1.1.1
Critical IP Address	10.53.13.224
Checking Critical IP	Enabled
Advertisement Interval	2
Preempt Mode	True
Virtual Router Up Time	0
<a href="#">Show All VRRP Interface Entries</a>	

Figure 5- 47. VRRP Interface Entry Display window

This window displays the following information:

Parameter	Description
<b>Interface Name</b>	An IP interface name that has been enabled for VRRP. This entry must have been previously set in the <b>IP Interface Settings</b> window.
<b>Authentication type</b>	Displays the type of authentication used to compare VRRP packets received by a virtual router. Possible authentication types include:  No authentication – No authentication has been selected to compare VRRP packets received by a virtual router.  Simple Text Password – A Simple password has been selected to compare VRRP packets received by a virtual router, for authentication.  IP Authentication Header – An MD5 message digest algorithm has been selected to compare VRRP packets received by a virtual router, for authentication.
<b>VRID</b>	Displays the virtual router ID set by the user. This will uniquely identify the VRRP Interface on the network.
<b>Virtual IP Address</b>	The IP address of the Virtual router configured on the Switch.
<b>Virtual MAC Address</b>	The MAC address of the device that holds the Virtual router.
<b>Virtual Router State</b>	Displays the current status of the virtual router. Possible states include: Initialize, Master and Backup.
<b>Admin. State</b>	Displays the current state of the router. Up will be displayed if the virtual router is enabled and Down if the virtual router is disabled.

	enabled and Down if the virtual router is disabled.
<b>Priority</b>	Displays the priority of the virtual router. A higher priority will increase the probability that this router will become the Master router of the group. A lower priority will increase the probability that this router will become the backup router. The lower the number, the higher the priority.
<b>Master IP Address</b>	Displays the IP address of the Master router for the VRRP function.
<b>Critical IP Address</b>	Displays the critical IP address of the VRRP function. This address will judge if a virtual router is qualified to be a master router.
<b>Checking Critical IP</b>	Displays the status of the Critical IP address. May be enabled or disabled.
<b>Advertisement Interval</b>	Displays the time interval, in seconds, that VRRP messages are sent out to the network.
<b>Preempt Mode</b>	Displays the mode for determining the behavior of backup routers set on this VRRP interface. True will denote that this will be the backup router, if the routers priority is set higher than the master router. False will disable the backup router from becoming the master router.
<b>Virtual Router Up Time</b>	Displays the time, in minutes, since the virtual router has been initialized

## IP Multicast

Controlling Multicast Routing on the Switch includes setting up IGMP for IP interfaces, PIM and DVMRP. This chapter describes how to set these up. For an explanation of how these protocols function, read Appendix C.

### IGMP Interface Settings

IGMP for IP interfaces function the same way they do for individual ports or VLANs in Layer 2. Most of the parameters are the same as well, except instead of configuring for VLANs you are setting up IGMP for different subnets (IP interfaces).

The IGMP interface links are located in the **IP Multicast** subfolder in the **Layer 3 IP Networking** configuration folder. Click **IGMP Interface Settings**:

IGMP Interface Table							
Interface Name	IP Address	Version	Query	Max Response Time	Robustness Value	Last Member Query Interval	State
<a href="#">System</a>	10.24.22.9	2	125	10	2	1	Disabled

**Figure 5- 48. IGMP Interface Table window**

The Internet Group Multicasting Protocol (IGMP) can be configured on the Switch on a per-IP interface basis. Each IP interface configured on the Switch is displayed in the IGMP Interface Table. To configure an IP interface click on the hyperlinked **Interface Name**:

## IGMP Interface Configuration

IGMP Interface Configuration	
Interface Name	System
IP Address	10.24.22.9
Version	2
Query Interval(1-65535)	125
Max Response Time(1-25)	10
Robustness Variable(1-255)	2
Last Member Query Interval(1-25)	1
State	Disabled

[Show All IGMP Interface Entries](#)

**Figure 5- 49. IGMP Interface Configuration window**

Configure IGMP settings for each IP interface and click on the **Apply** button to apply the new or changed settings. The new values will appear in the IGMP Interface Table. To view the table click [Show All IGMP Interface Entries](#).

The following IGMP interface parameters may be configured per interface:

Parameter	Description
<b>Interface Name &lt;System&gt;</b>	Displays the name of the IP interface that is to be configured for IGMP. This must be a previously configured IP interface.
<b>IP Address</b>	Displays the IP address corresponding to the IP interface name above.
<b>Version &lt;2&gt;</b>	Enter the IGMP version (1 or 2) that will be used to interpret IGMP queries on the interface.
<b>Query Interval(1-65535) &lt;125&gt;</b>	Allows the entry of a value between 1 and 65535 seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.
<b>Max Response Time(1-25) &lt;10&gt;</b>	Sets the maximum amount of time allowed before sending an IGMP response report. A value between 1 and 25 seconds can be entered, with a default of 10 seconds.
<b>Robustness Variable(1-255) &lt;2&gt;</b>	A tuning variable to allow for subnetworks that are expected to lose a large number of packets. A value between 1 and 255 can be entered, with larger values being specified for subnetworks that are expected to lose larger numbers of packets.



**NOTE:** The Robustness Variable field allows IGMP to be 'tuned' for sub-networks that are expected to lose many packets. A high value (max. 255) for the robustness variable will help compensate for 'lossy' sub-networks. A low value (min. 2) should be used for less 'lossy' sub-networks.

## DVMRP

For a description of how Distance Vector Multicast Routing Protocol (DVMRP) works, please read Appendix C.

The DVMRP settings links are located in the **DVMRP** subfolder located in the **Layer 3 IP Networking** configuration folder.

### DVMRP Global Setting

To use DVMRP on the Switch it must be enabled globally. Use the **DVMRP Global Setting** window to enable or disable DVMRP globally. Disabling DVMRP will not affect any DVMRP settings that have been configured so it can later be enabled and apply the same settings.



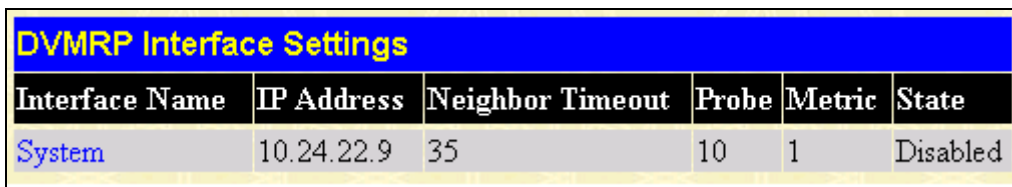
The screenshot shows the 'DVMRP Global Setting' window. It has a blue title bar with the text 'DVMRP Global Setting'. Below the title bar, there is a label 'DVMRP State' followed by a dropdown menu currently set to 'Disabled'. At the bottom right of the window is an 'Apply' button.

Figure 5- 50. DVMRP Global Setting window

Select *Enabled* or *Disabled* and click on the **Apply** button to make the change.

### DVMRP Interface Settings

To configure existing IP interfaces on the Switch for DVMRP, use the **DVMRP Interface Settings** window.

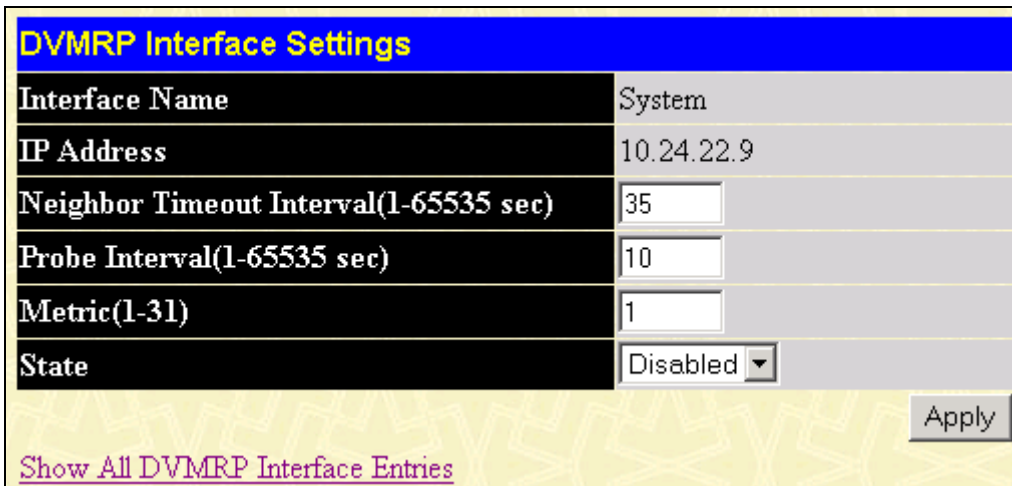


The screenshot shows the 'DVMRP Interface Settings' window. It has a blue title bar with the text 'DVMRP Interface Settings'. Below the title bar is a table with the following data:

Interface Name	IP Address	Neighbor Timeout	Probe	Metric	State
<a href="#">System</a>	10.24.22.9	35	10	1	Disabled

Figure 5- 51. 1<sup>st</sup> DVMRP Interface Settings window

DVMRP settings can be configured on the Switch for existing IP interfaces. Each IP interface configured on the Switch is displayed in the DVMRP Interface Settings table. To configure an IP interface, click on the hyperlinked **Interface Name**:



The screenshot shows the 'DVMRP Interface Settings' window for the 'System' interface. It has a blue title bar with the text 'DVMRP Interface Settings'. Below the title bar, there are several fields for configuration:

- Interface Name:** System
- IP Address:** 10.24.22.9
- Neighbor Timeout Interval(1-65535 sec):** 35
- Probe Interval(1-65535 sec):** 10
- Metric(1-31):** 1
- State:** Disabled (dropdown menu)

At the bottom right is an 'Apply' button. At the bottom left, there is a link: [Show All DVMRP Interface Entries](#).

Figure 5- 52. 2<sup>nd</sup> DVMRP Interface Settings window

Configure DVMRP settings for each IP interface and click on the **Apply** button to apply the new or changed settings. The new values will appear in the DVMRP Interface Settings table in the previous window. To view the table click [Show All DVMRP Interface Entries](#).

The table below describes the parameters necessary for DVMRP configuration.

Configure these settings for each DVMRP interface:

Parameter	Description
<b>Interface Name&lt;System&gt;</b>	Displays the name of the IP interface for which DVMRP is to be configured. This must be a previously defined IP interface.
<b>IP Address</b>	Displays the IP address corresponding to the IP Interface name entered above.
<b>Probe Interval &lt;10&gt;</b>	This field allows an entry between 0 and 65,535 seconds and defines the interval between 'probes'. The default is 10.
<b>Neighbor Timeout Interval &lt;35&gt;</b>	This field allows an entry between 1 and 65,535 seconds and defines the time period for DVMRP will hold Neighbor Router reports before issuing poison route messages. The default is 35 seconds.
<b>Metric &lt;1&gt;</b>	This field allows an entry between 1 and 31 and defines the route cost for the IP interface. The DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hop count in RIP. The default cost is 1.
<b>State &lt;Disabled&gt;</b>	This field can be toggled between <i>Enabled</i> and <i>Disabled</i> and enables or disables DVMRP for the IP interface. The default is <i>Disabled</i> .

## PIM

For a description of how Protocol Independent Multicast-Dense Mode (PIM-DM) functions, please read Appendix C.

The PIM-DM settings links are located in the **PIM** subfolder located in the **Layer 3 IP Networking** folder.

### PIM-DM Global Setting

To use PIM-DM on the Switch it must be enabled globally. Use the **PIM-DM Global Setting** window to enable or disable PIM-DM globally. Disabling PIM-DM will not affect any PIM-DM settings that have been configured so it can later be enabled and apply the same settings.



Figure 5- 53. PIM-DM Global Setting window

Select *Enabled* or *Disabled* and click on the **Apply** button to make the change.

### PIM-DM Interface Settings

PIM-DM Interface Settings				
Interface Name	IP Address	Hello Interval	Join/Purne Interval	State
<a href="#">System</a>	10.41.44.90	30	60	Disabled
<a href="#">if2</a>	20.1.1.1	30	60	Disabled

Figure 5- 54. 1<sup>st</sup> PIM-DM Interface Settings window

PIM-DM settings can be configured on the Switch for existing IP interfaces. Each IP interface configured on the Switch is displayed in the **PIM-DM Interface Settings** window. To configure an IP interface click on the hyperlinked **Interface Name**:

PIM-DM Interface Settings	
Interface Name	if2
IP Address	20.1.1.1
Hello Interval(1-18724 sec)	<input type="text" value="30"/>
Join-Prune Interval(1-18724 sec)	<input type="text" value="60"/>
State	Disabled ▾
<input type="button" value="Apply"/>	
<a href="#">Show All PIM-DM Interface Entries</a>	

Figure 5- 55. 2<sup>nd</sup> PIM-DM Interface Settings window

Configure PIM-DM settings for each IP interface and click on the **Apply** button to apply the new or changed settings. The new values will appear in the 1<sup>st</sup> **PIM-DM Interface Settings** window. To view the table click [Show All PIM-DM Interface Entries](#).

The table below describes the parameters necessary for PIM-DM configuration.

Configure these parameters for PIM-DM interfaces:

Parameter	Description
<b>Interface Name</b>	Allows the entry of the name of the IP interface for which PIM-DM is to be configured. This must be a previously defined IP interface.
<b>IP Address</b>	Displays the IP address for the IP interface named above.
<b>Hello Interval &lt;30&gt;</b>	This field allows an entry of between 0 and 18724 seconds and determines the interval between sending Hello packets to other routers on the network. The default is 30 seconds.
<b>Join/Prune Interval &lt;60 &gt;</b>	This field allows an entry of between 0 and 18724 seconds. This interval also determines the time interval the router uses to automatically remove prune information from a branch of a multicast delivery tree and begin to flood multicast messages to all branches of that delivery tree. These two actions are equivalent. The default is 60 seconds.
<b>State &lt;Disabled&gt;</b>	This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu, and is used to enable or disable PIM-DM for the IP interface. The default is <i>Disabled</i> .

## Section 6

# Security

**Trusted Host**

**Secure Socket Layer (SSL)**

**Download Certificate**

**Configuration**

**Secure Shell (SSH)**

**SSH Configuration**

**SSH Algorithm**

**SSH User Authentication**

**Access Authentication Control**

**Policy and Parameters**

**Application Authentication Settings**

**Authentication Server Group**

**Authentication Server Host**

**Login Method Lists**

**Enable Method Lists**

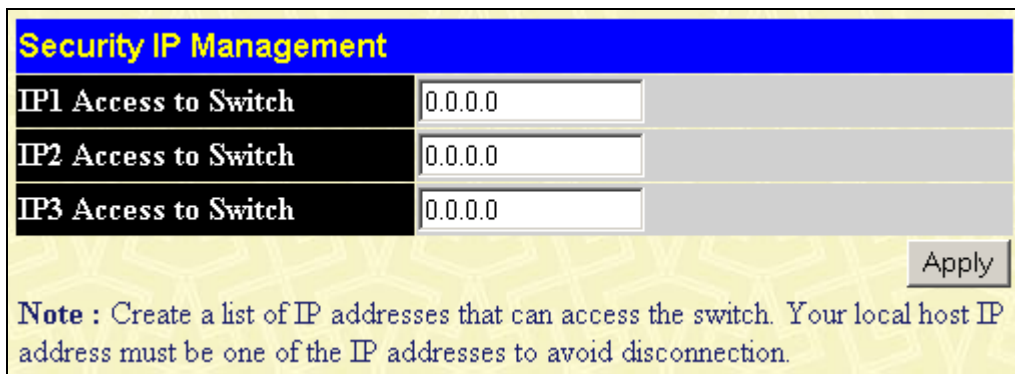
**Local Enable Password**

**Enable Admin**

## 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.



Security IP Management	
IP1 Access to Switch	0.0.0.0
IP2 Access to Switch	0.0.0.0
IP3 Access to Switch	0.0.0.0

Apply

**Note :** Create a list of IP addresses that can access the switch. Your local host IP address must be one of the IP addresses to avoid disconnection.

**Figure 6- 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.

## Secure Socket Layer (SSL)

Secure Sockets Layer or SSL is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a ciphersuite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

**Key Exchange:** The first part of the cyphersuite string specifies the public key algorithm to be used. This switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they “exchange keys” in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.

**Encryption:** The second part of the ciphersuite that includes the encryption used for encrypting the messages sent between client and host. The switch supports two types of cryptology algorithms:

Stream Ciphers – There are two types of stream ciphers on the switch, RC4 with 40-bit keys and RC4 with 128-bit keys. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.

CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The switch supports the 3DES EDE encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.

**Hash Algorithm:** This part of the ciphersuite allows the user to choose a message digest function that will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The switch supports two hash algorithms, MD5 (Message Digest 5) and SHA (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the ciphersuites available, yet different ciphersuites will affect the security level and the performance of the secured connection. The information included in the ciphersuites is not included with the switch and requires downloading from a third source in a file form called a certificate. This function of the switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the switch by utilizing a TFTP server. The switch supports SSLv3 and TLSv1. Other versions of SSL may not be compatible with this switch and may cause problems upon authentication and transfer of messages from client to host.

## Download Certificate

This window is used to download a certificate file for the SSL function on the switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The switch only supports certificate files with .der file extensions.

To view the following window, click **Security > Secure Socket Layer (SSL) > Download Certificate**:



**Figure 6- 2. Download Certificate window**

To download certificates, set the following parameters and click **Apply**.

Parameter	Description
<b>Server IP</b>	Enter the IP address of the TFTP server where the certificate files are located.
<b>Certificate File Name</b>	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)
<b>Key File Name</b>	Enter the path and the filename of the key file you wish to download. This file must have a .der extension (Ex. c:/pkey.der)

## Configuration

This window will allow the user to enable SSL on the Switch and implement any one or combination of listed ciphersuites on the switch. A ciphersuite is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The switch possesses four possible ciphersuites for the SSL function, which are all enabled by default. To utilize a particular ciphersuite, disable the unwanted ciphersuites, leaving the desired one for authentication. When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https://. (Ex. https://10.90.90.90) Any other method will result in an error and no access can be authorized for the web-based management.

To view the following window, click **Security > Secure Socket Layer (SSL) > Configuration**:

**Figure 6- 3. SSL Configuration window**

To set up the SSL function on the switch, configure the following parameters and click **Apply**.

Parameter	Description
<b>RSA with RC4 128 MD5</b>	This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.
<b>RSA with 3DES EDE CBC SHA</b>	This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.
<b>DHE DSS with 3DES EDE CBC SHA</b>	This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.
<b>RSA EXPORT with RC4 40 MD5</b>	This ciphersuite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys. Use the pull-down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.
<b>Status</b>	You can individually enable or disable these four ciphersuites above or use this Status drop-down menu to globally turn encryption on or off without changing the ciphersuite settings you have already made. The default is <i>Disabled</i> .



**NOTE:** Certain implementations concerning the function and configuration of SSL are not available on the web-based management of this Switch and need to be configured using the command line interface. For more information on SSL and its functions, see the ***DGS-3312SR Command Line Reference Manual***, located on the documentation CD of this product.



**NOTE:** Enabling the SSL command will disable the web-based switch management. To log on to the switch again, the header of the URL must begin with https://. Entering anything else into the address field of the web browser will result in an error and no authentication will be granted.

## Secure Shell (SSH)

SSH is the abbreviation of Secure Shell, which is a program allowing secure remote login and secure network services over an insecure network. It allows you to securely login to remote host computers, to execute commands safely in a remote computer and so forth, and to provide secure encrypted and authenticated communications between two non-trusted hosts. SSH with its array of unmatched security features is an essential tool in today's network environment. It is a powerful guardian against the numerous security hazards that nowadays threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH Client) and the Switch (the SSH Server), are as follows:

1. Create a user account with admin-level access using the **User Accounts** window in the **Management** folder. This is identical to creating any other admin-level User account on the Switch, including specifying a password. This password is used to login to the Switch, once secure communication has been established using the SSH protocol.
2. Configure the user account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the **SSH User Authentication** window. There are three

choices as to the method SSH will use to authorize the user, and they are Host Based, Password, Public Key, and None.

3. Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH Client and the SSH Server, using the **SSH Algorithm** window.

4. Finally, enable SSH on the Switch using the **SSH User Authentication** window.

After following the above steps, you can configure an SSH Client on the remote PC and manage the Switch using secure, in-band communication.

## SSH Configuration

The following window is used to configure and view settings on the SSH server and can be opened by clicking **Security > Secure Shell (SSH) > SSH Configuration**:

The screenshot displays the 'SSH Configuration' window, which is divided into two main sections: 'Current SSH Configuration Settings' and 'New SSH Configuration Settings'. The 'Current' section shows a table of existing settings. The 'New' section shows the same settings with input fields for modification. An 'Apply' button is located at the bottom right of the 'New' section.

Current SSH Configuration Settings	
SSH Server Status	Disabled
Max Session	8
Time Out	300
Auth. Fail	2
Session Rekeying	Never
Ports	22

New SSH Configuration Settings	
SSH Server Status	Disabled ▾
Max Session(1-8)	8
Time Out(120-600)	300
Auth. Fail(2-20)	2
Session Rekeying	Never ▾
Port(1-65535)	22

Apply

**Figure 6- 4. Current SSH Configuration Settings window**

To set up the SSH server on the switch, configure the following parameters and click **Apply**.

Parameter	Description
<b>SSH Server Status</b>	Use the pull-down menu to enable or disable SSH on the switch. The default is <i>Disabled</i> .
<b>Max Session(1-8)</b>	Enter a value between 1 and 8 to set the number of users that may simultaneously access the switch. The default is 8.
<b>Time Out(120-600)</b>	Allows the user to set the connection timeout. The user may set a time between 120 and 600 seconds. The default is 300 seconds.

<b>Auth. Fail(2-20)</b>	Allows the administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing SSH authentication. After the maximum number of attempts is exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between 2 and 20. The default is 2.
<b>Session Rekeying</b>	The user may set the time period that the switch will change the security shell encryptions by using the pull-down menu. The options are <i>Never</i> , <i>10 min</i> , <i>30 min</i> , and <i>60 min</i> . The default setting is <i>Never</i> .
<b>Port(1-65535)</b>	Enter the TCP port number associated with this function. The default TCP port number for SSH is 22.

## SSH Algorithm

The **Encryption Algorithm** window allows the configuration of the desired types of SSH algorithm used for authentication encryption. There are four categories of algorithms listed and specific algorithms in each may be enabled or disabled by using their corresponding pull-down menu. All algorithms are enabled by default. To view the following window, click **Security > Secure Shell (SSH) > SSH Algorithm**.

Encryption Algorithm	
3DES-CBC	Enabled ▾
Blow-fish-CBC	Enabled ▾
AES128-CBC	Enabled ▾
AES192-CBC	Enabled ▾
AES256-CBC	Enabled ▾
ARC4	Enabled ▾
Cast128-CBC	Enabled ▾
Twofish128	Enabled ▾
Twofish192	Enabled ▾
Twofish256	Enabled ▾
Data Integrity Algorithm	
HMAC-SHA1	Enabled ▾
HMAC-MD5	Enabled ▾
Public Key Algorithm	
HMAC-RSA	Enabled ▾
HMAC-DSA	Enabled ▾
Authentication Algorithm	
Password	Enabled ▾
Publickey	Enabled ▾
Host-based	Enabled ▾
Apply	

Figure 6- 5. Encryption Algorithm window

The user may set the following parameters:

Parameter	Description
<b>Encryption Algorithm</b>	
<b>3DES-CBC</b>	Use the pull-down menu to enable or disable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
<b>Blow-fish CBC</b>	Use the pull-down menu to enable or disable the Blowfish encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
<b>AES128-CBC</b>	Use the pull-down menu to enable or disable the Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
<b>AES192-CBC</b>	Use the pull-down menu to enable or disable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
<b>AES256-CBC</b>	Use the pull-down menu to enable or disable the Advanced Encryption Standard AES256 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
<b>ARC4</b>	Use the pull-down menu to enable or disable the Arcfour encryption algorithm. The default is <i>Enabled</i> .
<b>Cast128-CBC</b>	Use the pull-down menu to enable or disable the Cast128 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
<b>Twofish128</b>	Use the pull-down menu to enable or disable the twofish128 encryption algorithm. The default is <i>Enabled</i> .
<b>Twofish192</b>	Use the pull-down menu to enable or disable the twofish192 encryption algorithm. The default is <i>Enabled</i> .
<b>Twofish256</b>	Use the pull-down menu to enable or disable the twofish256 encryption algorithm. The default is <i>Enabled</i> .
<b>Data Integrity Algorithm</b>	
<b>HMAC-SHA1</b>	Use the pull-down menu to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Secure Hash Algorithm encryption. The default is <i>Enabled</i> .
<b>HMAC-MD5</b>	Use the pull-down menu to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the MD5 Message Digest encryption algorithm. The default is <i>Enabled</i> .
<b>Public Key Algorithm</b>	
<b>HMAC-RSA</b>	Use the pull-down menu to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. The default is <i>Enabled</i> .
<b>HMAC-DSA</b>	Use the pull-down menu to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Digital Signature Algorithm encryption. The default is <i>Enabled</i> .
<b>Authentication Algorithm</b>	

<b>Password</b>	This parameter may be enabled if the administrator wishes to use a locally configured password for authentication on the switch. The default is <i>Enabled</i> .
<b>Public Key</b>	This parameter may be enabled if the administrator wishes to use a publickey configuration set on a SSH server, for authentication. The default is <i>Enabled</i> .
<b>Host-based</b>	This parameter may be enabled if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. The default is <i>Enabled</i> .

Click **Apply** to implement changes made.

## SSH User Authentication

The following windows are user to configure parameters for users attempting to access the Switch through SSH. To access the following window, click **Security > Secure Shell (SSH) > SSH User Authentication**.

Current Accounts			
User Name	Auth. Mode	Host Name	Host IP

**Figure 6- 6. Current Accounts window**

In the example window above, the user account “TheTrinity” has been previously set using the **User Accounts** window in the **Management** folder. A user account **MUST** be set in order to set the parameters for the SSH user. To configure the parameters for the SSH user, click on the hyperlinked user name in the window above, which will reveal the following window.

<b>User Name</b>	<input type="text" value="TheTrinity"/>
<b>Auth. Mode</b>	<input type="text" value="None"/>
<b>Host Name</b>	<input type="text"/>
<b>Host IP</b>	<input type="checkbox"/> <input type="text" value="0.0.0.0"/>

[Show All User Authentication Entries](#)

**Figure 6- 7. SSH User window**

The user may set the following parameters:

Parameter	Description
<b>User Name</b>	Enter a username of no more than 15 characters to identify the SSH user. This User Name must be a previously configured user account on the switch.
<b>Auth. Mode</b>	<p>The administrator may choose one of the following to set the authorization for users attempting to access the switch:</p> <p><i>Host Based</i> – This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user.</p> <p><i>Host Name</i> – Enter an alphanumeric string of up to 31 characters identifying the remote SSH user.</p> <p><i>Host IP</i> – Enter the corresponding IP address of the SSH user.</p> <p><i>Password</i> – This parameter should be chosen if the user wishes to use an administrator-defined password for authentication. Upon entry of this command, the</p>

	<p>switch will prompt the user for a password, and then to retype the password for confirmation.</p> <p><i>Public Key</i> – This parameter should be chosen if the user wishes to use the public key on a SSH server for authentication.</p> <p><i>None</i> – Choose this parameter if no authentication is desired.</p>
<b>Host Name</b>	Enter an alphanumeric string of up to 31 characters identifying the remote SSH user. This parameter is only used in conjunction with the Host Based choice in the <i>Auth. Mode</i> .
<b>Host IP</b>	Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the Host Based choice in the <i>Auth. Mode</i> .

Click **Apply** to implement changes made.



**NOTE:** To set the SSH User Authentication parameters on the Switch, a user account must be previously configured. For more information on configuring local user accounts on the Switch, see the Security IP section of this document.

## Access Authentication Control

The TACACS/XTACACS/TACACS+/RADIUS commands let you secure access to the switch using the TACACS/XTACACS/TACACS+/RADIUS protocols. When a user logs in to the switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS/XTACACS/TACACS+/RADIUS authentication is enabled on the switch, it will contact a TACACS/XTACACS/TACACS+/RADIUS server to verify the user. If the user is verified, he or she is granted access to the switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The switch's software supports the following versions of TACACS:

- TACACS (Terminal Access Controller Access Control System) – Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.
- Extended TACACS (XTACACS) – An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.
- TACACS+ (Terminal Access Controller Access Control System plus) – Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery

In order for the TACACS/XTACACS/TACACS+/RADIUS security function to work properly, a TACACS/XTACACS/TACACS+/RADIUS server must be configured on a device other than the switch, called an Authentication Server Host and it must include usernames and passwords for authentication. When the user is prompted by the switch to enter usernames and passwords for authentication, the switch contacts the TACACS/XTACACS/TACACS+/RADIUS server to verify, and the server will respond with one of three messages:

- The server verifies the username and password, and the user is granted normal user privileges on the switch.
- The server will not accept the username and password and the user is denied access to the switch.
- The server doesn't respond to the verification query. At this point, the switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The switch has four built-in Authentication Server Groups, one for each of the TACACS, XTACACS, TACACS+, and RADIUS protocols. These built-in Authentication Server Groups are used to authenticate users trying to access the switch. The users will set Authentication Server Hosts in a preferable order in the built-in Authentication Server Groups and when a user tries to gain access to the switch, the switch will ask the first Authentication Server Hosts for authentication. If no



authentication is made, the second server host in the list will be queried, and so on. The built-in Authentication Server Groups can only have hosts that are running the specified protocol. For example, the TACACS Authentication Server Groups can only have TACACS Authentication Server Hosts.

The administrator for the switch may set up six different authentication techniques per user-defined method list (TACACS/XTACACS/TACACS+/RADIUS/local/none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the switch, and may contain up to eight authentication techniques. When a user attempts to access the switch, the switch will select the first technique listed for authentication. If the first technique goes through its Authentication Server Hosts and no authentication is returned, the switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Please note that users granted access to the switch will be granted normal user privileges on the switch. To gain access to administrator level privileges, the user must access the **Enable Admin** window and then enter a password, which was previously configured by the administrator of the switch.



**NOTE:** TACACS, XTACACS, and TACACS+ are separate entities and are not compatible. The switch and the server must be configured exactly the same, using the same protocol. (For example, if the switch is set up for TACACS authentication, so must be the host server.)

## Policy & Parameters

This command will enable an administrator-defined authentication policy for users trying to access the switch. When enabled, the device will check the **Login Method List** and choose a technique for user authentication upon login.

To access the following window, click **Security > Access Authentication Control > Policy & Parameters**:

**Figure 6- 8. Policy & Parameters Settings window**

The following parameters can be set:

Parameters	Description
<b>Authentication Policy</b>	Use the pull-down menu to enable or disable the Authentication Policy on the switch.
<b>Response timeout(1-255)</b>	This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between 1 and 255 seconds. The default setting is 30 seconds.
<b>User attempts(1-255)</b>	This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from 1 to 255. The default setting is 3.

Click **Apply** to implement changes made.



## Application Authentication Settings

This window is used to configure switch configuration applications (console, Telnet, SSH, and web) for login at the user level and at the administration level (Enable Admin) utilizing a previously configured method list.

Application's authentication settings		
Application	Login Method List	Enable Method List
Console	default ▼	default ▼
Telnet	default ▼	default ▼
SSH	default ▼	default ▼
HTTP	default ▼	default ▼

Apply

**Figure 6- 9. Application's authentication settings window**

The following parameters can be set:


Parameter	Description
<b>Application</b>	Lists the configuration applications on the switch. The user may configure the Login Method List and Enable Method List for authentication for users utilizing the Console (Command Line Interface) application, the Telnet application, the Secure Shell (SSH) application, and the Web (HTTP) application.
<b>Login Method List</b>	Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the <b>Login Method List Settings</b> window, in this section, for more information
<b>Enable Method List</b>	Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the <b>Enable Method List Settings</b> window, in this section, for more information

Click **Apply** to implement changes made.

## Authentication Server Group

This window will allow users to set up Authentication Server Groups on the Switch. A server group is a technique used to group RADIUS, TACACS, TACACS+, and XTACACS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The switch has four built-in Authentication Server Groups that cannot be removed but can be modified. Up to eight authentication server hosts may be added to any particular group.

To view the following window, click **Security > Access Authentication Control > Authentication Server Group**:







Authentication Server Group Settings	
Group Name	Delete
<a href="#">radius</a>	
<a href="#">tacacs</a>	
<a href="#">tacacs+</a>	
<a href="#">xtacacs</a>	

Figure 6- 10. Authentication Server Group Settings window

This window displays the Authentication Server Groups on the Switch. The Switch has four built-in Authentication Server Groups that cannot be removed but can be modified. To modify a particular group, click its hyperlinked Group Name, which will then display the following window.


Add a Server Host to Server Group ( radius )		
IP Address	<input type="text" value="0.0.0.0"/>	
Protocol	TACACS 	
<input type="button" value="Add"/>		
Server Group ( radius )		
IP Address	Protocol	Delete
<a href="#">Show All Server Group Entries</a>		

Figure 6- 11. Add a Server Host to Server Group (radius) window

To add an Authentication Server Host to the list, enter its IP address in the IP Address field, choose the protocol associated with the IP address of the Authentication Server Host (*RADIUS*, *TACACS*, *TACACS+*, or *XTACACS*) and click **Add** to add this Authentication Server Host to the group.



**NOTE:** The user must configure Authentication Server Hosts using the **Authentication Server Host Settings** window before adding hosts to the list. Authentication Server Hosts must be configured for their specific protocol on a remote centralized server before this function can work properly.



**NOTE:** The four built in server groups can only have server hosts running the same TACACS/RADIUS daemon. RADIUS, TACACS, TACACS+, and XTACACS protocols are separate entities and are not compatible with each other.

## Authentication Server Host

This window will set user-defined Authentication Server Hosts for the RADIUS, TACACS, TACACS+, and XTACACS security protocols on the switch. When a user attempts to access the switch with Authentication Policy enabled, the switch will send authentication packets to a remote RADIUS/TACACS/XTACACS/TACACS+ server host on a remote host. The RADIUS/TACACS/TACACS+/XTACACS server host will then verify or deny the request and return the appropriate message to the switch. More than one authentication protocol can be run on the same physical server host but, remember

that RADIUS/TACACS/TACACS+/XTACACS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

To view the following window, click **Security > Access Authentication Control > Authentication Server Host**:

**Figure 6- 12. Authentication Server Host Settings window**

To add an Authentication Server Host, click the **Add** button, revealing the following window:

**Figure 6- 13. Authentication Server Host Setting window – Add window**

Configure the following parameters to add an Authentication Server Host:

Parameter	Description
<b>IP Address</b>	The IP address of the remote server host the user wishes to add.
<b>Protocol</b>	<p>The protocol used by the server host. The user may choose one of the following:</p> <p><i>TACACS</i> – Enter this parameter if the server host utilizes the TACACS protocol.</p> <p><i>XTACACS</i> – Enter this parameter if the server host utilizes the XTACACS protocol.</p> <p><i>TACACS+</i> – Enter this parameter if the server host utilizes the TACACS+ protocol.</p> <p><i>RADIUS</i> – Enter this parameter if the server host utilizes the RADIUS protocol.</p>
<b>Port(1-65535)</b>	Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+/RADIUS servers but the user may set a unique port number for higher security.
<b>Timeout(1-255)</b>	Enter the time in seconds the switch will wait for the server host to reply to an authentication request. The default value is 5 seconds.

	authentication request. The default value is 5 seconds.
<b>Retransmit(1-255)</b>	Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS/RADIUS server does not respond.
<b>Key</b>	Authentication key to be shared with a configured TACACS+ server only. Specify an alphanumeric string up to 254 characters.

Click **Apply** to add the server host.



**NOTE:** More than one authentication protocol can be run on the same physical server host but, remember that RADIUS, TACACS, TACACS+, and XTACACS are separate entities and are not compatible with each other

## Login Method Lists

This command will configure a user-defined or default Login Method List of authentication techniques for users logging on to the Switch. The sequence of techniques implemented in this command will affect the authentication result. For example, if a user enters a sequence of techniques, for example TACACS – XTACACS – local, the Switch will send an authentication request to the first TACACS host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the local account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch.

Successful login using any of these techniques will give the user a “user” privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must use the **Enable Admin** window, in which the user must enter a previously configured password, set by the administrator. (See the **Enable Admin** part of this section for more detailed information concerning the **Enable Admin** command.)

To view the following window, click **Security > Access Authentication Control > Login Method Lists**:

Login Method List Settings					
Method List Name	Method 1	Method 2	Method 3	Method 4	Delete
default	local				

**Figure 6- 14. Login Method Lists Settings window**

The Switch contains one Method List that is set and cannot be removed, yet can be modified. To delete a Login Method List defined by the user, click the under the **Delete** heading corresponding to the entry desired to be deleted. To modify a Login Method List, click on its hyperlinked Method List Name. To configure a Method List, click the **Add** button.

Both actions will result in the same window to configure:

Figure 6- 15. Login Method List – Add window

Figure 6- 16. Login Method List – Edit window

To define a Login Method List, set the following parameters and click **Apply**:

Parameter	Description
<b>Method List Name</b>	Enter a method list name defined by the user of up to 15 characters.
<b>Method 1, 2, 3, 4</b>	<p>The user may add one, or a combination of up to four of the following authentication methods to this method list:</p> <p><i>local</i> - Adding this parameter will require the user to be authenticated using the local user account database on the switch.</p> <p><i>none</i> – Adding this parameter will require no authentication to access the switch.</p> <p><i>radius</i> - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.</p> <p><i>tacacs</i> – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.</p> <p><i>tacacs+</i> – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.</p> <p><i>xtacacs</i> – Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server.</p>

## Enable Method Lists

This window is used to set up Method Lists to promote users with normal level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like TACACS – XTACACS – Local Enable, the Switch will send an authentication request to the first TACACS host in the server group. If no verification is found, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the Local Enable password set in the Switch is used to authenticate the user.

Successful authentication using any of these methods will give the user an “Admin” privilege.



**NOTE:** To set the Local Enable Password, see the next section, entitled **Local Enable Password**.

To view the following table, click **Security > Access Authentication Control > Enable Method Lists**:

Add					
Enable Method List Settings					
Method List Name	Method 1	Method 2	Method 3	Method 4	Delete
<a href="#">default</a>	local_enable				

**Figure 6- 17. Enable Method List Settings window**

To delete an Enable Method List defined by the user, click the under the **Delete** heading corresponding to the entry desired to be deleted. To modify an Enable Method List, click on its hyperlinked Enable Method List Name. To configure a Method List, click the **Add** button.

Both actions will result in the same window to configure:

Enable Method List - Add	
Method List Name	<input type="text"/>
Method 1	local_enable
Method 2	<input type="text"/>
Method 3	<input type="text"/>
Method 4	<input type="text"/>
<input type="button" value="Apply"/>	
<a href="#">Show All Authentication Enable List Entries</a>	

**Figure 6- 18. Enable Method List – Add window**



Figure 6- 19. Enable Method List – Edit window

To define an **Enable Login Method List**, set the following parameters and click **Apply**:

Parameter	Description
<b>Method List Name</b>	Enter a method list name defined by the user of up to 15 characters.
<b>Method 1, 2, 3, 4</b>	<p>The user may add one, or a combination of up to four of the following authentication methods to this method list:</p> <p><i>local_enable</i> - Adding this parameter will require the user to be authenticated using the local enable password database on the Switch. The local enable password must be set by the user in the next section, entitled Local Enable Password.</p> <p><i>none</i> – Adding this parameter will require no authentication to access the switch.</p> <p><i>radius</i> - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.</p> <p><i>tacacs</i> – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.</p> <p><i>tacacs+</i> – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.</p> <p><i>xtacacs</i> – Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server.</p>

## Local Enable Password

This window will configure the locally enabled password for Enable Admin. When a user chooses the Local\_Enable method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.

To view the following window, click **Security > Access Authentication Control > Local Enable Password**:

Figure 6- 20. Configure Local Enable Password window

To set the Local Enable Password, set the following parameters and click **Apply**.

Parameter	Description
<b>Old Local Enable</b>	If a password was previously configured for this entry, enter it here in order to change it to a new password
<b>New Local Enable</b>	Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters.
<b>Confirm Local Enable</b>	Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

## Enable Admin

This window is for users who have logged on to the Switch on the normal user level, and wish to be promoted to the administrator level. After logging on to the Switch, users will have only user level privileges. To gain access to administrator level privileges, the user will open this window and will have to enter an authentication password. Possible authentication methods for this function include RADIUS, TACACS, TACACS+, and XTACACS, local enable (local account on the switch), or no authentication (none). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host, which has the username “enable”, and a password configured by the administrator that will support the enable function. This function becomes inoperable when the authentication policy is disabled.

To view the following window, click **Security > Access Authentication Control > Enable Admin**:



**Figure 6- 21. Enable Admin window**

When this window appears, click the **Enable Admin** button revealing a dialog box for the user to enter authentication (password, username), as seen below. A successful entry will promote the user to Administrator level privileges on the switch.





**Figure 6- 22. Enter Network Password dialog box**

## Section 7

# Management

*User Accounts*

*SNMPV3*

*SNMP User Table*

*SNMP View Table*

*SNMP Group Table*

*SNMP Community Table*

*SNMP Host Table*

*SNMP Engine ID*

## User Accounts

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, as shown below.

User Account Management		
User Name	Access Right	Add
br5-49	Admin	Modify
dilbert1	User	Modify
routergods	Admin	Modify
sinatra	User	Modify

Figure 7- 1. User Account Management window

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

User Account Modify Table		
User Name	<input type="text" value="newguy3"/>	
New Password	<input type="password" value="*****"/>	
Confirm New Password	<input type="password" value="*****"/>	
Access Right	<div> <div>User</div> <div>User</div> <div>Admin</div> </div>	
<a href="#">Show All User Account Entries</a>		<input type="button" value="Apply"/>

Figure 7- 2. User Account Modify Table window

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.

**Figure 7- 3. User Account Modify Table window**

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 7- 1. Admin and User Privileges**

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

## SNMPV3

The DGS-3312SR 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 DGS-3312SR 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.

User Name	Group Name	SNMP Version	Delete
<a href="#">initial</a>	initial	V3	X

**Figure 7- 4. 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 hyperlinked User Name. This will open the **SNMP User Table Display** window, as shown below.

Parameter	Value
User Name	initial
Group Name	initial
SNMP Version	V3
Auth-Protocol	None
Priv-Protocol	None

[Show All SNMP User Table Entries](#)

**Figure 7- 5. 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.

*None* – Indicates that no authorization protocol is in use.

**Priv-Protocol**

*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 7- 6. SNMP User Table Configuration window**

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.

**Add**

Total Entries:8 (Note: It is allowed insert 30 entries into the table only.)

SNMP View Table			
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 7- 7. 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

**SNMP View Table Configuration**

View Name:

Subtree OID:

View Type: Included ▼

**Apply**

[Show All SNMP View Table Entries](#)

Figure 7- 8. 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.



**View Type**

Select *Included* to include this object in the list of objects that an SNMP 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 7- 9. 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

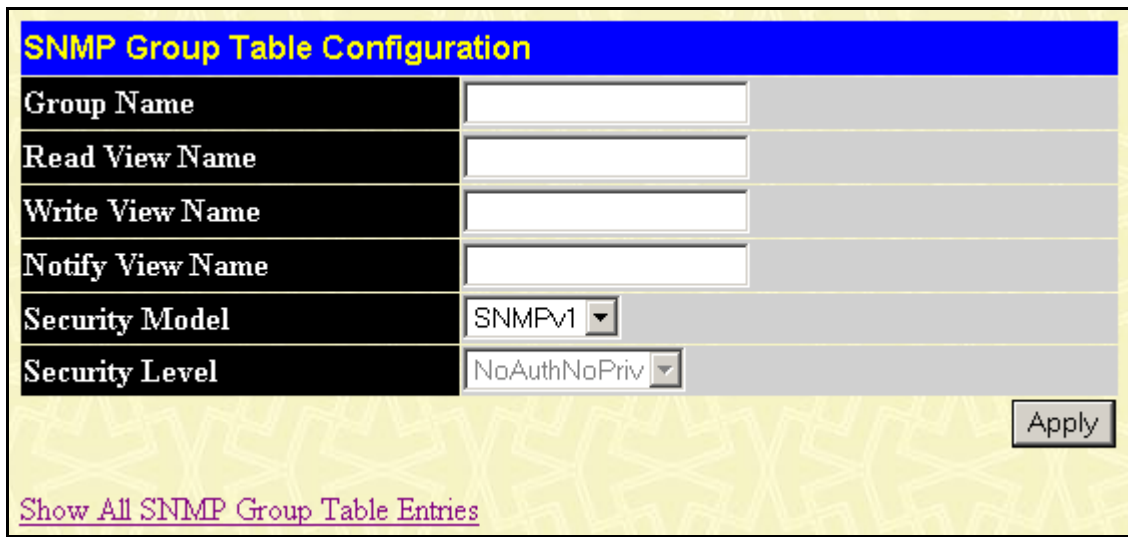
To display the current settings for an existing SNMP Group Table entry, click the blue hyperlink for the entry under the Group Name heading.

SNMP Group Table Display	
Group Name	public
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 7- 10. 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



The image shows a web-based configuration window titled "SNMP Group Table Configuration". It contains several input fields and dropdown menus. The fields are: "Group Name", "Read View Name", "Write View Name", and "Notify View Name", each with a text input box. The "Security Model" field has a dropdown menu with "SNMPv1" selected. The "Security Level" field has a dropdown menu with "NoAuthNoPriv" selected. There is an "Apply" button at the bottom right. Below the form, there is a link that says "Show All SNMP Group Table Entries".

**Figure 7- 11. 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>SNMPv3</i> – 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 sent between the Switch and a remote SNMP manger will be encrypted.</p>

## 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.

The image shows a web-based configuration window titled "SNMP Community Table Configuration". It contains a form with three input fields: "Community Name", "View Name", and "Access Right" (a dropdown menu currently set to "Read\_Only"). An "Apply" button is located to the right of the form. Below the form, it states "Total Entries: 2 (Note: It is allowed insert 10 entries into the table only.)". Below this is a table titled "SNMP Community Table" with four columns: "Community Name", "View Name", "Access Right", and "Delete". The table contains two entries: one for "private" with "CommunityView" and "Read\_Write" permissions, and another for "public" with "CommunityView" and "Read\_Only" permissions. Each entry has an "X" icon in the "Delete" column.

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

Figure 7- 12. 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.

Add

Total Entries:0 (Note: It is allowed insert 10 entries into the table only.)

SNMP Host Table			
Host IP Address	SNMP Version	Community Name/SNMPv3 User Name	Delete

Figure 7- 13. 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

SNMP Host Table Configuration

Host IP Address: 0.0.0.0

SNMP Version: V1

Community String / SNMPv3 User Name:

Apply

[Show All SNMP Host Table Entries](#)

Figure 7- 14. SNMP Host Table Configuration window

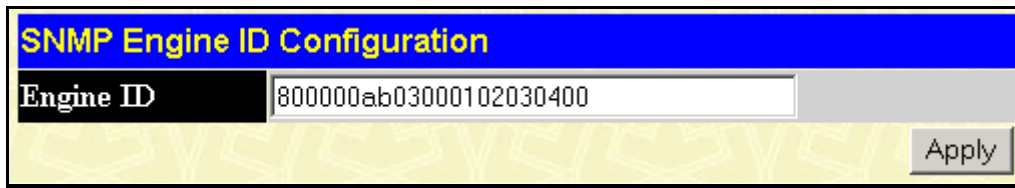
The following parameters can set:

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>	<p>V1 – Specifies that SNMP version 1 will be used.</p> <p>V2c – Specify that SNMP version 2c will be used.</p> <p>V3-NoAuth-NoPriv – Specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level.</p> <p>V3-Auth-NoPriv – Specify that the SNMP version 3 will be used, with an Auth-NoPriv security level.</p> <p>V3-Auth-Priv – Specify that the SNMP version 3 will be used, with an Auth-Priv security level.</p>
<b>Community String or SNMP V3 User Name</b>	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.

The image shows a web-based configuration window titled "SNMP Engine ID Configuration". The title bar is blue with yellow text. Below the title bar, there is a label "Engine ID" in a black box. To the right of the label is a text input field containing the hexadecimal string "8000000ab03000102030400". To the right of the input field is a grey "Apply" button. The background of the window has a light yellow pattern.

**Figure 7- 15. SNMP Engine ID Configuration window**

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

<h2>Section 8</h2>
--------------------

# Monitoring

*Stack Information*

*Port Utilization*

*CPU Utilization*

*Packets*

*Received (RX)*

*UMB\_cast (RX)*

*Transmitted (TX)*

*Errors*

*Received (RX)*

*Transmitted (TX)*

*Size*

*Packet Size*

*MAC Address*

*Switch History*

*IGMP Snooping*

*Browse Router Port*

*VLAN Status*

*Session Table*

*Layer 3 Feature*

*Browse IP Address Table*

*Browse Routing Table*

*Browse ARP Table*

*Browse IP Multicast Forwarding Table*

*Browse IGMP Group Table*

*OSPF Monitor*

*Browse OSPF LSDB Table*

*Browse OSPF Neighbor Table*

*Browse OSPF Virtual Neighbor Table*

*DVMRP Monitor*

*Browse DVMRP Routing Table*

*Browse DVMRP Neighbor Table*

*Browse DVMRP Routing Next Hop Table*

*PIM Monitor*

*Browse PIM Neighbor Table*

The DGS-3312SR provides extensive network monitoring capabilities that can be viewed from the **Monitoring** folder. Links to monitoring windows associated with Layer 3 Switch operations are located in a sub-folder within the **Monitoring** folder.

## Stack Information

The DGS-3312SR 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 DEM-540 Stacking modules must be installed in order to use the Switch in a stacked configuration.
2. Slave Switch units in a stacked Switch group must be uniform in type and model, furthermore they must be one of the Switch models intended for use with the DGS-3312SR, namely the DES-3226S Switches.

One stacking module can be installed to stack up to four additional slave Switch units or two modules can be installed to stack up to eight additional slave Switch units.

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.

Stack Mode Setup												
Stack Topology	Auto Detect											
Setting	MASTER											
Current	MASTER											
Stack Mode State	Enable ▾											
Stack Port	1	2	3	4	5	6	7	8	9	10	11	12
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Apply												
Total Entries : 1												
Stack Information Table												
ID	MAC Address	Port Range	Mode	Version	RPS Status	Model Name						
15	00-80-c8-32-12-e0	1-12	MASTER	2.00-B17	Present	DGS-3312SR						

**Figure 8- 1. 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 DGS-3312SR will always display an F (15 in hex), regardless of whether the DGS-3312SR 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 Port 1.

Stack Mode Setup												
Stack Topology	Auto Detect											
Setting	MASTER											
Current	MASTER											
Stack Mode State	Enable <input type="button" value="v"/>											
Stack Port	1	2	3	4	5	6	7	8	9	10	11	12
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Apply"/>												
Total Entries : 2												
Stack Information Table												
ID	MAC Address	Port Range	Mode	Version	RPS Status	Model Name						
15	00-80-c8-32-12-e0	1-12	MASTER	2.00-B17	Present	DGS-3312SR						
5	00-01-02-41-44-01	251-276	SLAVE	4.02-B03	Not Support	DES-3226S						

**Figure 8- 2. Stack Mode Setup (stacking enabled) window**

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>RPS Status</b>	Displays the status of an optional Redundant Power Supply.
<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.

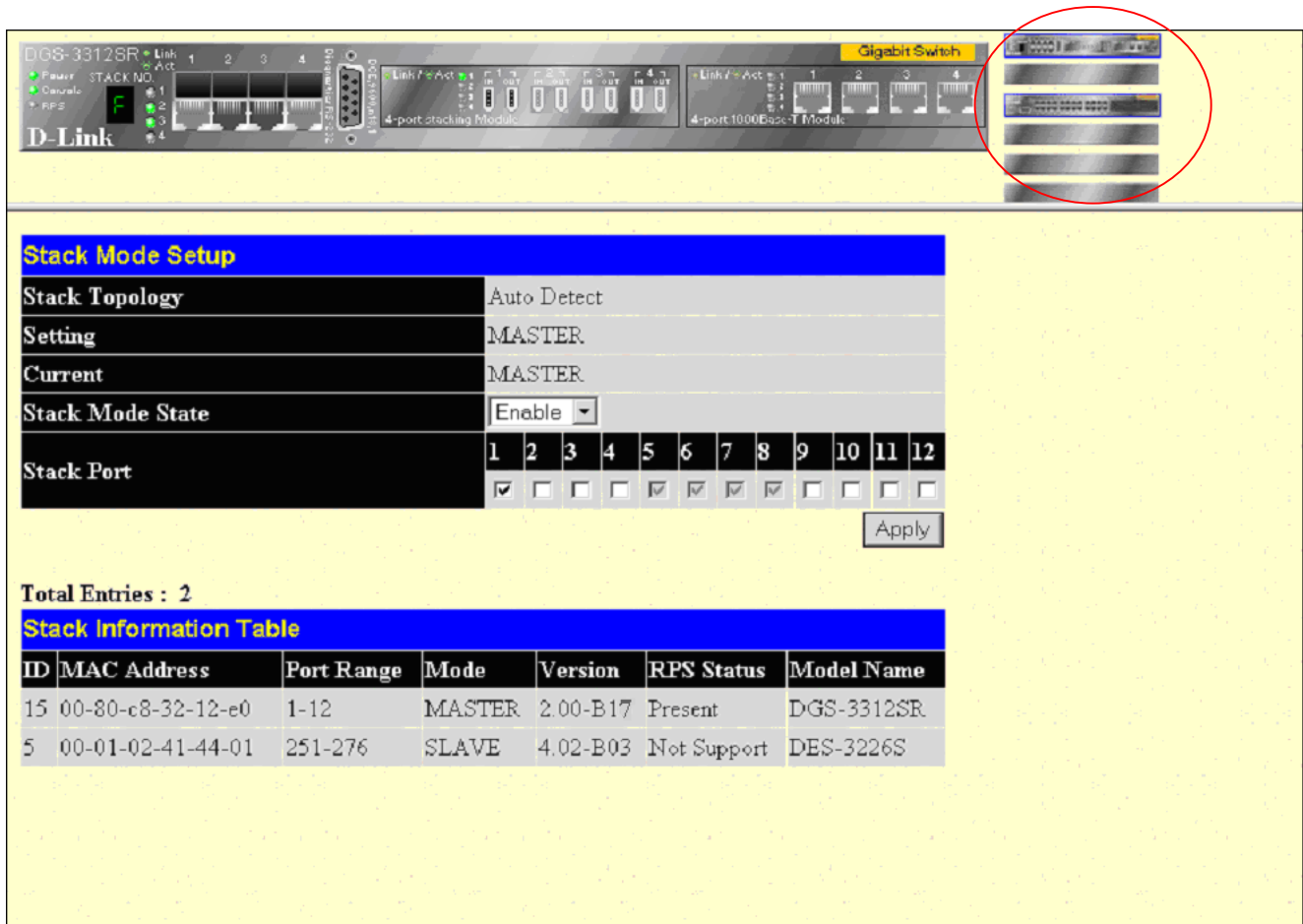


Figure 8- 3. Stack Information web page

## 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:

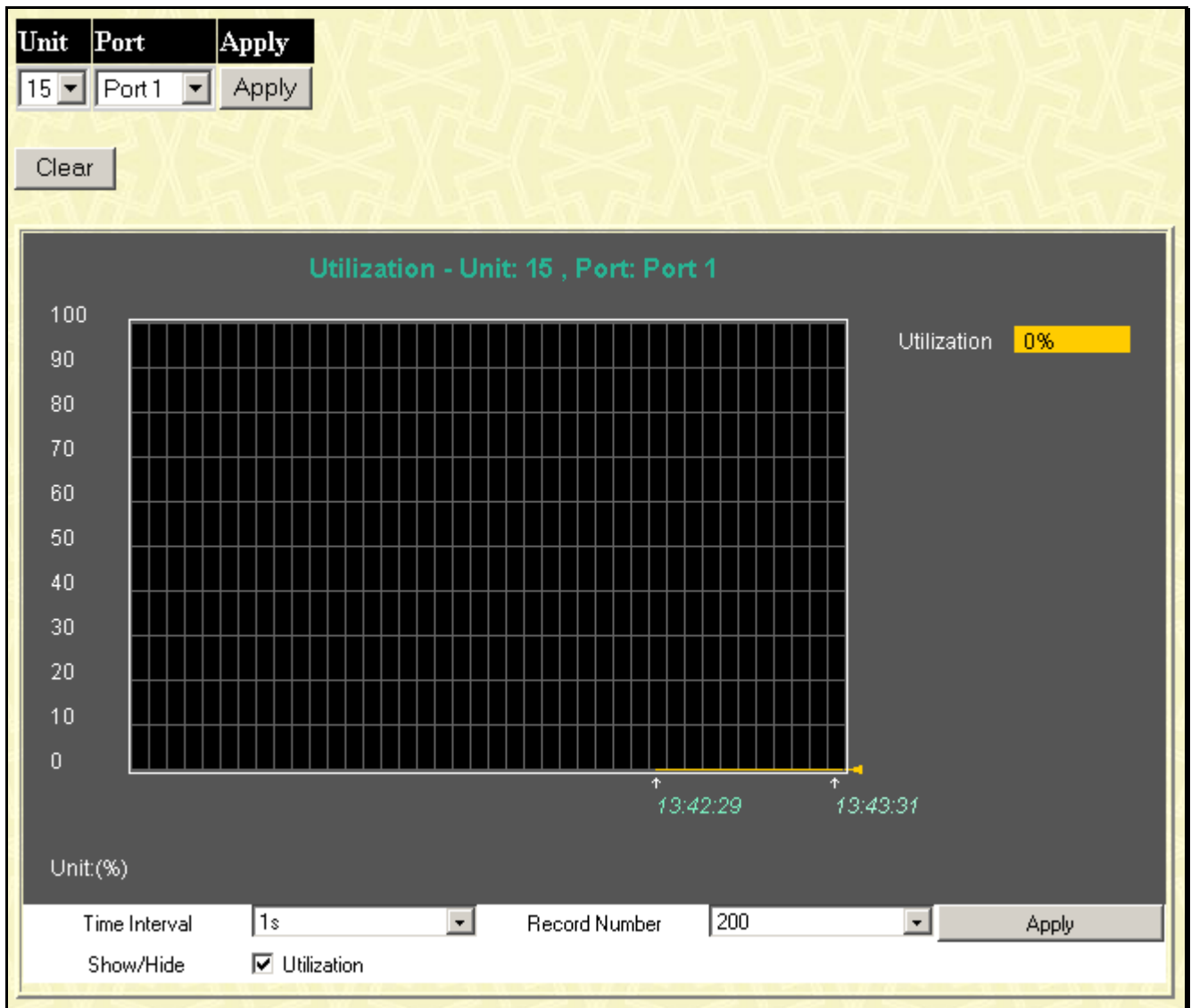


Figure 8- 4. Utilization window

The following field can be set:

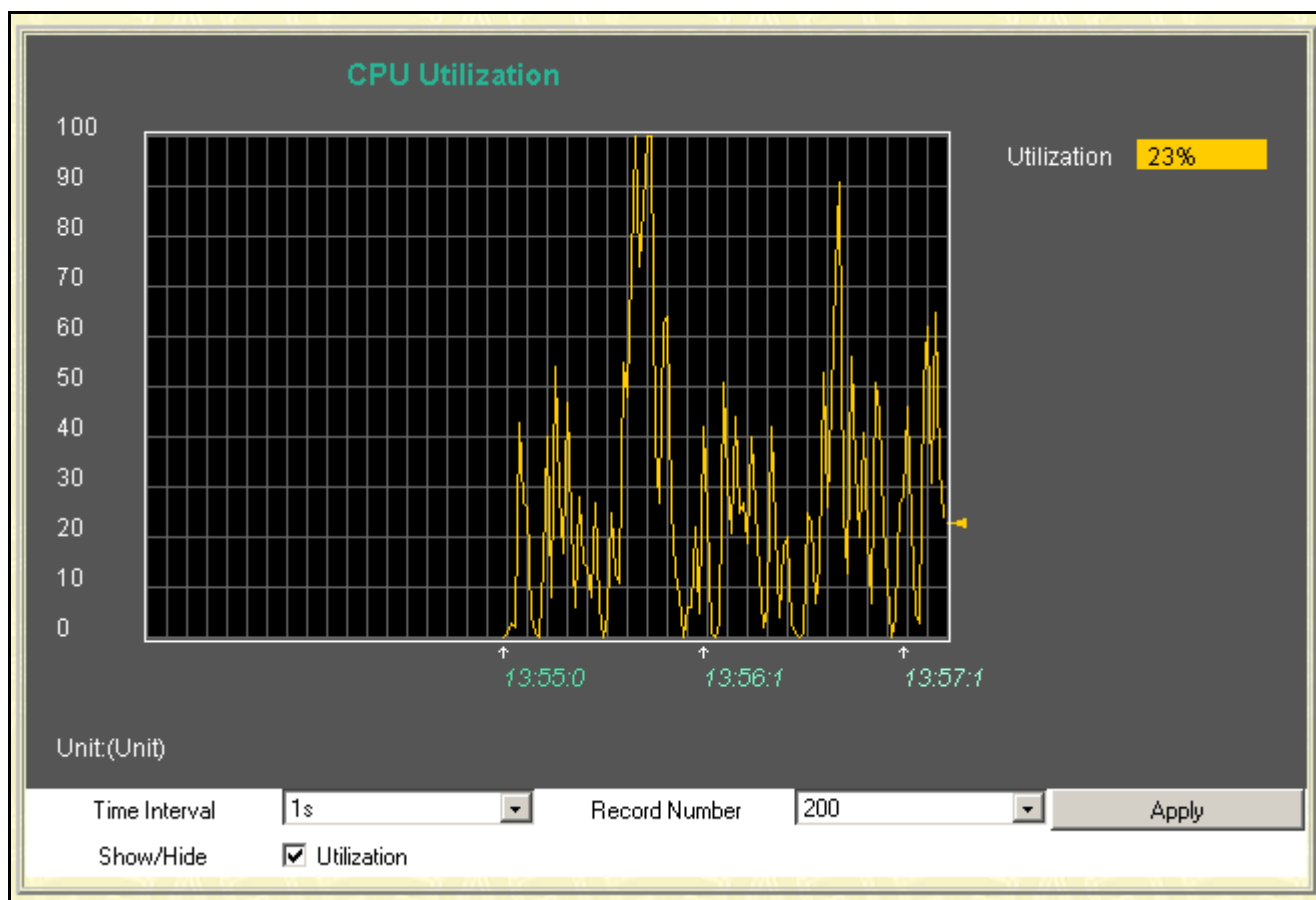
Parameter	Description
<b>Unit</b>	Allows you to specify a Switch in a Switch stack using that Switch's Unit ID. The number 15 indicates a Switch in standalone mode.
<b>Port</b>	Allows you to specify a port to monitor from the Switch selected above.
<b>Clear</b>	Clicking this button clears all statistics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



## CPU Utilization

This **CPU Utilization** window displays the moving average of the CPU.

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



**Figure 8- 5. CPU Utilization window**

The following field can be set:

Parameter	Description
<b>Time Interval</b> <1s>	Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.
<b>Record Number</b> <200>	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

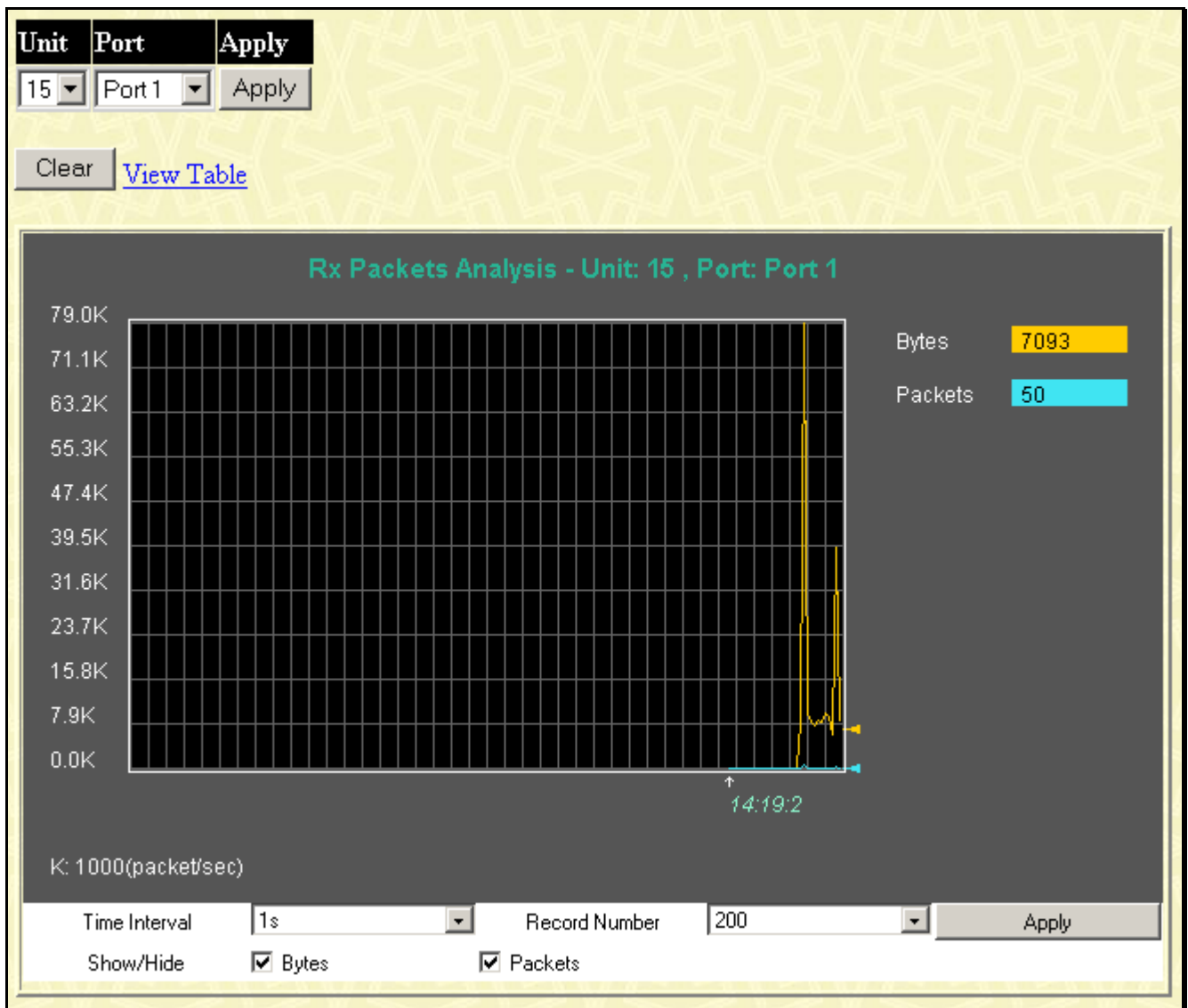
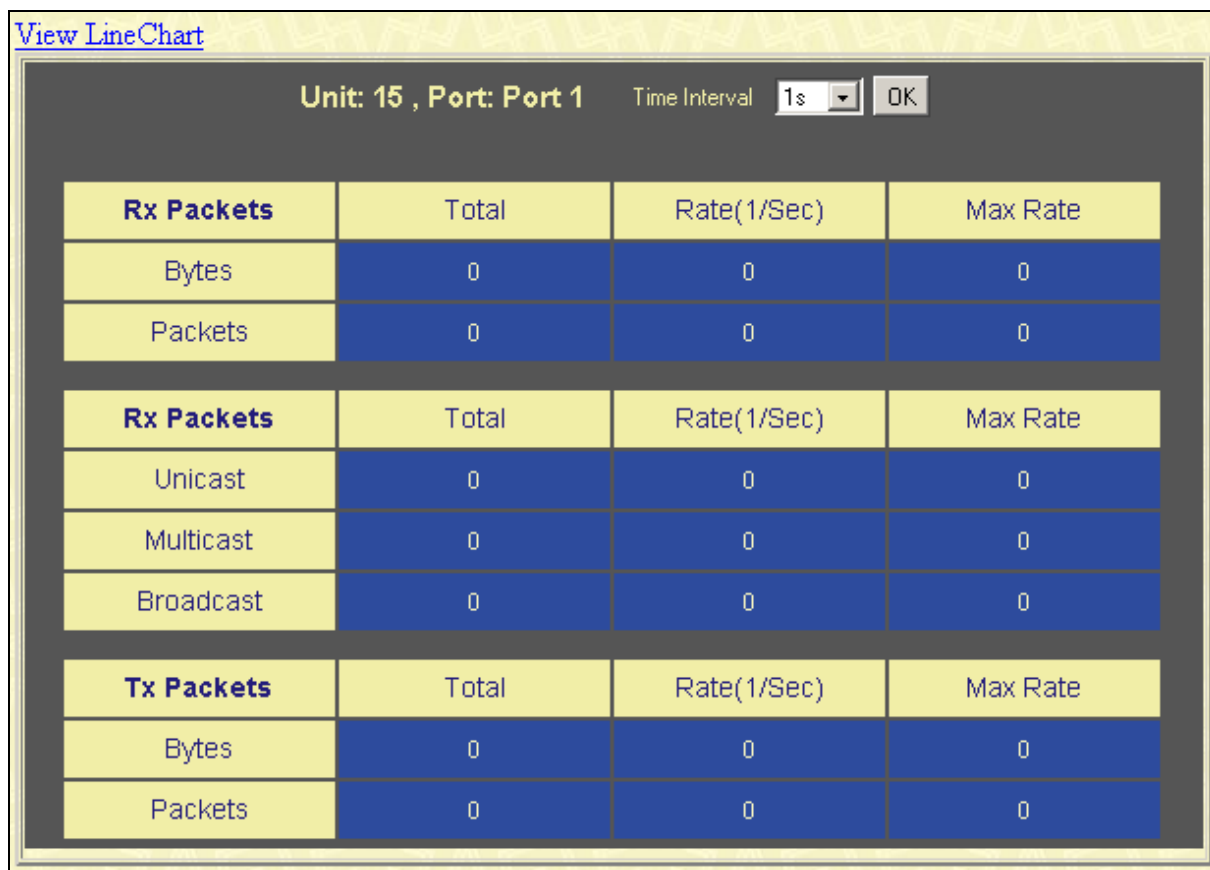


Figure 8- 6. Rx Packets Analysis (line graph for Bytes & Packets) window



**Figure 8- 7. 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

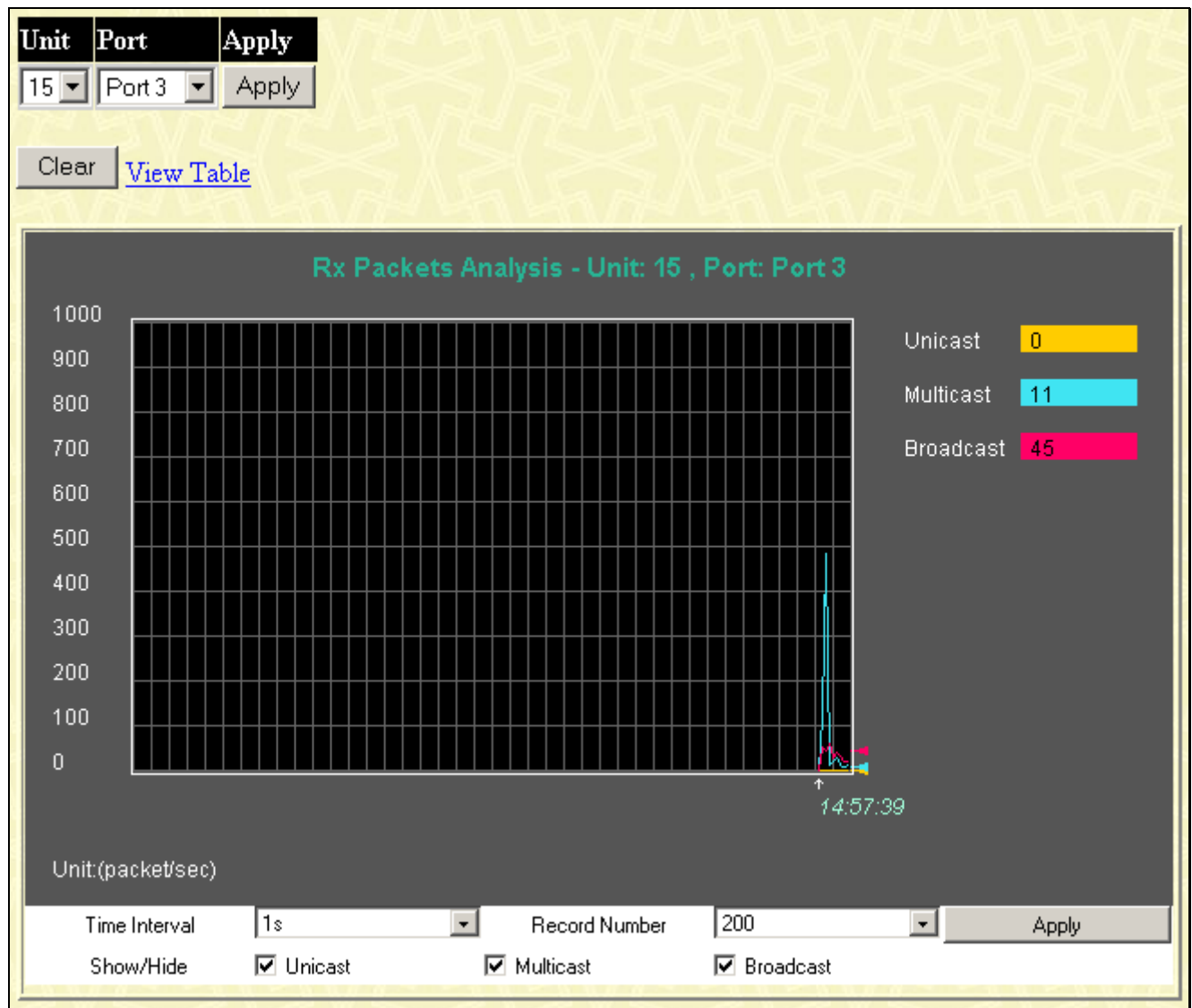
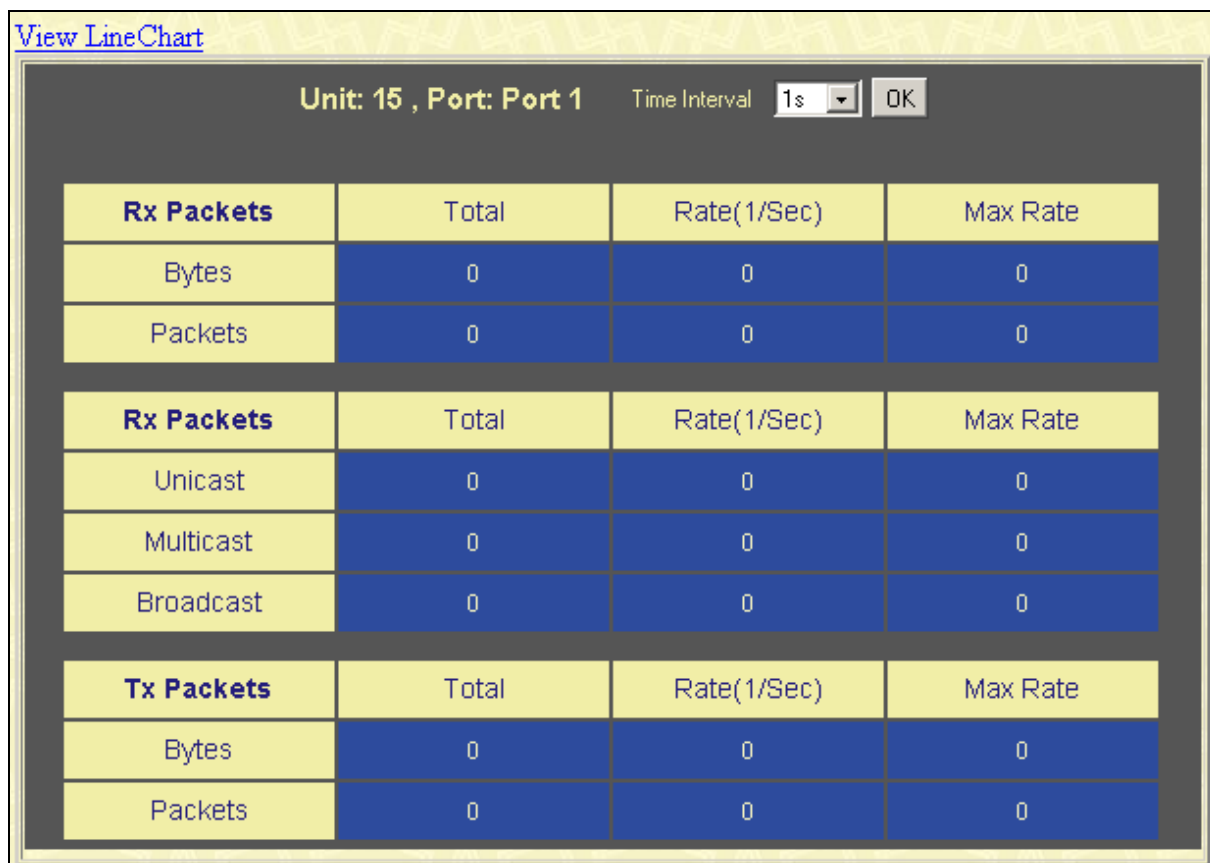


Figure 8- 8. Rx Packets Analysis (line graph for Unicast, Multicast, & Broadcast) window



**Figure 8- 9. Rx Packets Analysis (table for Unicast, Multicast, & Broadcast) window**

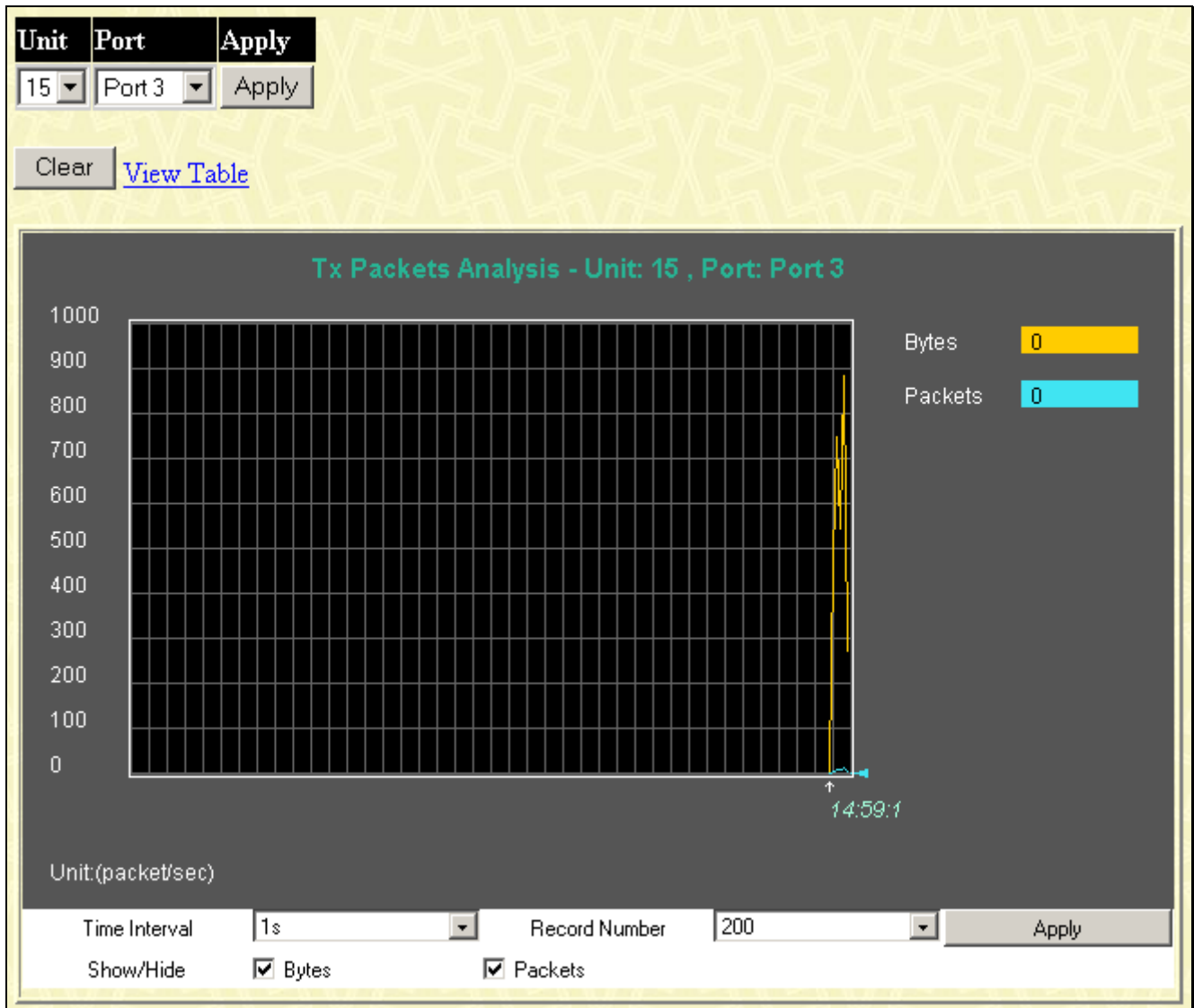
Select the desired Switch using the **Unit** drop-down menu and the desired port using the **Port** drop-down menu. The **Time Interval** field sets the interval at which the error statistics are updated.

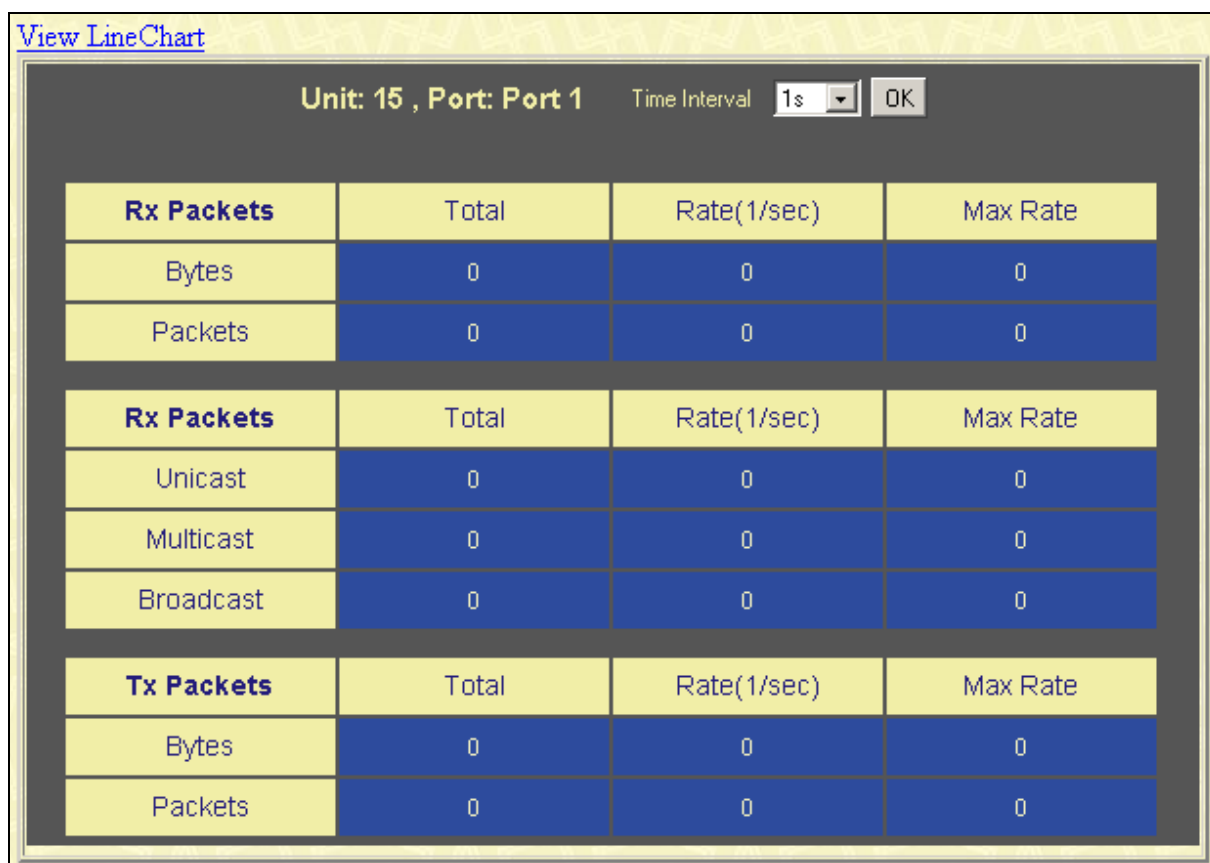
The following fields can be set:

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 8- 10. Tx Packets Analysis (line graph for Bytes & Packets) window**



**Figure 8- 11. 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

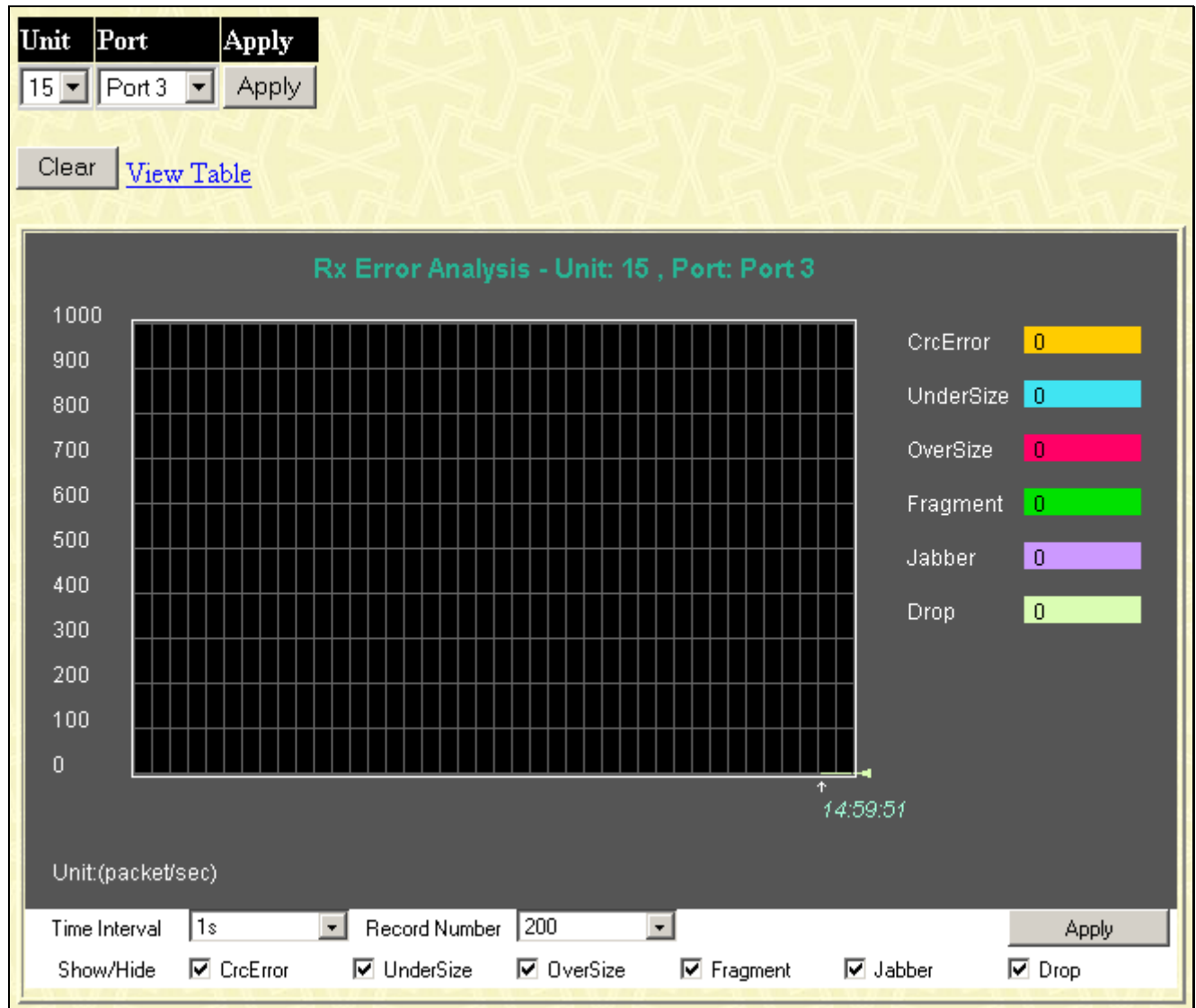
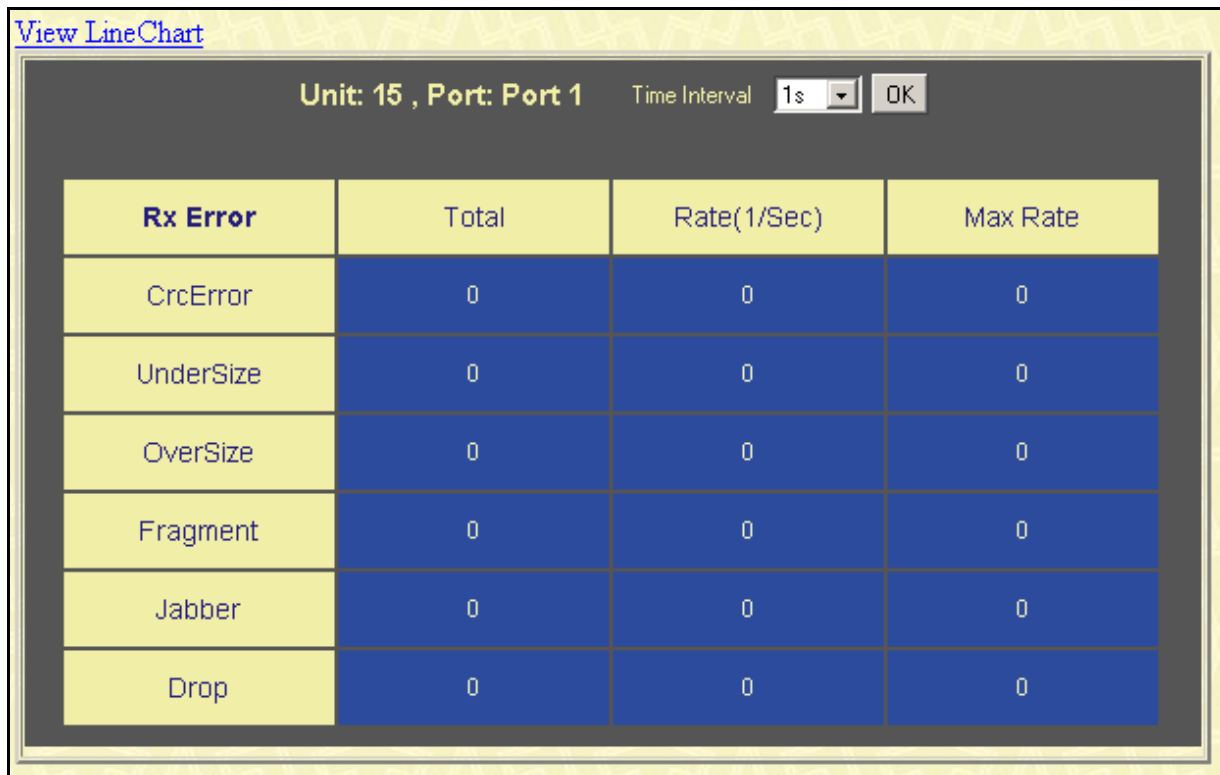


Figure 8- 12. Rx Error Analysis (line graph) window





**Figure 8- 13. Rx Error 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 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.

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

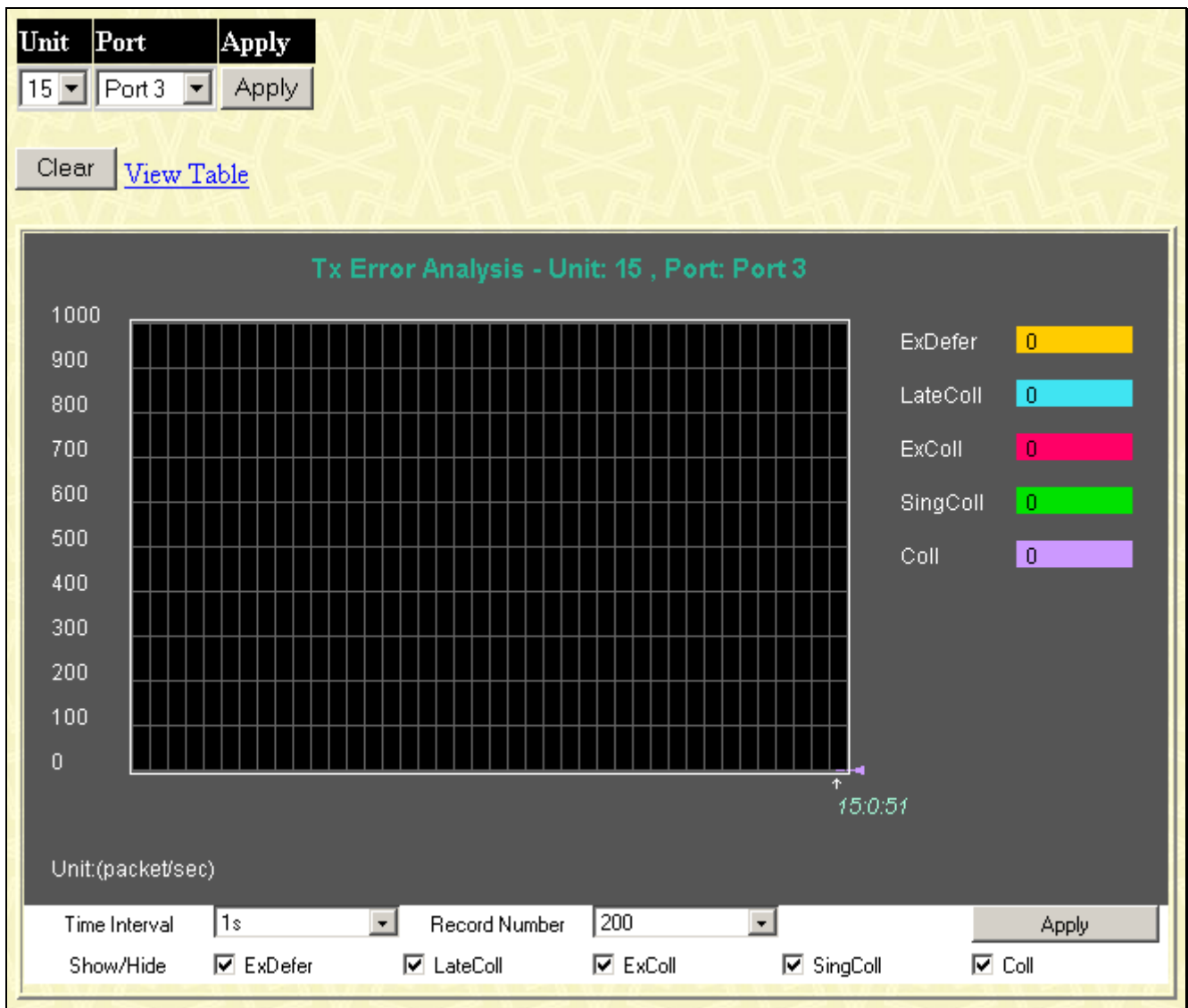
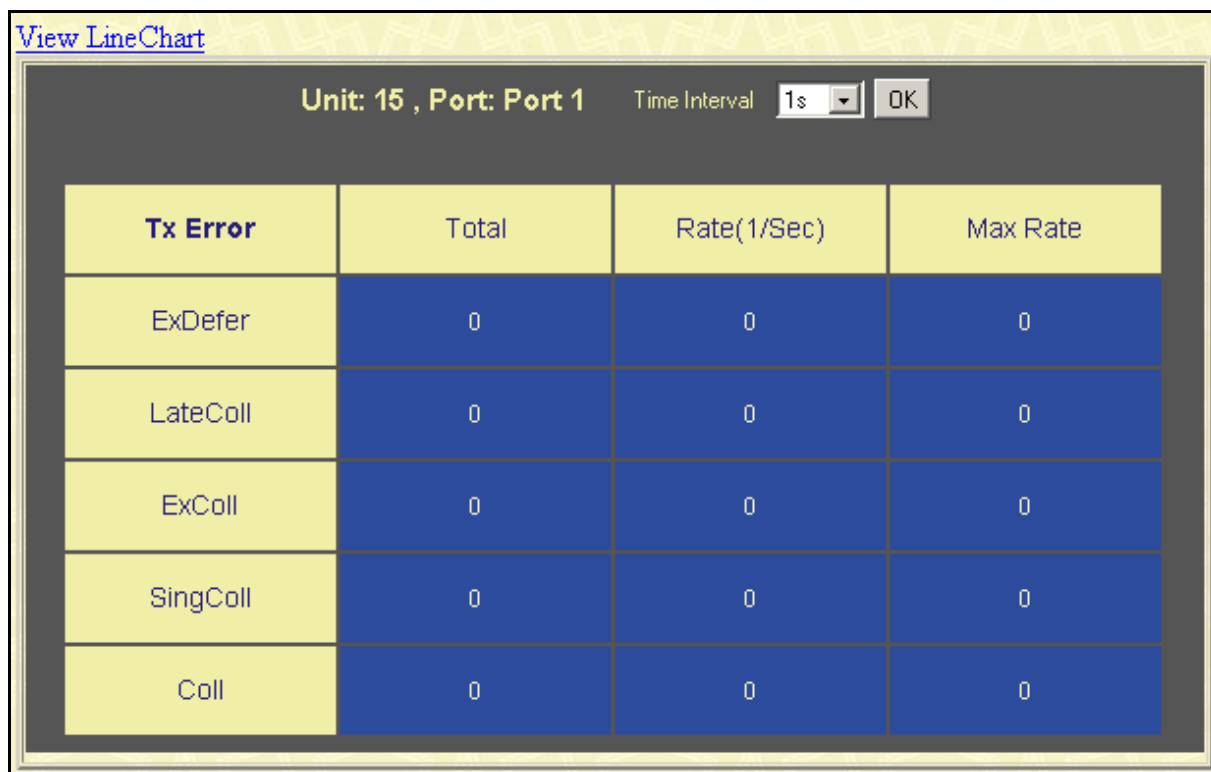


Figure 8- 14. Tx Error Analysis (line graph) window



**Figure 8- 15. Tx Error 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 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</b> (Excessive Deferral)	The number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.
<b>LateColl</b> (Late Collision)	Late Collisions. The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
<b>ExColl</b> (Excessive Collision)	Excessive Collisions. The number of frames for which transmission failed due to excessive collisions.
<b>SingColl</b> (Single Collision)	Single Collision Frames. The number of successfully transmitted frames for which transmission is inhibited by more than one collision.
<b>Coll</b> (Collision)	An estimate of the total number of collisions on this network segment.
<b>Time Interval</b> <1s>	The time between updates received from the Switch, in seconds. The default is 1s.

<b>Record Number</b> <200>	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.

## Size

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

- Packet Size

### Packet Size

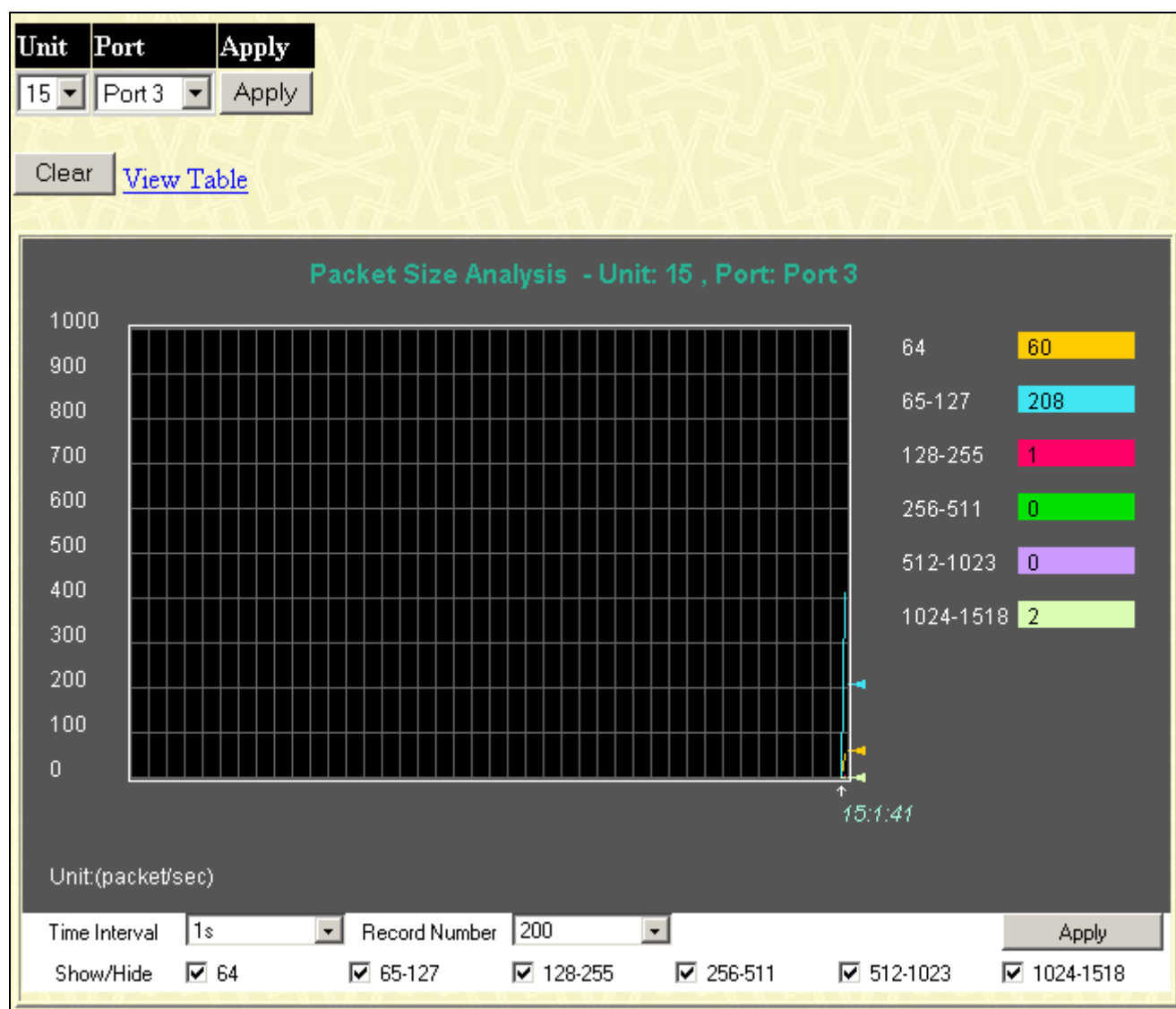
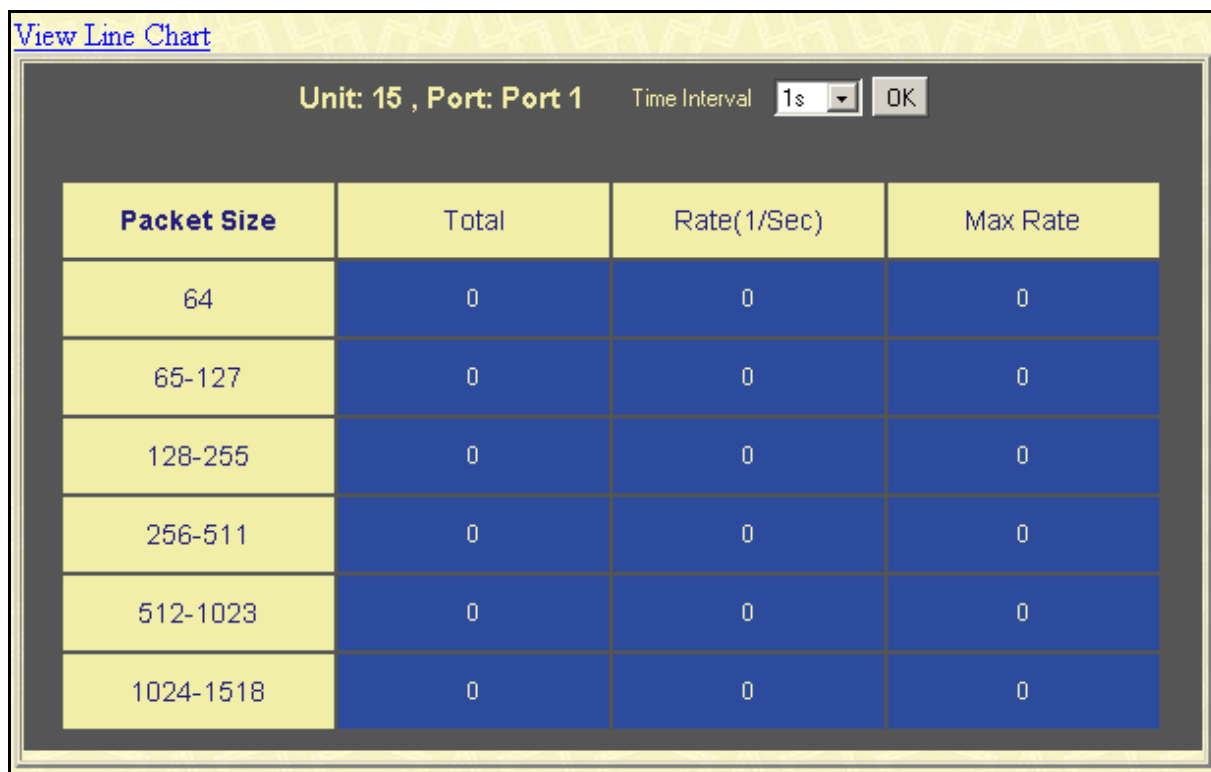


Figure 8- 16. Packet Size Analysis (line graph) window



**Figure 8- 17. 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.

<b>VLAN ID</b>	<input type="text"/>	<input type="button" value="Find"/>	<input type="button" value="Delete"/>
<b>MAC Address</b>	<input type="text" value="00-00-00-00-00-00"/>		
<b>Unit - Port</b>	<input type="text" value="15"/> <input type="text" value="Port 1"/>	<input type="button" value="Find"/>	<input type="button" value="Delete"/>
		<input type="button" value="View All Entry"/>	<input type="button" value="Delete All Entry"/>

MAC Address Table				
VID	MAC Address	Unit	Port	Learned
1	00-00-00-52-33-01	15	3	Dynamic
1	00-00-44-73-50-01	15	3	Dynamic
1	00-00-48-af-62-23	15	3	Dynamic
1	00-00-5e-00-01-5f	15	3	Dynamic
1	00-00-80-c8-09-89	15	3	Dynamic
1	00-01-24-02-45-00	15	3	Dynamic
1	00-01-30-12-13-02	15	3	Dynamic
1	00-02-06-12-34-56	15	3	Dynamic
1	00-02-3f-72-c4-eb	15	3	Dynamic
1	00-03-09-18-10-01	15	3	Dynamic
1	00-03-10-31-30-00	15	3	Dynamic
1	00-03-11-04-10-00	15	3	Dynamic
1	00-03-12-16-10-00	15	3	Dynamic
1	00-04-13-04-01-00	15	3	Dynamic
1	00-04-13-04-03-00	15	3	Dynamic
1	00-04-23-57-1d-8c	15	3	Dynamic
1	00-05-5d-00-00-0c	15	3	Dynamic
1	00-05-5d-25-28-d2	15	3	Dynamic
1	00-05-5d-7e-8f-b2	15	3	Dynamic
1	00-05-5d-ed-84-8a	15	3	Dynamic

**Total Entries: 143**

Figure 8- 18. 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
266	0 days 01:14:39	Port 15:5 link up, 1000Mbps FULL duplex
265	0 days 01:14:38	Port 15:5 link down
264	0 days 01:14:21	Port 15:5 link up, 1000Mbps FULL duplex
263	0 days 01:14:07	Port 15:5 link down
262	0 days 01:10:36	Port 15:5 link up, 1000Mbps FULL duplex
261	0 days 01:10:35	Port 15:5 link down
260	0 days 01:10:19	Port 15:5 link up, 1000Mbps FULL duplex
259	0 days 01:10:05	Port 15:5 link down
258	0 days 01:06:33	Port 15:5 link up, 1000Mbps FULL duplex
257	0 days 01:06:32	Port 15:5 link down
256	0 days 01:06:16	Port 15:5 link up, 1000Mbps FULL duplex
255	0 days 01:06:01	Port 15:5 link down
254	0 days 01:02:29	Port 15:5 link up, 1000Mbps FULL duplex
253	0 days 01:02:28	Port 15:5 link down
252	0 days 01:02:11	Port 15:5 link up, 1000Mbps FULL duplex
251	0 days 01:01:57	Port 15:5 link down
250	0 days 00:58:26	Port 15:5 link up, 1000Mbps FULL duplex
249	0 days 00:58:25	Port 15:5 link down
248	0 days 00:58:09	Port 15:5 link up, 1000Mbps FULL duplex
247	0 days 00:57:55	Port 15:5 link down
Clear		Next

**Figure 8- 19. 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 Table

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 : 0

Search

**Total Entries : 1**

IGMP Snooping Table				
VLAN ID	Multicast Group	MAC Address	Queries	Reports
0	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 8- 20. 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.

## Browser 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													▶▶▶																	

Figure 8- 21. Browse Router Port window

VLAN Status

This window displays the status of VLANs on any Switch in a Switch stack managed by a DGS-3312SR.

Total VLAN Entries: 1																													
VLAN Status																													
VLAN ID			VLAN Name										VLAN Type					Advertisement											
1			default										static					Enabled											
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	ET	E-	E-	E-	E-	ET	ET	ET	ET	E-	E-	E-	E-																
1	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-			
	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-			
2	- Non_Stacking Module -																												
3	- Non_Stacking Module -																												
4	- Non_Stacking Module -																												
5	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-			
	ET	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--			
6	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-			
	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-			
7	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-			
	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-			
8	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-			
	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-	E-			
9	- Non_Stacking Module -																												
10	- Non_Stacking Module -																												
11	- Non_Stacking Module -																												
12	- Non_Stacking Module -																												

Figure 8- 22. VLAN Status window

## Session Table

This window displays the management sessions since the Switch was last rebooted.

Reload					
Total Entries :1					
Current Session Table					
ID	Login Time	Live Time	From	Level	Name
8	00000 days 00:00:08	06:07:10.620	Serial Port	1	Anonymous

Figure 8- 23. Current Session Table window

## Layer 3 Feature

The Switch's Layer 3 monitoring windows are described below.

### Browse IP Address

The **IP Address Table** window may be found in the **Monitoring** folder in the **Layer 3 Feature** sub-folder. This window allows the user to view IP addresses discovered by the Switch. To search a specific IP address, enter it into the field labeled IP Address at the top of the screen and click **Find** to begin your search.

IP Address		<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>
IP Address Table			
Interface	IP Address	Port	Learned
System	10.0.0.3	15:3	Dynamic
System	10.0.25.77	15:3	Dynamic
System	10.1.1.7	15:3	Dynamic
System	10.1.1.101	15:3	Dynamic
System	10.1.1.102	15:3	Dynamic
System	10.1.1.103	15:3	Dynamic
System	10.1.1.151	15:3	Dynamic
System	10.1.1.152	15:3	Dynamic
System	10.1.1.154	15:3	Dynamic
System	10.1.1.157	15:3	Dynamic
System	10.1.1.161	15:3	Dynamic
System	10.1.1.162	15:3	Dynamic
System	10.1.1.163	15:3	Dynamic
System	10.1.1.164	15:3	Dynamic
System	10.1.1.166	15:3	Dynamic
System	10.1.1.167	15:3	Dynamic
System	10.1.1.168	15:3	Dynamic
System	10.1.1.169	15:3	Dynamic
System	10.1.1.170	15:3	Dynamic
System	10.1.1.171	15:3	Dynamic
Total Entries: 263			<input type="button" value="Next"/>

Figure 8- 24. IP Address window

### Browse Routing Table

The **Routing Table** window may be found in the **Monitoring** folder in the **Layer 3 Feature** sub-folder. This window shows the current IP routing table of the Switch. To find a specific IP route, enter an IP address into the **Destination Address** field along with a proper subnet mask into the **Mask** field.

Destination Address	<input type="text" value="0.0.0.0"/>	
Mask	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>

Routing Table					
IP Address	Netmask	Gateway	Interface	Cost	Protocol
10.0.0.0	255.0.0.0	0.0.0.0	System	1	Local

Total Entries: 1

Figure 8- 25. Routing Table window

## Browse ARP Table

The **ARP Table** window may be found in the **Monitoring** folder in the **Layer 3 Feature** sub-folder. This window will show current ARP entries on the Switch. To search a specific ARP entry, enter an interface name into the Interface Name or an IP address and click **Find**.

<b>Interface Name</b>	<input type="text"/>		
<b>IP Address</b>	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>	<input type="button" value="Clear All"/>

<b>ARP Table</b>			
<b>Interface Name</b>	<b>IP Address</b>	<b>Mac Address</b>	<b>Type</b>
System	10.0.0.0	ff-ff-ff-ff-ff-ff	Local/Broadcast
System	10.0.34.1	00-0c-6e-6e-14-13	Dynamic
System	10.0.46.1	00-80-c8-91-15-eb	Dynamic
System	10.0.51.12	00-50-ba-da-00-1d	Dynamic
System	10.0.58.4	00-0c-6e-43-13-ae	Dynamic
System	10.1.1.4	00-ff-7f-47-d9-42	Dynamic
System	10.1.1.7	00-00-48-af-62-23	Dynamic
System	10.1.1.100	00-80-c8-f6-f0-8d	Dynamic
System	10.1.1.101	00-50-ba-15-48-56	Dynamic
System	10.1.1.102	00-50-ba-97-d7-c0	Dynamic
System	10.1.1.103	00-50-ba-97-d7-c9	Dynamic
System	10.1.1.119	00-80-c8-50-50-11	Dynamic
System	10.1.1.151	00-50-ba-70-d6-d0	Dynamic
System	10.1.1.152	00-13-00-00-00-01	Dynamic
System	10.1.1.153	00-10-10-53-00-00	Dynamic
System	10.1.1.154	00-50-ba-97-d9-56	Dynamic
System	10.1.1.157	00-50-ba-71-20-d6	Dynamic
System	10.1.1.161	00-50-ba-70-e4-89	Dynamic
System	10.1.1.162	00-50-ba-70-e4-5a	Dynamic
System	10.1.1.163	00-50-ba-70-e4-55	Dynamic

**Total Entries: 475**

Figure 8- 26. ARP Table window

## Browse IP Multicast Forwarding Table

The **Browse IP Multicast Forwarding Table** window may be found in the **Monitoring** folder in the **Layer 3 Feature** sub-folder. This window will show current IP multicasting information on the Switch. To search a specific entry, enter an multicast group IP address into the Multicast Group field or a Source IP address and click **Find**.

<b>Multicast Group</b>	<input type="text" value="0.0.0.0"/>	<input type="text"/>
<b>Source IP</b>	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>

IP Multicast Forwarding Table					
Multicast Group	Source IP Address	Source Mask	Upstream Neighbor	Expire Time	Protocol
Total Entries: 0					

Figure 8- 27. IP Multicast Forwarding Table window

## Browse IGMP Group Table

The **IGMP Group Table** window may be found in the **Monitoring** folder in the **Layer 3 Feature** sub-folder. This window will show current IGMP group entries on the Switch. To search a specific IGMP group entry, enter an interface name into the **Interface Name** field or a **Multicast Group** IP address and click **Find**.

<b>Interface Name</b>	<input type="text"/>	<input type="text"/>
<b>Multicast Group</b>	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>

IGMP Group Table				
Interface Name	Multicast Group	Last Reporter IP	IP Querier	IP Expire
Total Entries: 0				

Figure 8- 28. IGMP Group Table window

## OSPF Monitor

This section offers windows regarding OSPF (Open Shortest Path First) information on the Switch, including the **OSPF LSDB Table**, **OSPF Neighbor Table** and the **OSPF Virtual Neighbor Table**. To view these tables, open the **Monitoring** folder, go to the **Layer 3 Feature** sub-folder, and then click **OSPF Monitor**.

### Browse OSPF LSDB Table

This table can be found in the **OSPF Monitor** folder by clicking on the **Browse OSPF LSDB Table** link. The Link-State Database table displays the current link-state database in use by the OSPF routing protocol on a per-OSPF area basis.

<b>Search Type</b>	<input type="text" value="ALL"/>	<input type="text"/>
<b>Area ID</b>	<input type="text" value="0.0.0.0"/>	<input type="text"/>
<b>Advertise Router ID</b>	<input type="text" value="0.0.0.0"/>	<input type="text"/>
<b>LSDB Type</b>	<input type="text" value="RTRLink"/>	<input type="button" value="Find"/>

OSPF LSDB Table					
Area ID	LSDB Type	Adv. Router ID	Link State ID	Cost	Sequence

Figure 8- 29. OSPF LSDB Table window

The user may search for a specific entry by entering the following information into the fields at the top of the window:

To browse the OSPF LSDB Table, you first must select which browse method you want to use. The choices are *Area ID*, *Advertise Router ID*, *LSDB*, *Area ID & Advertise Router ID*, *Area ID & LSDB*, *Advertise Router ID & LSDB*, and *ALL*.

If *Area ID* is selected as the browse method, you must enter the IP address in the Area ID field, and then click **Find**.

If *Advertise Router ID* is selected, you must enter the IP address in the Advertise Router ID field, and then click **Find**.

If *LSDB* is selected, you must select the type of link state (*RTRLink*, *NETLink*, *Summary*, *ASSummary*, and *ASExtLink*) in the LSDB Type field, and then click **Find**.

If *Area ID & Advertise Router ID* is selected as the browse method, you must enter the IP address in the Area ID field and the IP address in the Advertise Router ID field, and then click **Find**.

If *Area ID & LSDB* is selected as the browse method, you must enter the IP address in the Area ID field and select the type of link state (*RTRLink*, *NETLink*, *Summary*, *ASSummary*, and *ASExtLink*) in the LSDB Type field, and then click **Find**.

If *Advertise Router ID & LSDB* is selected as the browse method, you must enter the IP address in the Advertise Router ID field and select the type of link state (*RTRLink*, *NETLink*, *Summary*, *ASSummary*, and *ASExtLink*) in the LSDB Type field, and then click **Find**.

If *ALL* is selected, you must enter the IP address in the Area ID field and the IP address in the Advertise Router ID field and select the type of link state (*RTRLink*, *NETLink*, *Summary*, *ASSummary*, and *ASExtLink*) in the LSDB Type field, and then click **Find**.

The following fields are displayed:

Parameter	Description										
<b>Area ID</b>	Allows the entry of an OSPF Area ID. This Area ID will then be used to search the table, and display an entry – if there is one.										
<b>Search Type</b>	Select the browse method you want to use: <i>Area ID</i> , <i>Advertise Router ID</i> , <i>LSDB</i> , <i>Area ID &amp; Advertise Router ID</i> , <i>Area ID &amp; LSDB</i> , <i>Advertise Router ID &amp; LSDB</i> , or <i>ALL</i> .										
<b>LSDB Type</b>	Displays which one of eight types of link advertisements by which the current link was discovered by the switch: Router link ( <i>RTRLink</i> ), Network link ( <i>NETLink</i> ), Summary link ( <i>Summary</i> ), Autonomous System link ( <i>ASSummary</i> ), and Autonomous System external link ( <i>ASExtLink</i> ).										
<b>Adv. Router ID</b>	Displays the Advertising Router's ID.										
<b>Link State ID</b>	<p>This field identifies the portion of the Internet environment that is being described by the advertisement. The contents of this field depend on the advertisement's LS type.</p> <table> <tr> <th>LS Type</th><th>Link State ID</th></tr> <tr> <td>1</td><td>The originating router's Router ID.</td></tr> <tr> <td>2</td><td>The IP interface address of the network's Designated Router.</td></tr> <tr> <td>3</td><td>The destination network's IP address.</td></tr> <tr> <td>4</td><td>The Router ID of the described AS boundary router.</td></tr> </table>	LS Type	Link State ID	1	The originating router's Router ID.	2	The IP interface address of the network's Designated Router.	3	The destination network's IP address.	4	The Router ID of the described AS boundary router.
LS Type	Link State ID										
1	The originating router's Router ID.										
2	The IP interface address of the network's Designated Router.										
3	The destination network's IP address.										
4	The Router ID of the described AS boundary router.										
<b>Cost</b>	Displays the cost of the table entry.										
<b>Sequence</b>	Displays a sequence number corresponding to number of times the current link has been advertised as changed.										

## Browse OSPF Neighbor Table

This table can be found in the **OSPF Monitor** folder by clicking on the **Browse OSPF Neighbor Table** link. Routers that are connected to the same area or segment become neighbors in that area. Neighbors are elected via the Hello protocol. IP multicast is used to send out Hello packets to other routers on the segment. Routers become neighbors when they see



themselves listed in a Hello packet sent by another router on the same segment. In this way, two-way communication is guaranteed to be possible between any two neighbor routers. This table displays OSPF neighbors of the Switch.

Figure 8- 30. OSPF Neighbor Table window

## Browse OSPF Virtual Neighbor Table

This table can be found in the **OSPF Monitor** folder by clicking on the **Browse OSPF Virtual Neighbor Table** link. This table displays a list of Virtual OSPF neighbors of the switch. The user may choose specifically search a virtual neighbor by using one of the two search options at the top of the window:

Figure 8- 31. OSPF Virtual Neighbor Table window

Parameter	Description
<b>Transit Area ID</b>	Allows the entry of an OSPF Area ID – previously defined on the switch – that allows a remote area to communicate with the backbone (area 0). A Transit Area cannot be a Stub Area or a Backbone Area.
<b>Neighbor ID</b>	The OSPF router ID for the remote router. This IP address uniquely identifies the remote area's Area Border Router.

## DVMRP Monitor

This window allows the **DVMRP** (Distance-Vector Multicast Routing Protocol) to be monitored for each IP interface defined on the switch. This folder, found in the **Monitoring** folder, offers three windows for monitoring; **DVMRP Routing Table**, **DVMRP Neighbor Address Table** and **DVMRP Routing Next Hop Table**.

### Browse DVMRP Routing Table

Multicast routing information is gathered and stored by DVMRP in the DVMRP Routing Table, which may be found in the **Monitoring** folder, in the **Layer 3 Feature** sub-folder, under **DVMRP Monitor**, contains one row for each port in a DVMRP mode. Each routing entry contains information about the source and multicast group, and incoming and outgoing interfaces. You may define your search by entering a Source IP Address and its subnet mask into the fields at the top of the window and clicking **Browse**.

Source IP Address	<input type="text" value="0.0.0.0"/>	
Source Mask	<input type="text" value="0.0.0.0"/>	<input type="button" value="Browse"/>

DVMRP Routing Table						
Source IP Address	Source Mask	Upstream Neighbor	Metric	Learned	Interface Name	Expire
Total Entries: 0						

Figure 8- 32. DVMRP Routing Table window

## Browse DVMRP Neighbor Address Table

This table, found in the **Monitoring** folder, in the **Layer 3 Feature** sub-folder, under **DVMRP Monitor** contains information about DVMRP neighbors of the Switch. You may define your search by entering an Interface Name and Neighbor Address in the fields at the top of the window and clicking **Find**.

Interface Name	<input type="text"/>	
Neighbor Address	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>

DVMRP Neighbor Table			
Interface Name	Neighbor Address	Generation ID	Expire Time
Total Entries: 0			

Figure 8- 33. DVMRP Neighbor Table window

## Browse DVMRP Routing Next Hop Table

This table contains information regarding the next-hop for forwarding multicast packets on outgoing interfaces. Each entry in the **DVMRP Routing Next Hop Table** window refers to the next-hop of a specific source to a specific multicast group address. This table is found in the **Monitoring** window, in the **Layer 3 Feature** sub-folder, under **DVMRP Monitor**. You may define your search by entering an Interface Name and Source IP Address in the fields at the top of the window and clicking **Find**.

Interface Name	<input type="text"/>	
Source IP Address	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>

DVMRP Routing Next Hop Table			
Source IP Address	Source Mask	Interface Name	Type
Total Entries: 0			

Figure 8- 34. DVMRP Routing Next Hop Table window

## PIM Monitor

Multicast routers use Protocol Independent Multicast (PIM) to determine which other multicast routers should receive multicast packets. To find out more information concerning PIM and its configuration on the Switch, see the IP Multicasting chapter of Section 4, Configuration.

## Browse PIM Neighbor Address Table

This window contains information regarding each of a router's PIM neighbors. This window may be found in the **Monitoring** folder, in the **Layer 3 Feature** sub-folder, under the heading **PIM Monitor**. You may define your search by entering an **Interface Name** and **Neighbor Address** in the fields at the top of the window and clicking **Find**.

Interface Name	<input type="text"/>	
Neighbor Address	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>
<b>PIM Neighbor Table</b>		
Interface Name	Neighbor Address	Expire Time
Total Entries: 0		

Figure 8- 35. PIM Neighbor Table window

## Section 9

# 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 Services** folder and then the **Download Firmware** link:

Download Firmware	
Unit Number	<input checked="" type="checkbox"/> ALL 15
Server IP Address	0.0.0.0
File Name	
Start	

**Figure 9- 1. Download Firmware window**

Use the **Unit Number** 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.

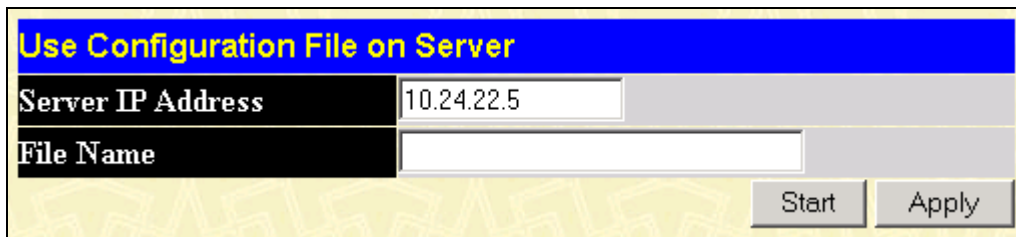
The TFTP server must be on the same IP subnet as the Switch.

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 9- 2. Use Configuration File on Server window**

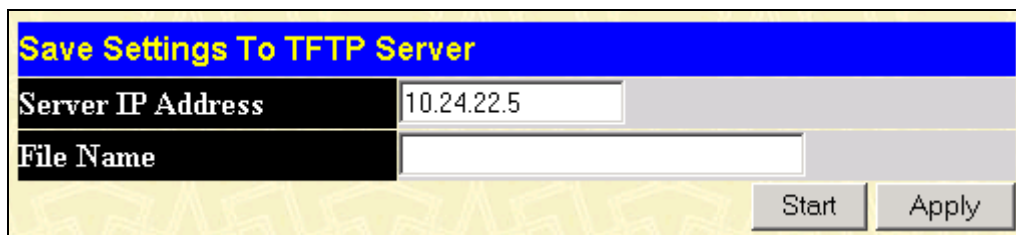
Enter the IP address of the TFTP server and specify the location of the Switch configuration file on the TFTP server.

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:



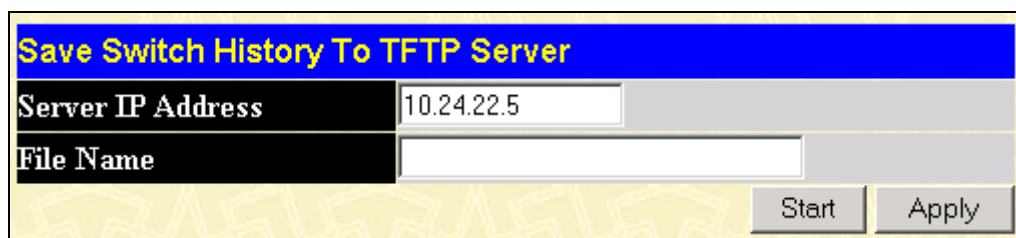
**Figure 9- 3. Save Settings To TFTP Server window**

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 9- 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.

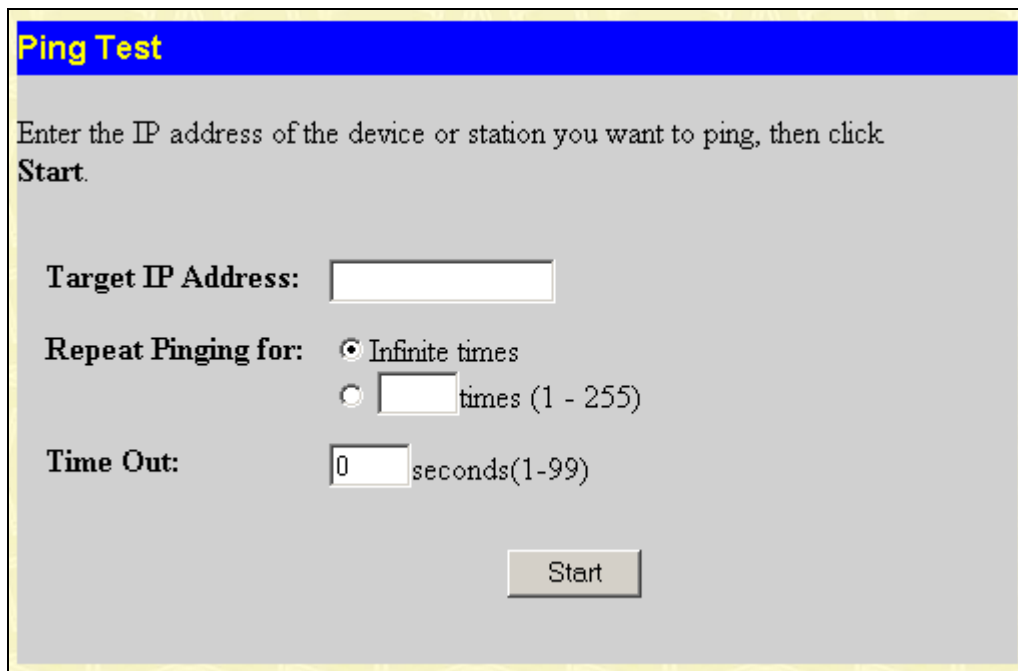
The image shows a 'Ping Test' window with a blue title bar. Below the title bar, there is a text instruction: 'Enter the IP address of the device or station you want to ping, then click Start.' The window contains three input fields: 'Target IP Address:' followed by a text box; 'Repeat Pinging for:' followed by two radio button options, 'Infinite times' (which is selected) and a text box followed by 'times (1 - 255)'; and 'Time Out:' followed by a text box containing '0' and the label 'seconds(1-99)'. At the bottom center of the window is a 'Start' button.

Figure 9- 5. Ping Test window

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

## Save Changes

The DGS-3312SR 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.

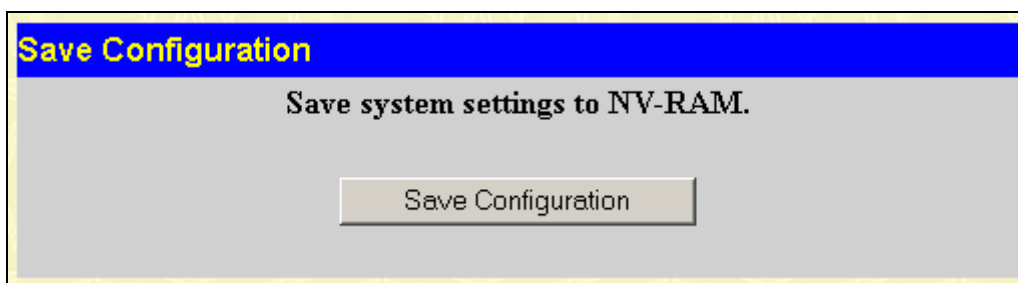
The image shows a 'Save Configuration' window with a blue title bar. Below the title bar, the text 'Save system settings to NV-RAM.' is displayed. At the bottom center of the window is a 'Save Configuration' button.

Figure 9- 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.

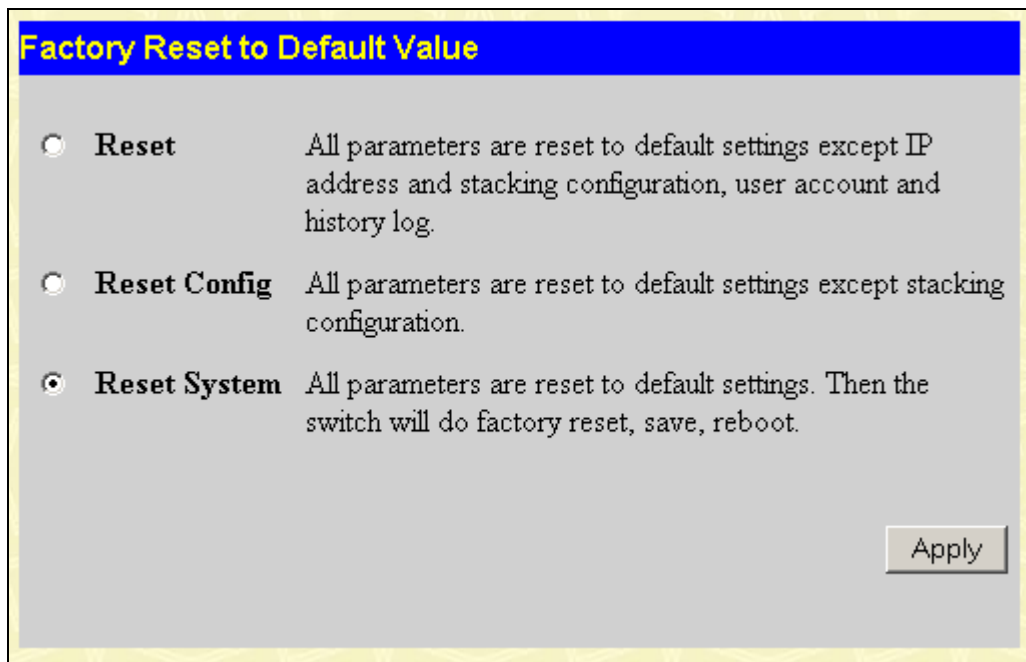


Figure 9- 7. Factory Reset to Default Value window

## 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.

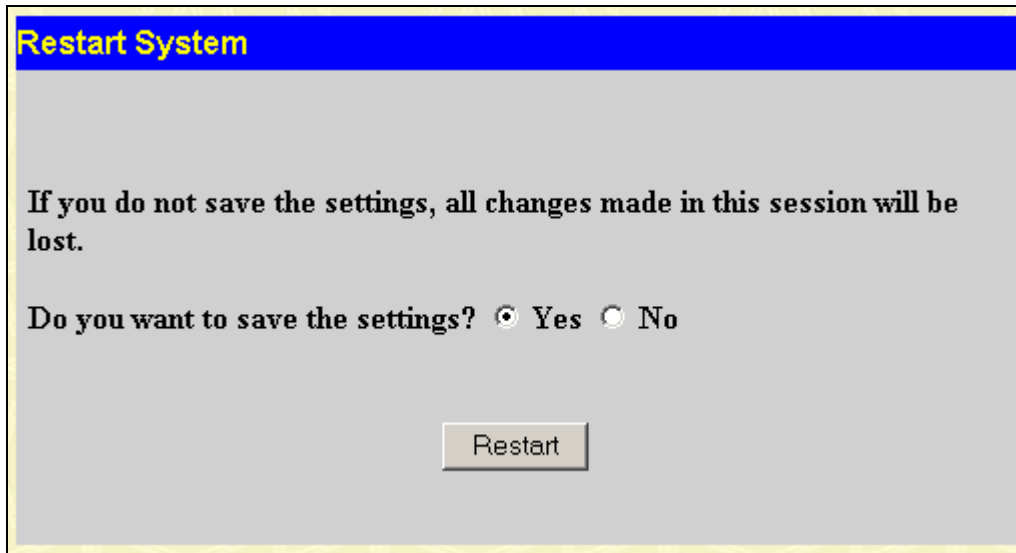


Figure 9- 8. Restart System window

## Logout

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

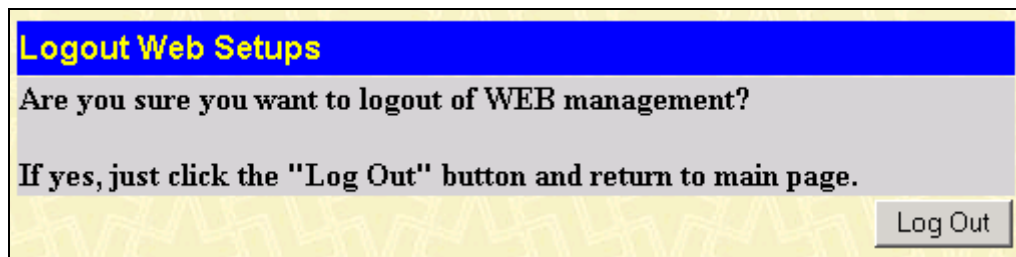


Figure 9- 9. Logout Web Setups window



## Section 10

# Single IP Management

### *SIM Settings*

### *Topology*

### *Firmware Upgrade*

### *Configuration Backup/Restore*

Simply put, Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. There are some advantages to implement “Single IP Management” feature:

1. SIM can simplify management of small workgroups or wiring closets while scaling the network to handle increased bandwidth demand.
2. SIM can reduce the number of IP address needed in your network.
3. SIM can eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technology.

Switches using Single IP Management (labeled here as SIM) must conform to the following rules:

- SIM is an optional feature on the Switch and can easily be enabled or disabled through the Command Line Interface. SIM grouping has no effect on the normal operation of the Switch in the user’s network.
- There are three classifications for switches using SIM. The Commander Switch (CS), which is the master switch of the group, Member Switch (MS), which is a switch that is recognized by the CS a member of a SIM group, and a Candidate Switch (CaS), which is a Switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.
- A SIM group can only have one Commander Switch (CS).
- All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.
- A SIM group accepts up to 32 switches (numbered 0-31), including the Commander Switch (numbered 0).
- There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.
- If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.
- SIM allows intermediate devices that do not support SIM. This enables the user to manage a switch that is more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The DGS-3312SR may take on three different roles:

- **Commander Switch (CS)** – This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:

- It has an IP Address.

- It is not a command switch or member switch of another Single IP group.

- It is connected to the member switches through its management VLAN.

- **Member Switch (MS)** – This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:

- It is not a CS or MS of another IP group.

It is connected to the CS through the CS management VLAN.

→ **Candidate Switch (CaS)** – This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group through an automatic function of the DGS-3312SR, or by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:

It is not a CS or MS of another Single IP group.

It is connected to the CS through the CS management VLAN

The following rules also apply to the above roles:

- Each device begins in a Commander state.
- CS's must change their role to CaS and then to MS, to become a MS of a SIM group. Thus the CS cannot directly be converted to a MS.
- The user can manually configure a CS to become a CaS.

A MS can become a CaS by:

- Being configured as a CaS through the CS.
- If report packets from the CS to the MS time-out.
- The user can manually configure a CaS to become a CS
- The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional DGS-3312SR switches may join the group either by an automatic method or by manually configuring the switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, and then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send it back to the administrator.

When a CS becomes a MS, it automatically becomes a member of the first SNMP community (include read/write and read only) to which the CS belongs. However if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

All DGS-3312SR switches are set as Candidate (CaS) switches, as their factory default configuration and the Single IP Management feature will be disabled. To enable SIM for the Switch using the Web interface, go to the **Single IP Management** folder and click the **SIM Settings** link, revealing the following window.

## SIM Settings



**Figure 10- 1. SIM Settings window (disabled)**

Change the SIM State to *Enabled* using the pull down menu and click **Apply**. The window will then refresh and the **SIM Settings** window will look like this:

SIM Settings	
SIM State	Enabled ▼
Role State	Commander ▼
Discovery Interval	60 (30..90 sec)
Holdtime	180 (100..255 sec)
Apply	

Figure 10- 2. SIM Settings window (enabled)

The following parameters can be set:

Parameters	Description
<b>SIM State</b>	Use the pull down menu to either enable or disable the SIM state on the Switch. <i>Disabled</i> will render all SIM functions on the Switch inoperable.
<b>Role State</b>	Use the pull down menu to change the SIM role of the Switch. The two choices are:  <i>Candidate</i> - A Candidate Switch (CaS) is not the member of a SIM group but is connected to a Commander Switch. This is the default setting for the SIM role of the DGS-3312SR.  <i>Commander</i> - Choosing this parameter will make the Switch a Commander Switch (CS). The user may join other switches to this Switch, over Ethernet, to be part of its SIM group. Choosing this option will also enable the Switch to be configured for SIM.
<b>Discovery Interval</b>	The user may set the discovery protocol interval, in seconds, that the Switch will send out discovery packets. Returning information to a Commander Switch will include information about other switches connected to it. (Ex. MS, CaS). The user may set the Discovery Interval from 30 to 90 seconds.
<b>Holdtime</b>	This parameter may be set for the time, in seconds, the Switch will hold information sent to it from other switches, utilizing the Discovery Interval. The user may set the hold time from 100 to 255 seconds.

Click **Apply** to implement the settings changed.

After enabling the Switch to be a Commander Switch (CS), the **Single IP Management** folder will then contain three added links to aid the user in configuring SIM through the web, including **Topology**, **Firmware Upgrade** and **Configuration Backup/Restore**.

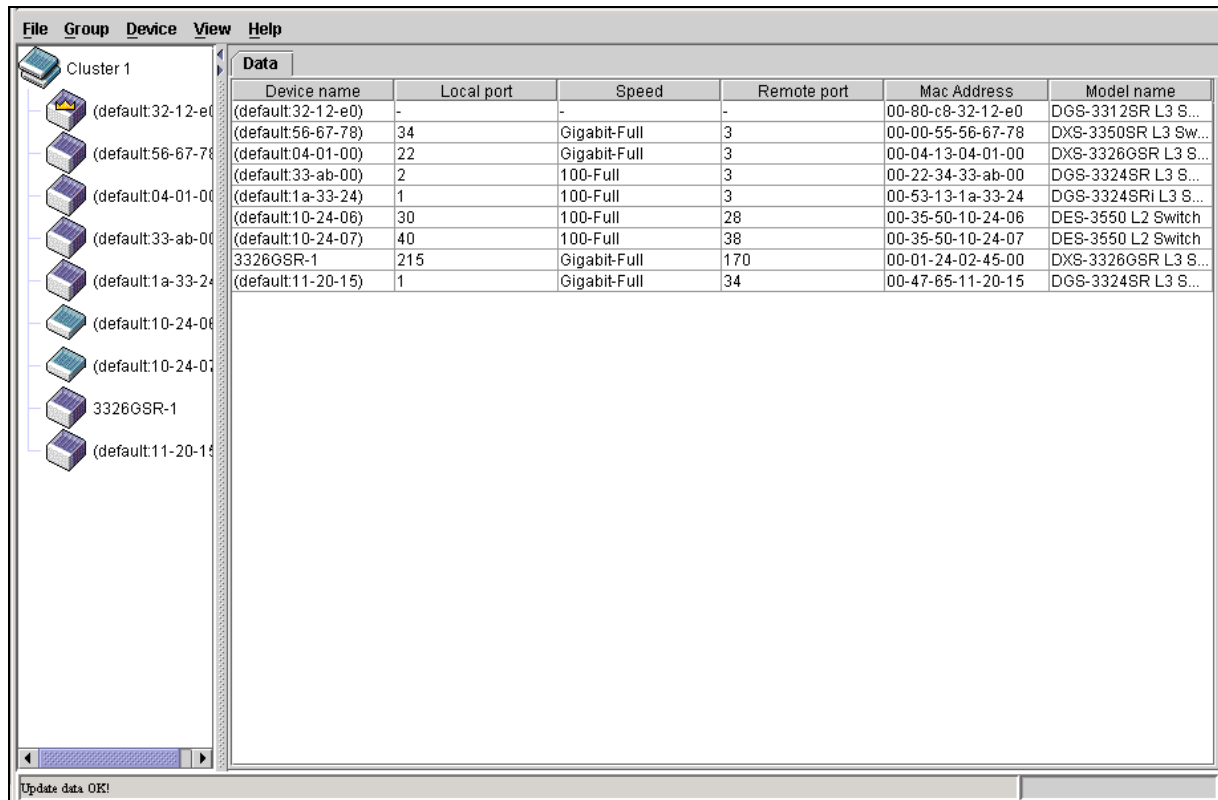
## Topology

The **Topology** window will be used to configure and manage the Switch within the SIM group and requires Java script to function properly on your computer. The following message should appear the first time the user clicks the **Topology** link in the **Single IP Management** folder.

It is necessary to setup your Java Runtime Environment to v1.4.2 to view the topology.  
Click [here](#) to link to the topology page and it will setup your  
Java Runtime Environment automatically.

Figure 10- 3. Java window

Clicking the [here](#) link will setup the Java Runtime Environment on your server and lead you to the topology window, as seen below.



**Figure 10- 4. Single IP Management window-Tree View**





The Tree View window holds the following information under the Data tab:

Parameter	Description
<b>Device Name</b>	This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
<b>Local Port</b>	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
<b>Speed</b>	Displays the connection speed between the CS and the MS or CaS.
<b>Remote Port</b>	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
<b>MAC Address</b>	Displays the MAC Address of the corresponding Switch.
<b>Model Name</b>	Displays the full Model Name of the corresponding Switch.

To view the **Topology Map**, click the **View** menu in the toolbar and then **Topology**, which will produce the following screen. The Topology View will refresh itself periodically (20 seconds by default).

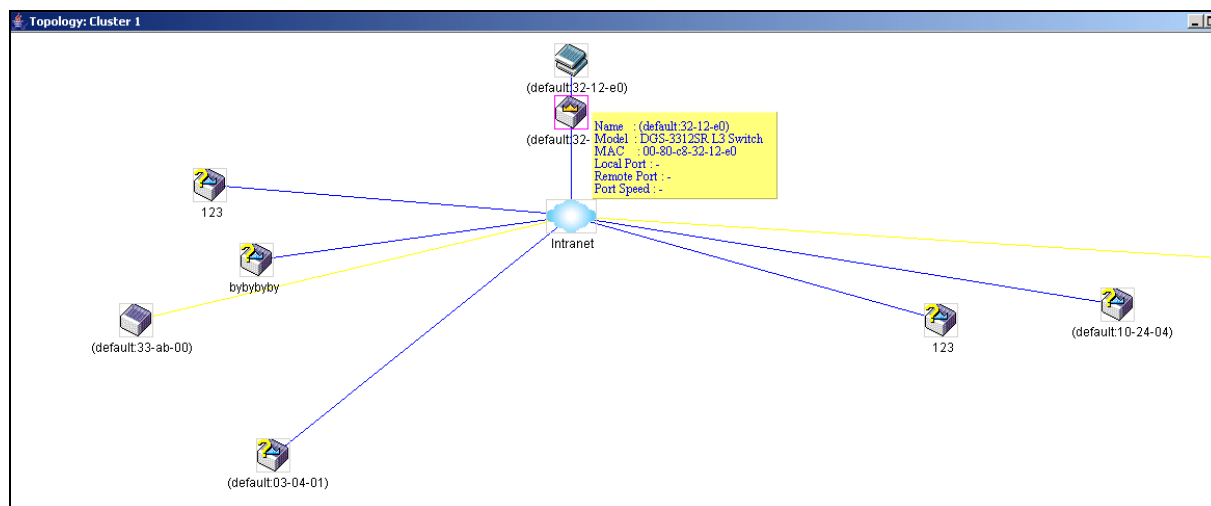
This screen will display how the devices within the Single IP Management Group are connected to other groups and devices. Possible icons in this screen are as follows:

204

	Layer 2 candidate switch
	Layer 3 candidate switch
	Unknown device
	Non-SIM devices

## Tool Tips

In the Topology view window, the mouse plays an important role in configuration and in viewing device information. Setting the mouse cursor over a specific device in the topology window (tool tip) will display the same information about a specific device as the Tree view does. See the window below for an example.



**Figure 10- 6. Device Information Utilizing the Tool Tip**

Setting the mouse cursor over a line between two devices will display the connection speed between the two devices, as shown below.

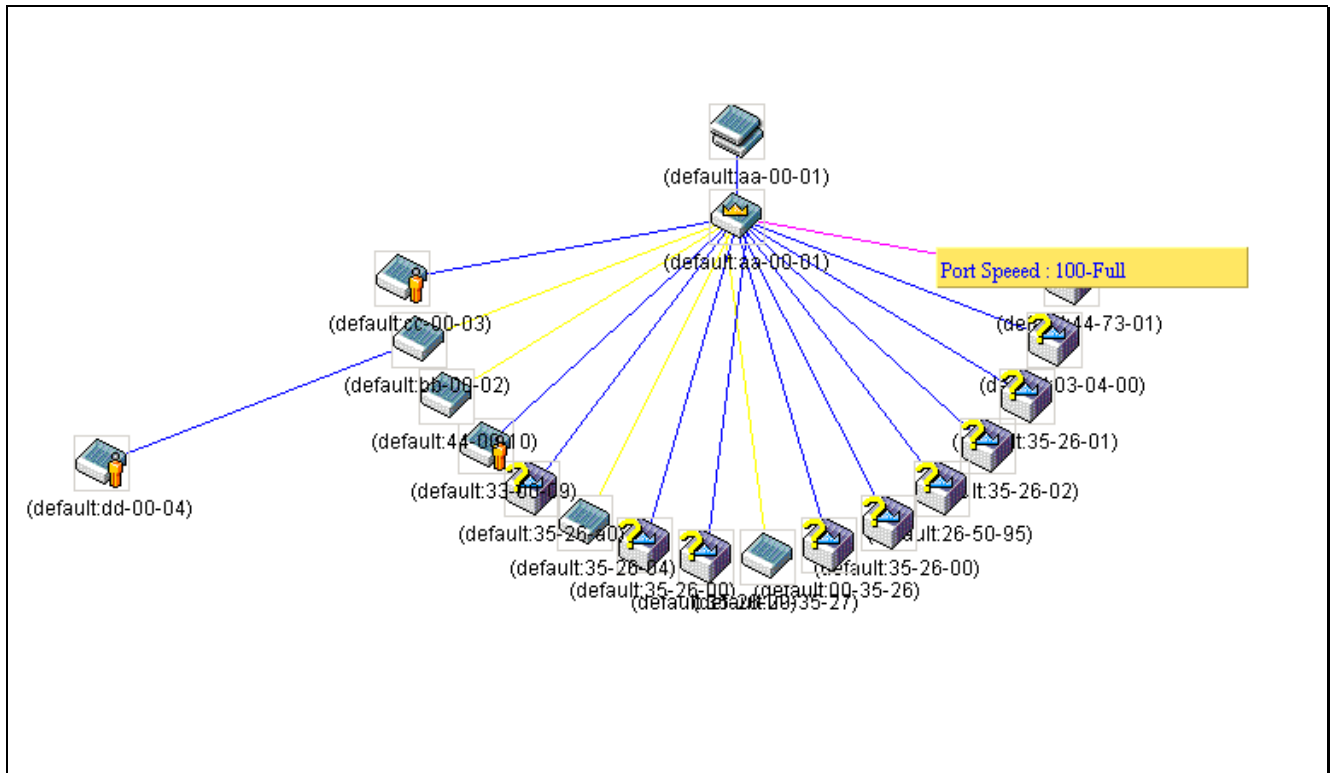


Figure 10- 7. Port Speed Utilizing the Tool Tip

## Right-click

Right clicking on a device will allow the user to perform various functions, depending on the role of the Switch in the SIM group and the icon associated with it.

## Group Icon

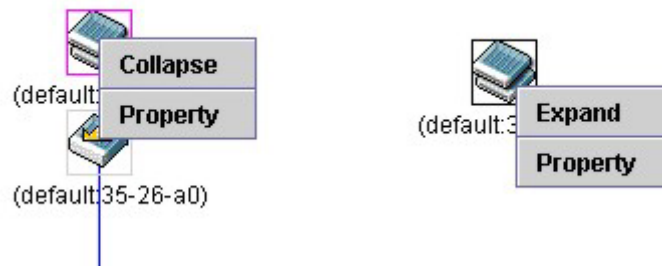


Figure 10- 8. Right-clicking a Group Icon

The following options may appear for the user to configure:

- **Collapse** - to collapse the group that will be represented by a single icon.
- **Expand** - to expand the SIM group, in detail.
- **Property** - to pop up a window to display the group information.

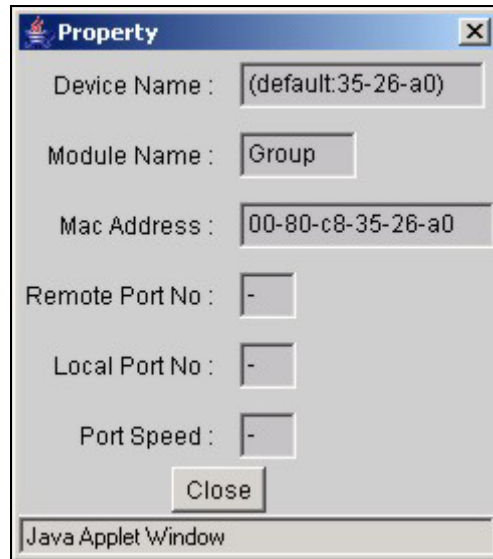


Figure 10- 9. Property dialog box

## Commander Switch Icon

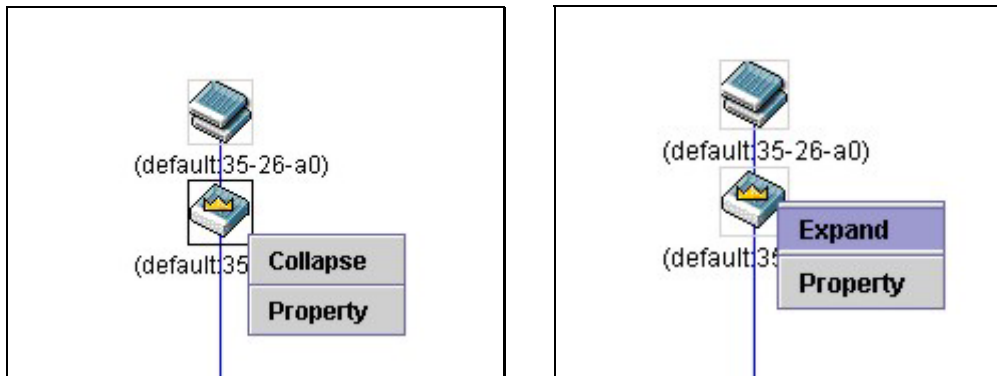


Figure 10- 10. Right-clicking a Commander Icon

The following options may appear for the user to configure:

- **Collapse** - to collapse the group that will be represented by a single icon.
- **Expand** - to expand the SIM group, in detail.
- **Property** - to pop up a window to display the group information.



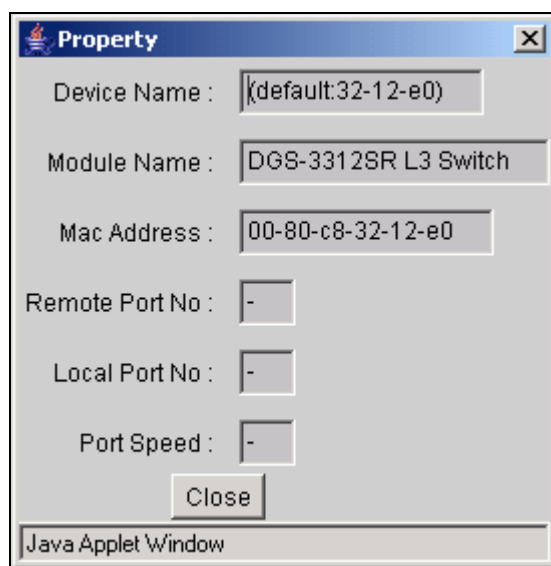


Figure 10- 11. Property dialog box

## Member Switch Icon

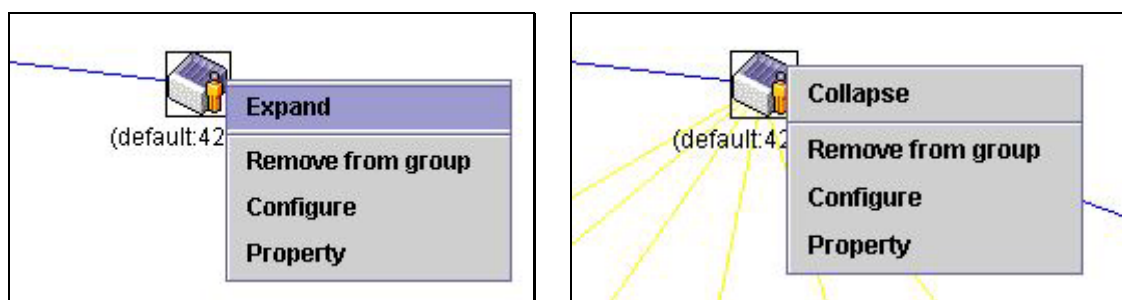


Figure 10- 12. Right-clicking a Member icon

The following options may appear for the user to configure:

- **Collapse** - to collapse the group that will be represented by a single icon.
- **Expand** - to expand the SIM group, in detail.
- **Remove from group** - remove a member from a group.
- **Configure** - launch the web management to configure the Switch.
- **Property** - to pop up a window to display the device information.

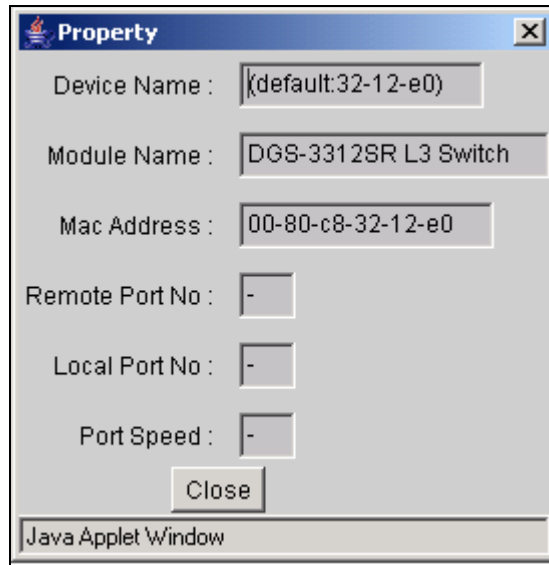


Figure 10-13. Property window

## Candidate Switch Icon

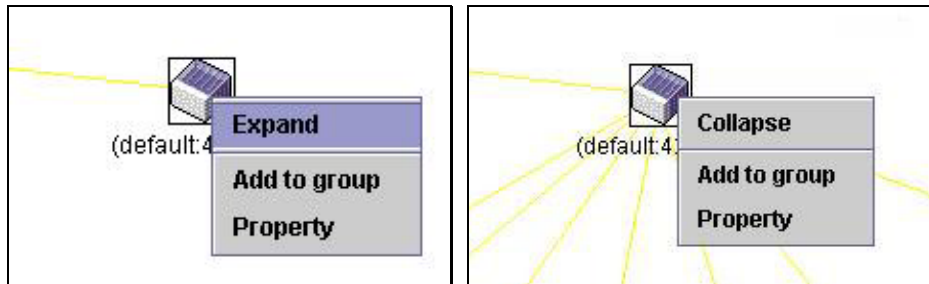


Figure 10-14. Right-clicking a Candidate icon

The following options may appear for the user to configure:

- **Collapse** - to collapse the group that will be represented by a single icon.
- **Expand** - to expand the SIM group, in detail.
- **Add to group** - add a candidate to a group. Clicking this option will reveal the following screen for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click OK to enter the password or Cancel to exit the window.

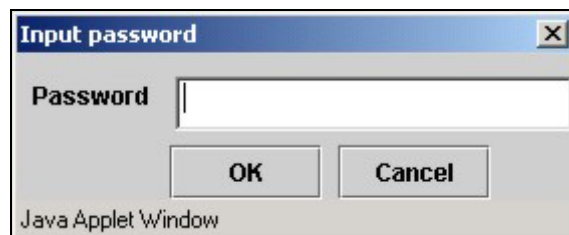
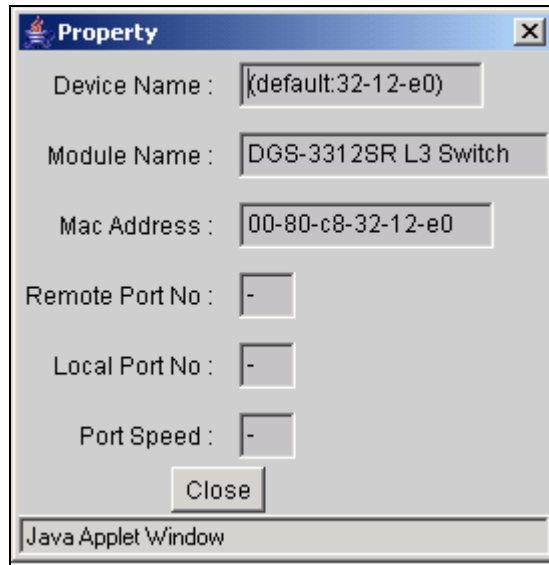


Figure 10-15. Input Password dialog box

- **Property** - to pop up a window to display the device information, as shown below.



**Figure 10- 16. Device Property dialog box**

This window holds the following information:

Parameter	Description
<b>Device Name</b>	This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
<b>Module Name</b>	Displays the full module name of the switch that was right-clicked.
<b>MAC Address</b>	Displays the MAC Address of the corresponding Switch.
<b>Remote Port No.</b>	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
<b>Local Port No.</b>	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
<b>Port Speed</b>	Displays the connection speed between the CS and the MS or CaS

Click **Close** to close the **Property** window.

## Menu Bar

The **Single IP Management** window contains a menu bar for device configurations, as seen below.



**Figure 10- 17. Menu Bar of the Topology View**

The five menus on the menu bar are as follows.

## File

- **Print Setup** - will view the image to be printed.
- **Print Topology** - will print the topology map.
- **Preference** - will set display properties, such as polling interval, and the views to open at SIM startup.

## Group

- **Add to group** - add a candidate to a group. Clicking this option will reveal the following screen for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click OK to enter the password or Cancel to exit the window.



Figure 10- 18. Input Password window

- **Remove from Group** - remove an MS from the group.

## Device

- **Configure** - will open the web manager for the specific device.

## View

- **Refresh** - update the views with the latest status.
- **Topology** - display the Topology view.

## Help

- **About** - Will display the SIM information, including the current SIM version.



Figure 10- 19. About window



**NOTE:** Upon this firmware release, some functions of the SIM can only be configured through the Command Line Interface. See the ***DGS-3312SR Command Line Interface Reference Manual*** for more information on SIM and its configurations.

## Firmware Upgrade

This screen is used to upgrade firmware from the Commander Switch to the Member Switch. Member Switches will be listed in the table and will be specified by Port (port on the CS where the MS resides), MAC Address, Model Name and Version. To specify a certain Switch for firmware download, click its corresponding check box under the Port heading. To update the firmware, enter the Server IP Address where the firmware resides and enter the Path/File name of the firmware. Click **Download** to initiate the file transfer.

Firmware Upgrade			
Port	Mac Address	Model Name	Version
<div>Server IP Address</div> <div>0 0 0 0</div>			
<div>Path \ Filename</div> <div></div>			
<div>Download</div>			

Figure 10- 20. Firmware Upgrade window

## Configuration File Backup/Restore

This screen is used to upgrade configuration files from the Commander Switch to the Member Switch. Member Switches will be listed in the table and will be specified by Port (port on the CS where the MS resides), MAC Address, Model Name and Version. To specify a certain Switch for upgrading configuration files, click its corresponding radio button under the Port heading. To update the configuration file, enter the Server IP Address where the firmware resides and enter the Path/Filename of the firmware. Click **Download** to initiate the file transfer.

Configuration File Backup/Restore			
Port	Mac Address	Model Name	Version
<div>Server IP Address</div> <div>0 0 0 0</div>			
<div>Path \ Filename</div> <div></div>			
<div>Upload</div> <div>Download</div>			

Figure 10- 21. Configuration File Backup/Restore 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



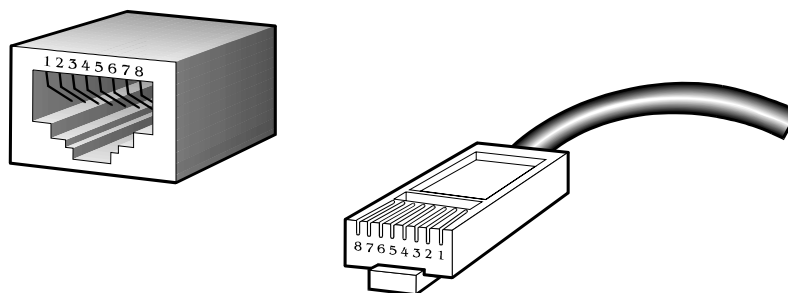


## Appendix B

### Cables and Connectors

When connecting the Switch to another switch, a bridge or hub, a normal cable is necessary. Please review these products for matching cable pin assignment.

The following diagrams and tables show the standard RJ-45 receptacle/connector and their pin assignments.



**Figure B- 1. The standard RJ-45 port and connector**

RJ-45 Pin Assignments		
Contact	MDI-X Port	MDI-II Port
1	RD+ (receive)	TD+ (transmit)
2	RD- (receive)	TD- (transmit)
3	TD+ (transmit)	RD+ (receive)
4	Not used	Not used
5	Not used	Not used
6	TD- (transmit)	RD- (receive)
7	Not used	Not used
8	Not used	Not used

**Figure B- 2. The standard RJ-45 pin assignments**

## Appendix C

### Cable Lengths

Use the following table to as a guide for the maximum cable lengths.

Standard	Media Type	Maximum Distance
Mini-GBIC	1000BASE-LX, Single-mode fiber module	10km
	1000BASE-SX, Multi-mode fiber module	550m
	1000BASE-LHX, Single-mode fiber module	40km
	1000BASE-ZX, Single-mode fiber module	80km
1000BASE-T	Category 5e UTP Cable	100m
	Category 5 UTP Cable (1000 Mbps)	
100BASE-TX	Category 5 UTP Cable (100 Mbps)	100m
10BASE-T	Category 3 UTP Cable (10 Mbps)	100m

# Glossary

---

**1000BASE-LX:** A short laser wavelength on multimode fiber optic cable for a maximum length of 550 meters

**1000BASE-SX:** A long wavelength for a "long haul" fiber optic cable for a maximum length of 10 kilometers

**100BASE-FX:** 100Mbps Ethernet implementation over fiber.

**100BASE-TX:** 100Mbps Ethernet implementation over Category 5 and Type 1 Twisted Pair cabling.

**10BASE-T:** The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.

**ageing:** The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.

**ATM:** Asynchronous Transfer Mode. A connection oriented transmission protocol based on fixed length cells (packets). ATM is designed to carry a complete range of user traffic, including voice, data and video signals.

**auto-negotiation:** A feature on a port which allows it to advertise its capabilities for speed, duplex and flow control. When connected to an end station that also supports auto-negotiation, the link can self-detect its optimum operating setup.

**backbone port:** A port which does not learn device addresses, and which receives all frames with an unknown address. Backbone ports are normally used to connect the Switch to the backbone of your network. Note that backbone ports were formerly known as designated downlink ports.

**backbone:** The part of a network used as the primary path for transporting traffic between network segments.

**bandwidth:** Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10Mbps, the bandwidth of Fast Ethernet is 100Mbps.

**baud rate:** The switching speed of a line. Also known as line speed between network segments.

**BOOTP:** The BOOTP protocol allows you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.

**bridge:** A device that interconnects local or remote networks no matter what higher level protocols are involved. Bridges form a single logical network, centralizing network administration.

**broadcast:** A message sent to all destination devices on the network.

**broadcast storm:** Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.

**console port:** The port on the Switch accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.

**CSMA/CD:** Channel access method used by Ethernet and IEEE 802.3 standards in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.

**data center switching:** The point of aggregation within a corporate network where a switch provides high-performance access to server farms, a high-speed backbone connection and a control point for network management and security.

**Ethernet:** A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.

**Fast Ethernet:** 100Mbps technology based on the Ethernet/CD network access method.

**Flow Control:** (IEEE 802.3z) A means of holding packets back at the transmit port of the connected end station. Prevents packet loss at a congested switch port.

**forwarding:** The process of sending a packet toward its destination by an internetworking device.

**full duplex:** A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

**half duplex:** A system that allows packets to be transmitted and received, but not at the same time. Contrast with full duplex.

**IP address:** Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.

**IPX:** Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.

**LAN - Local Area Network:** A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.

**latency:** The delay between the time a device receives a packet and the time the packet is forwarded out of the destination port.

**line speed:** See baud rate.

**main port:** The port in a resilient link that carries data traffic in normal operating conditions.

**MDI - Medium Dependent Interface:** An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.

**MDI-X - Medium Dependent Interface Cross-over:** An Ethernet port connection where the internal transmit and receive lines are crossed.

**MIB - Management Information Base:** Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.

**multicast:** Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.

**protocol:** A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

**resilient link:** A pair of ports that can be configured so that one will take over data transmission should the other fail. See also main port and standby port.

**RJ-45:** Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.

**RMON:** Remote Monitoring. A subset of SNMP MIB II that allows monitoring and management capabilities by addressing up to ten different groups of information.

**RPS - Redundant Power System:** A device that provides a backup source of power when connected to the Switch.

**server farm:** A cluster of servers in a centralized location serving a large user population.

**SLIP - Serial Line Internet Protocol:** A protocol which allows IP to run over a serial line connection.

**SNMP - Simple Network Management Protocol:** A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and end station operation.

**Spanning Tree Protocol (STP):** A bridge-based system for providing fault tolerance on networks. STP works by allowing you to implement parallel paths for network traffic, and ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.

**stack:** A group of network devices that are integrated to form a single logical device.

**standby port:** The port in a resilient link that will take over data transmission if the main port in the link fails.

**switch:** A device which filters, forwards and floods packets based on the packet's destination address. The switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.

**TCP/IP:** A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

**telnet:** A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.

**TFTP - Trivial File Transfer Protocol:** Allows you to transfer files (such as software upgrades) from a remote device using your switch's local management capabilities.

**UDP - User Datagram Protocol:** An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.

**VLAN - Virtual LAN:** A group of location- and topology-independent devices that communicate as if they are on a common physical LAN.

**VLT - Virtual LAN Trunk:** A Switch-to-Switch link which carries traffic for all the VLANs on each Switch.

**VT100:** A type of terminal that uses ASCII characters. VT100 screens have a text-based appearance.

**Australia****D-Link Australasia**

1 Giffnock Avenue, North Ryde, NSW 2113, Sydney, Australia

TEL: 61-2-8899-1800 FAX: 61-2-8899-1868

URL: [www.dlink.com.au](http://www.dlink.com.au)

**Belgium****D-Link Belgium**

Rue des Colonies 11, B-1000 Brussels, Belgium

TEL: 32 (0)2 517 7111 FAX: 32 (0)2 517 6500

URL: [www.dlink-benelux.com](http://www.dlink-benelux.com)

**Brazil****D-Link Brasil Ltda.**

Av das Nações Unidas, 11857, cj 132 - Brooklin Novo, São Paulo, Brasil 04578-000

TEL: (55 11) 5503-9320 FAX: (55 11) 5503-9321

URL: [www.dlink.com.br](http://www.dlink.com.br)

**Canada****D-Link Canada**

2180 Winston Park Drive, Oakville, Ontario, L6H 5W1 Canada

TEL: 1-905-829-5033 FAX: 1-905-829-5223

URL: [www.dlink.ca](http://www.dlink.ca)

**Chile****D-Link South America (Sudamérica)**

Isidora Goyenechea 2934 Oficina 702

Las Condes Fono 2323185, Santiago, Chile

TEL: 56-2-232-3185 FAX: 56-2-232-0923

URL: [www.dlink.cl](http://www.dlink.cl)

**China****D-Link China**

Room 507/508, Tower W1, The Towers, Oriental Plaza No. 1

East Chang An Ave., Dong Cheng District, Beijing, 100738, China

TEL: (86-010) 85182533 FAX: (86-010) 85182250

URL: [www.dlink.com.cn](http://www.dlink.com.cn)

**Denmark****D-Link Denmark**

Naverland 2, DK-2600 Glostrup, Denmark

TEL: 45-43-96-90-40 FAX: 45-43-42-43-47

URL: [www.dlink.dk](http://www.dlink.dk)

**Egypt****D-Link Egypt**

19 El-Shahed Helmy, El Masry, Al-Maza, Heliopolis, Cairo, Egypt

TEL: 202-41-44-295 FAX: 202-41-56-704

URL: [www.dlink-me.com](http://www.dlink-me.com)

<b>Finland</b>	<b>D-Link Finland</b> Pakkalankuja 7A, 3 <sup>rd</sup> floor, 01510 Vantaa, Finland TEL: 358-9-2707-5080 FAX: 358-9-2707-5081 URL: <a href="http://www.dlink.fi">www.dlink.fi</a>
<b>France</b>	<b>D-Link France</b> Le Florilege, No. 2, Allée de la Fresnerie, 78330 Fontenay le Fleury, France TEL: 33-1-3023-8688 FAX: 33-1-3023-8689 URL: <a href="http://www.dlink-france.fr">www.dlink-france.fr</a>
<b>Germany</b>	<b>D-Link Central Europe (D-Link Deutschland GmbH)</b> Schwalbacher Strasse 74, D-65760 Eschborn, Germany TEL: 49-6196-77990 FAX: 49-6196-7799300 URL: <a href="http://www.dlink.de">www.dlink.de</a>
<b>India</b>	<b>D-Link India</b> D-Link House, Kurla-Bandra Complex Rd., Off Cst Rd., Santacruz (East), Mumbai, 400 098 India TEL: 91-022-652-6696/6578/6623 FAX: 91-022-652-8914/8476 URL: <a href="http://www.dlink.co.in">www.dlink.co.in</a> & <a href="http://www.dlink-india.com">www.dlink-india.com</a>
<b>Israel</b>	<b>D-Link Israel</b> 11 Hamanofim Street, Ackerstein Towers, Regus Business Center P.O.B. 2148, Hertzelia-Pituach 46120, Israel TEL: 972-9-9715700 FAX: 972-9-9715601 URL: <a href="http://www.dlink.co.il">www.dlink.co.il</a>
<b>Italy</b>	<b>D-Link Mediterraneo Srl/D-Link Italia</b> Via Nino Bonnet n. 6/B, 20154, Milano, Italy TEL: 39-02-2900-0676 FAX: 39-02-2900-1723 URL: <a href="http://www.dlink.it">www.dlink.it</a>
<b>Netherlands</b>	<b>D-Link Netherlands</b> Weena 290, 3012 NJ Rotterdam, The Netherlands TEL: 31 (0)10 282 1445 FAX: 31 (0)10 282 1331 URL: <a href="http://www.dlink-benelux.com">www.dlink-benelux.com</a>
<b>Norway</b>	<b>D-Link Norway</b> Karihaugveien 89, N-1086 Oslo TEL: 47-23-89-71-89 FAX: 47-22-30-90-85 URL: <a href="http://www.dlink.no">www.dlink.no</a>

<b>Russia</b>	<b>D-Link Russia</b> Grafsky per., 14, floor 6, Moscow 129626 Russia TEL: 7 (095) 744-0099 FAX: 7 (095) 744-0099 #350 URL: <a href="http://www.dlink.ru">www.dlink.ru</a>
<b>Singapore</b>	<b>D-Link International</b> 1 International Business Park, #03-12 The Synergy, Singapore 609917 TEL: 65-6774-6233 FAX: 65-6774-6322 URL: <a href="http://www.dlink-intl.com">www.dlink-intl.com</a>
<b>South Africa</b>	<b>D-Link South Africa</b> Einstein Park II, Block B, 102-106 Witch-Hazel Avenue Highveld Technopark, Centurion, Gauteng, Republic of South Africa TEL: 27-12-665-2165 FAX: 27-12-665-2186 URL: <a href="http://www.d-link.co.za">www.d-link.co.za</a>
<b>Spain</b>	<b>D-Link Iberia</b> C/Sabino de Arana, 56 Bajos, 08028 Barcelona, Spain TEL: 34 93 409 0770 FAX: 34 93 491 0795 URL: <a href="http://www.dlink.es">www.dlink.es</a>
<b>Sweden</b>	<b>D-Link Sweden</b> P. O. Box 15036, S-167 15 Bromma, Sweden TEL: 46-(0)8564-61900 FAX: 46-(0)8564-61901 URL: <a href="http://www.dlink.se">www.dlink.se</a>
<b>Taiwan</b>	<b>D-Link Taiwan</b> 2F, No. 119, Pao-chung Road, Hsin-tien, Taipei, Taiwan TEL: 886-2-2910-2626 FAX: 886-2-2910-1515 URL: <a href="http://www.dlinktw.com.tw">www.dlinktw.com.tw</a>
<b>Turkey</b>	<b>D-Link Turkey</b> Regus Offices Beybi Giz Plaza, Ayazaga Mah. Meydan Sok. No. 28 Maslak 34396, Istanbul-Turkiye TEL: 90-212-335-2553 FAX: 90-212-335-2500 URL: <a href="http://www.dlink.com.tr">www.dlink.com.tr</a>
<b>U.A.E.</b>	<b>D-Link Middle East</b> P.O. Box 500376, Office No. 103, Building 3 Dubai Internet City, Dubai, United Arab Emirates TEL: 971-4-3916480 FAX: 971-4-3908881 URL: <a href="http://www.dlink-me.com">www.dlink-me.com</a>



**U.K.****D-Link Europe (United Kingdom)**

4<sup>th</sup> Floor, Merit House, Edgware Road, Colindale, London

NW9 5AB United Kingdom

TEL: 44-020-8731-5555 FAX: 44-020-8731-5511

URL: [www.dlink.co.uk](http://www.dlink.co.uk)

**U.S.A.****D-Link Systems, Inc.**

17595 Mt. Herrmann, Fountain Valley, CA 92708, USA

TEL: 1-714-885-6000 FAX: 1-866-743-4905

URL: [www.dlink.com](http://www.dlink.com)

## WARRANTIES EXCLUSIVE

IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS

D-LINK SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY THE CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

## LIMITATION OF LIABILITY

IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF A D- LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

IF YOU PURCHASED A D-LINK PRODUCT IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

## Limited Warranty

### Hardware:

D-Link warrants each of its hardware products to be free from defects in workmanship and materials under normal use and service for a period commencing on the date of purchase from D-Link or its Authorized Reseller and extending for the length of time stipulated by the Authorized Reseller or D-Link Branch Office nearest to the place of purchase.

This Warranty applies on the condition that the product Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card.

If the product proves defective within the applicable warranty period, D-Link will provide repair or replacement of the product. D-Link shall have the sole discretion whether to repair or replace, and replacement product may be new or reconditioned. Replacement product shall be of equivalent or better specifications, relative to the defective product, but need not be identical. Any product or part repaired by D-Link pursuant to this warranty shall have a warranty period of not less than 90 days, from date of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.

Warranty service may be obtained by contacting a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing/shipping/insurance prepaid. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.

Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

## **Software:**

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system/platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system/platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.

## **D-Link Offices for Registration and Warranty Service**

The product's Registration Card, provided at the back of this manual, must be sent to a D-Link office. To obtain an RMA number for warranty service as to a hardware product, or to obtain warranty service as to a software product, contact the D-Link office nearest you. An address/telephone/fax/e-mail/Web site list of D-Link offices is provided in the back of this manual.



## Limited Warranty (USA Only)

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited warranty for its product only to the person or entity that originally purchased the product from:

- D-Link or its authorized reseller or distributor and
- Products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, addresses with an APO or FPO.

**Limited Warranty:** D-Link warrants that the hardware portion of the D-Link products described below will be free from material defects in workmanship and materials from the date of original retail purchase of the product, for the period set forth below applicable to the product type ("Warranty Period"), except as otherwise stated herein.

Limited Lifetime Warranty for the Product(s) is defined as follows:

- Hardware for as long as the original customer/end user owns the product, or five years after product discontinuance, whichever occurs first (excluding power supplies and fans)
- Power Supplies and Fans Three (3) Year
- Spare parts and spare kits Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund at D-Link's sole discretion. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or have an identical make, model or part. D-Link may in its sole discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement Hardware will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

**Limited Software Warranty:** D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund at D-Link's sole discretion. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Software will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

**Non-Applicability of Warranty:** The Limited Warranty provided hereunder for hardware and software of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

**Submitting A Claim:** The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.

The original product owner must obtain a Return Material Authorization ("RMA") number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the Product and will not ship back any accessories.

The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrman Street, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are

lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

**What Is Not Covered:** This limited warranty provided by D-Link does not cover: Products, if in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. Repair by anyone other than D-Link or an Authorized D-Link Service Office will void this Warranty.

**Disclaimer of Other Warranties:** EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

**Limitation of Liability:** TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY

**Governing Law:** This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

**Trademarks:** D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective manufacturers or owners.

**Copyright Statement:** No part of this publication or documentation accompanying this Product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976. Contents are subject to change without prior notice. Copyright© 2002 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

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

**FCC Statement:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

For detailed warranty outside the United States, please contact corresponding local D-Link office.

***Register online your D-Link product at  
<http://support.dlink.com/register/>***

## Registration Card

**Print, type or use block letters.**

Your name: Mr./Ms \_\_\_\_\_  
 Organization: \_\_\_\_\_ Dept. \_\_\_\_\_  
 Your title at organization: \_\_\_\_\_  
 Telephone: \_\_\_\_\_ Fax: \_\_\_\_\_  
 Organization's full address: \_\_\_\_\_

Country: \_\_\_\_\_  
 Date of purchase (Month/Day/Year): \_\_\_\_\_

Product Model	Product Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(\* Applies to adapters only)

**Product was purchased from:**

Reseller's name: \_\_\_\_\_  
 Telephone: \_\_\_\_\_ Fax: \_\_\_\_\_  
 Reseller's full address: \_\_\_\_\_

**Answers to the following questions help us to support your product:**

**1. Where and how will the product primarily be used?**

☐Home ☐Office ☐Travel ☐Company Business ☐Home Business ☐Personal Use

**2. How many employees work at installation site?**

☐1 employee ☐2-9 ☐10-49 ☐50-99 ☐100-499 ☐500-999 ☐1000 or more

**3. What network protocol(s) does your organization use ?**

☐XNS/IPX ☐TCP/IP ☐DECnet ☐Others \_\_\_\_\_

**4. What network operating system(s) does your organization use ?**

☐D-Link LANsmart ☐Novell NetWare ☐NetWare Lite ☐SCO Unix/Xenix ☐PC NFS ☐3Com 3+Open  
☐Banyan Vines ☐DECnet Pathwork ☐Windows NT ☐Windows NTAS ☐Windows '95  
☐Others \_\_\_\_\_

**5. What network management program does your organization use ?**

☐D-View ☐HP OpenView/Windows ☐HP OpenView/Unix ☐SunNet Manager ☐Novell NMS  
☐NetView 6000 ☐Others \_\_\_\_\_

**6. What network medium/media does your organization use ?**

☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP  
☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others \_\_\_\_\_

**7. What applications are used on your network?**

☐Desktop publishing ☐Spreadsheet ☐Word processing ☐CAD/CAM  
☐Database management ☐Accounting ☐Others \_\_\_\_\_

**8. What category best describes your company?**

☐Aerospace ☐Engineering ☐Education ☐Finance ☐Hospital ☐Legal ☐Insurance/Real Estate ☐Manufacturing  
☐Retail/Chainstore/Wholesale ☐Government ☐Transportation/Utilities/Communication ☐VAR  
☐System house/company ☐Other \_\_\_\_\_

**9. Would you recommend your D-Link product to a friend?**

☐Yes ☐No ☐Don't know yet

**10. Your comments on this product?**

\_\_\_\_\_



**TO:**

Three vertical lines for an address.

**D-Link®**