D-Link ™ DXS-3326GSR

Managed 24-port Gigabit and 4 1000Base-T Combo Ports Layer 3 Stackable Ethernet Switch

Manual

_____

Information in this document is subject to change without notice.

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.

July 2004 P/N 651XS3326015

Table of Contents

Preface

The *DXS-3326GSR Manual* is divided into sections that describe the system installation and operating instructions with examples.

Section 1, "Introduction" – Describes the Switch and its features.

Section 2, "Installation" – Helps you get started with the basic installation of the Switch and also describes the front panel, rear panel, side panels, and LED indicators of the Switch.

Section 3, "Connecting the Switch" – Tells how you can connect the Switch to your Ethernet network.

Section 4, "Introduction to Switch Management" – Introduces basic Switch management features, including password protection, SNMP settings, IP address assignment and connecting devices to the Switch.

Section 5, "Introduction to Web-based Switch Management" – Talks about connecting to and using the Web-based switch management feature on the Switch.

Section 6, "Configuration" – A detailed discussion about configuring some of the basic functions of the Switch, including accessing the Switch information, using the Switch's utilities and setting up network configurations, such as Quality of Service, The Access Profile Table, port mirroring and configuring the Spanning Tree.

Section 7, "Layer 3 IP Networking" – A discussion about Layer 3 IP Networking features including RIP, OSPF, DHCP/BOOTP Relay, DNS Relay, VRRP, IP Multicast Routing Protocol, and PIM-DM.

Section 8, "Security Management" – A discussion of the security features of the Switch, including Security IP, User Accounts, and Access Authentication Control.

Section 9, "SNMP Manager" – A detailed discussion regarding the Simple Network Monitoring Protocol including description of features and a brief introduction to SNMP.

Section 10, "Monitoring" – Features graphs and windows used in monitoring features and packets on the Switch.

Section 11, "Maintenance" – Features information on Switch utility functions, including TFTP Services, Switch History, Ping Test Save Changes and Rebooting Services.

Section 12, "Single IP Management" – Discussion on the Single IP Management function of the Switch, including functions and features of the Java based user interface and the utilities of the SIM function.

Appendix A, "Technical Specifications" – The technical specifications of the DGS-3324SRi

Appendix B, "Cables and Connectors" – Describes the RJ-45 receptacle/connector, straight-through and crossover cables and standard pin assignments.

Appendix C, "Cable Lengths" – Information on cable types and maximum distances.

Glossary – Lists definitions for terms and acronyms used in this document.

Intended Readers

The *DXS-3326GSR Manual* contains information for setup and management of the Switch. It 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.
Bold font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the **File** menu and choose **Cancel**. Used for emphasis. May also indicate system messages or prompts appearing on your screen. For example: You have mail. Bold font is also used to represent filenames, program names and commands. For example: use the copy command.
Boldface Typewriter Font	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.
Italics	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 filename means that you should type the actual filename instead of the word shown in italic.
Menu Name > Menu Option	**Menu Name > Menu Option** Indicates the menu structure. **Device > Port > Port Properties** 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.

	Section 1

Introduction

Fast Ethernet

The growing importance of LANs and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies are proposed to provide greater bandwidth and improve client/server response times. Among them, Fast Ethernet, or 100BASE-T, provides a non-disruptive, smooth evolution from 10BASE-T technology.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Ethernet protocol.

Gigabit Ethernet Technology

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet utilizing the same packet structure, format, and support for CSMA/CD protocol, full duplex, flow control, and management objects, but with a tenfold increase in theoretical throughput over 100Mbps Fast Ethernet and a one hundred-fold increase over 10Mbps Ethernet. Since it is compatible with all 10Mbps and 100Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting a company's existing investment in hardware, software, and trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet are essential to coping with the network bottlenecks that frequently develop as computers and their busses get faster and more users use applications that generate more traffic. Upgrading key components, such as your backbone and servers to Gigabit Ethernet can greatly improve network response times as well as significantly speed up the traffic between your subnetworks.

Gigabit Ethernet enables fast optical fiber connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies.

Switching Technology

Another key development pushing the limits of Ethernet technology is in the field of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by making it possible for a local area network to be divided into different segments, which are not competing with each other for network transmission capacity, and therefore decreasing the load on each segment.

The Switch acts as a high-speed selective bridge between the individual segments. Traffic that needs to go from one segment to another (from one port to another) is automatically forwarded by the Switch, without interfering with any other segments (ports). This allows the total network capacity to be multiplied, while still maintaining the same network cabling and adapter cards.

For Fast Ethernet or Gigabit Ethernet networks, a switch is an effective way of eliminating problems of chaining hubs beyond the "two-repeater limit." A switch can be used to split parts of the network into different collision domains, for example, making it possible to expand your Fast Ethernet network beyond the 205-meter network diameter limit for 100BASE-TX networks. Switches supporting both traditional 10Mbps Ethernet and 100Mbps Fast Ethernet are also ideal for bridging between existing 10Mbps networks and new 100Mbps networks.

Switching LAN technology is a marked improvement over the previous generation of network bridges, which were characterized by higher latencies. Routers have also been used to segment local area networks, but the cost of a router and the setup and maintenance required make routers relatively impractical. Today's switches are an ideal solution to most kinds of local area network congestion problems.

Switch Description

The DXS-3326GSR is a manageable Gigabit stackable switch designed to uplink network backbones, servers, workstations, and internetwork systems. The DXS-3326GSR is equipped with 24 SFP (Small Form Factor Portable) ports, which are to be used with fibre optical transceiver cabling in order to uplink various other networking devices for a gigabit link that may span great distances. These 24 SFP ports support full-duplex transmissions, have auto-negotiation and can be used with DEM-310GT (1000BASE-LX), DEM-311GT (1000BASE-SX), DEM-314GT (1000BASE-LH) and DEM-315GT (1000BASE-ZX) transceivers.

In addition, the Switch has four 1000BASE-T combo ports that may be used in uplinking various network devices to the Switch, including PCs, hubs and other switches to provide a gigabit Ethernet uplink in full-duplex mode. These four ports are referred to as "combo" ports which means that both the SFP ports and the 1000BASE-T ports are numbered the same (21-24) and cannot be used simultaneously.

Also included at the rear of the Switch are two 10-gigabit stacking ports used to stack up to eight other switches. The DXS-3326GSR may be used as a slave or master unit of a switch stack when utilizing these two ports and can be configured in a Star or Ring topology, and in total, may provide a stacking solution of up to 288 gigabit ports. More information will be provided later in this manual concerning stacking and the DXS-3326GSR.

This Switch may also be equipped with an optional 2-port 10-gigabit XFP module utilizing the module slot at the rear of the Switch. This optional module can provide a 10-gigabit fiber-optic networking solution for network administrators and is operational in full duplex only. This optional module is only compliant with XPF MSA transceivers.

NOTE: The four 1000BASE-T combo ports on the Switch, numbered 21-24 cannot be used simultaneously with the corresponding SFP ports, numbered 21-24. If both ports are in use at the same time (ex. port 21 of the SFP and port 21 of the 1000BASE-T), the SFP ports will take priority over the combo ports and render the 1000BASE-T ports inoperable.

Features

- IEEE 802.3z compliant
- IEEE 802.3x Flow Control in full-duplex compliant

- IEEE 802.3u compliant
- IEEE 802.3ab compliant
- IEEE 802.3ae compliant (for optional XFP module)
- IEEE 802.1p Priority Queues
- IEEE 802.3ad Link Aggregation Control Protocol support.
- IEEE 802.1x Port-based and MAC-based Access Control
- IEEE 802.1Q VLAN
- IEEE 802.1D Spanning Tree, IEEE 802.1W Rapid Spanning Tree and IEEE 802.1s Multiple Spanning Tree support
- Stacking support in either Ring or Star topology
- Access Control List (ACL) support
- IP Multinetting support
- Protocol VLAN support
- Single IP Management support
- Access Authentication Control utilizing TACACS, XTACACS, TACACS+ and RADIUS protocols
- Dual Image Firmware
- Simple Network Time Protocol support
- MAC Notification support
- System and Port Utilization support
- System Log Support
- High performance switching engine performs forwarding and filtering at full wire speed up to 128Gbps.
- Full- and half-duplex for all gigabit ports. Full duplex allows the switch port to simultaneously transmit and receive data. It only works with connections to full-duplex-capable end stations and switches. Connections to a hub must take place at half-duplex.
- Support broadcast storm filtering
- Non-blocking store and forward switching scheme capability to support rate adaptation and protocol conversion
- Supports by-port Egress/Ingress rate control
- Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed
- Support port-based enable and disable
- Address table: Supports up to 8K MAC addresses per device
- Supports a packet buffer of up to 3 Mbits
- Supports Port-based VLAN Groups
- Port Trunking with flexible load distribution and fail-over function
- IGMP Snooping support
- Layer 3 support including DVMRP, OSPF and RIP
- SNMP support
- Secure Sockets Layer (SSL) and Secure Shell (SSH) support
- Port Mirroring support
- MIB support for:
- RFC1213 MIB II
- RFC1493 Bridge

- RFC1757 RMON

- RFC1643 Ether-like MIB

- RFC2233 Interface MIB

- IF MIB

- Private MIB

- RFC2674 for 802.1p

- IEEE 802.1x MIB

- RS-232 DCE console port for Switch management

- Provides parallel LED display for port status such as link/act, speed, etc.

Ports

- Twenty-four high-performance SFP ports for a fiber-optic connection to various network connections, for use over great distances.

- Four 1000BASE-T combo ports that may be used in uplinking various network devices to the Switch, including PCs, hubs and other switches to provide a gigabit Ethernet uplink in full-duplex mode.

- Two 10 gigabit stacking ports at the rear of the Switch for stacking switches utilizing either a ring or star topology.

- An optional module slot at the rear of the Switch to add an optional 2-port 10-gigabit XFP module for uplionking using fibre optic cabling.

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

NOTE: For customers interested in D-View, D-Link Corporation's proprietary SNMP management software, go to the D-Link Website (www.dlink.com.cn) and download the software and manual.

Installing the SFP ports

The Switch is equipped with 24 SFP (Small Form Factor Portable) ports, which are to be used with fiber optical transceiver cabling in order to uplink various other networking devices for a gigabit link that may span great distances. These 24 SFP ports support full-duplex transmissions, have auto-negotiation and can be used with DEM-310GT (1000BASE-LX), DEM-311GT (1000BASE-SX), DEM-314GT (1000BASE-LH) and DEM-315GT (1000BASE-ZX) transceivers. See the figure below for installing the SFP ports in the Switch.
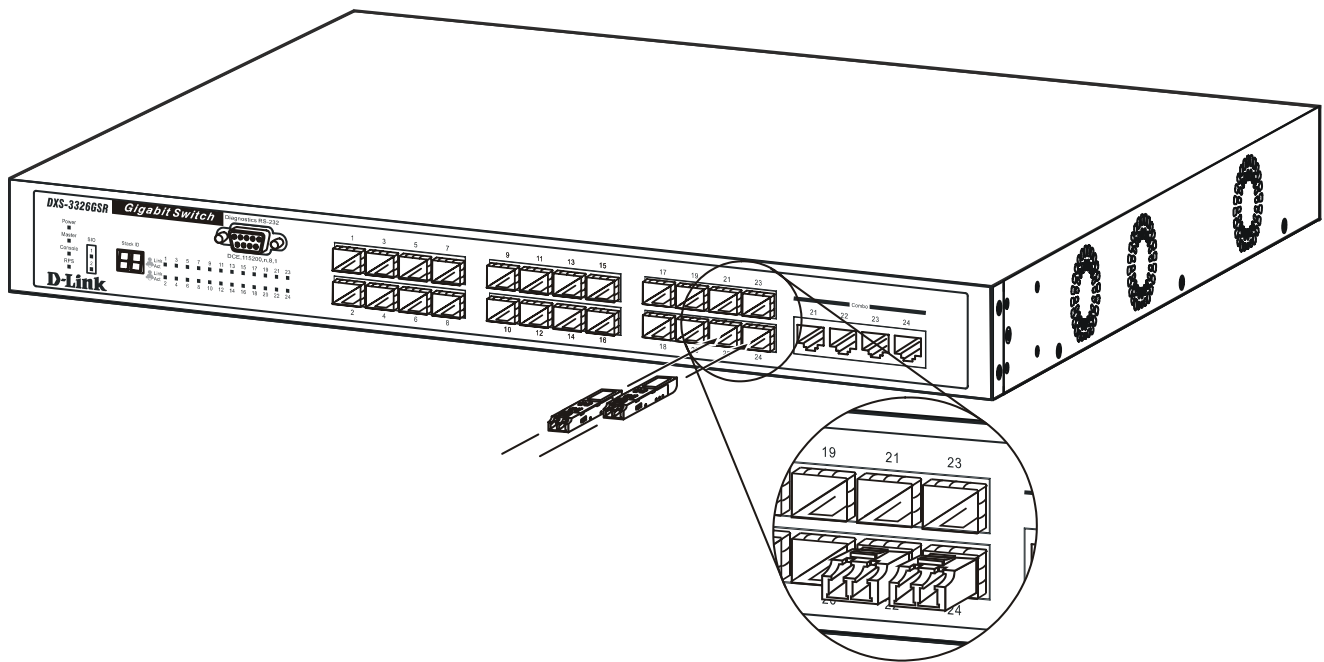
Figure 1- 1. Inserting the fibe-optic transceivers into the DXS-3326GSR

Front-Panel Components

The front panel of the Switch consists of LED indicators for Power, Master, Console RPS, SIO (stacking), and Link/Act for each port on the Switch. The front panel also includes a seven-segment LED indicating the Stack ID number, as well as 24 SFP ports, four 1000BASE-T gigabit Ethernet ports and a RS-232 DCE console port for Switch management.

DXS-3326GSR
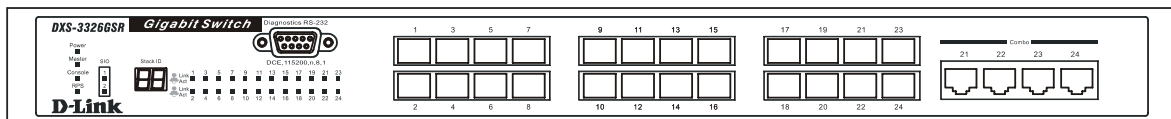
Figure 1- 2. Front Panel View of the DXS-3326GSR as shipped

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

LED Indicators

The Switch supports LED indicators for Power, Master, Console, RPS, SIO (stacking indicators), and Port LEDs. The following shows the LED indicators for the Switch along with an explanation of each indicator.

Figure 1- 3. LED Indicators

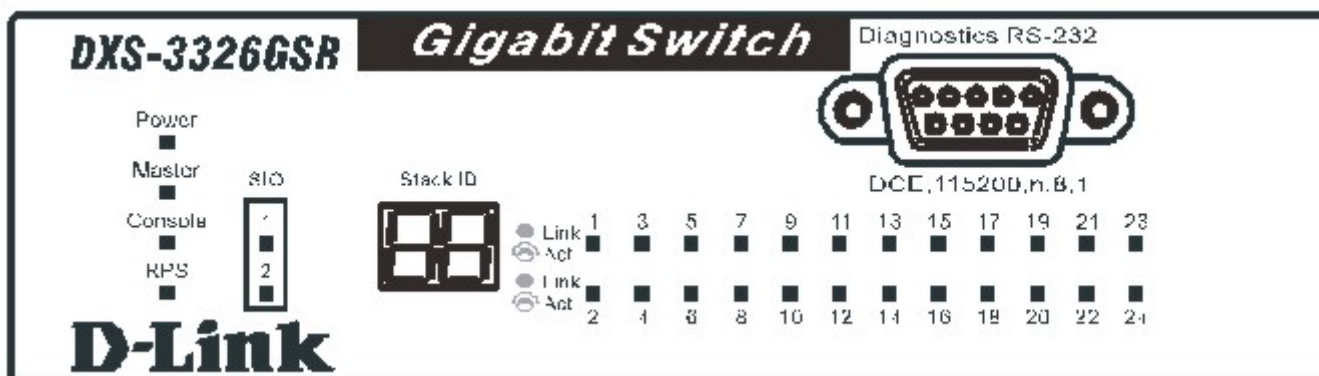| LED	Description
Power	This LED will light green after the Switch is powered on to indicate the ready state of the device. The indicator is dark when the Switch is powered off.
Master	This LED will light solid green when the Switch is configured to be a master switch of a switch stack in a ring topology or when it is in use as a stand-alone switch. This LED will remain dark if the Switch is not configured to be a master switch of a switch stack.
Console	This LED should blink during the Power-On Self Test (POST). When the POST is finished successfully, the LED goes dark. This indicator will light solid green when the Switch is being logged into via out-of-band/local console management through the RS-232 console port in the front of the Switch using a straight-through serial cable. This LED will light solid amber if the Power-On-Self-Test has failed.
RPS	This LED will be lit when the internal power has failed and the RPS has taken over the power supply to the Switch. Otherwise, it will remain dark.
Port LEDs	One row of LEDs for each port is located above the ports on the front panel. The first LED is for the top port and the second one is for the bottom ports. A solid light denotes activity on the port while a blinking light indicates a valid link. These LEDs will remain dark if there is no link/activity on the port.
Stacking Ports (SIO)	There are two LEDs in the front of the Switch marked SIO, and they relate to the two 10-gigabit stacking ports at the rear of the Switch. These LEDs are marked 1 and 2 and will light solid green to denote activity on the port, while a blinking light will indicate a valid link.
Stack ID	These two seven segment LEDs display the current switch stack order of the Switch while in use. Possible numbers to be displayed range from 1-12.

Rear Panel Description

The rear panel of the Switch contains an AC power connector, an optional module slot for uplinking two XFP fiber-optic ports, two 10-gigabit stacking ports, a redundant power supply connector, and a system fan.
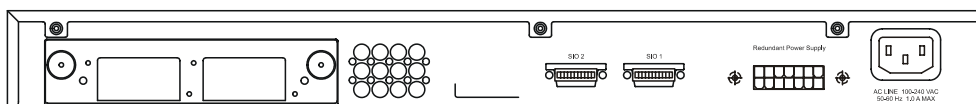
Figure 1- 4. Rear panel view of the Switch

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.

The rear panel also includes an outlet for an optional external power supply. When power fails, the optional external RPS will take over all the power immediately and automatically.

Side Panel Description

The right-hand side panel of the Switch contains three system fans, while the left hand panel includes two heat vents.

The system fans are used to dissipate heat. The sides of the system also provide heat vents to serve the same purpose. Do not block these openings, and leave at least 6 inches of space at the rear and sides of the Switch for proper ventilation. Be reminded that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.
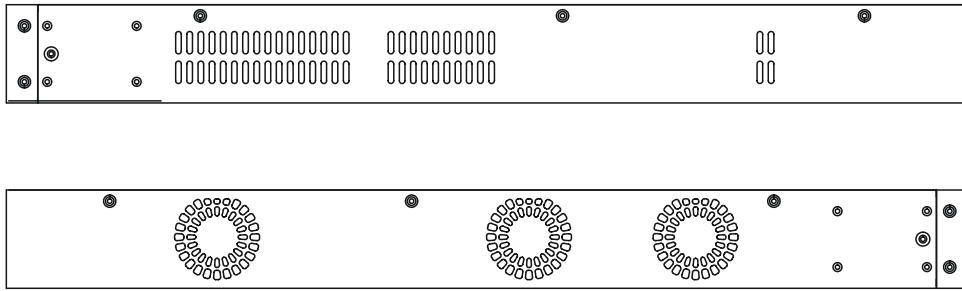
Figure 1- 5. Side Panels

$$\boxed{\textbf{SECTION 2}}$$

Installation

Package Contents

Before You Connect to the Network

Installing the Switch Without the Rack

Installing the Switch In a Rack

Optional Module

External Redundant Power System

Package Contents

Open the shipping carton of the Switch and carefully unpack its contents. The carton should contain the following items:

- One DXS-3326GSR Stackable Switch
- One AC power cord
- Registration card
- Mounting kit (two brackets and screws)
- Four rubber feet with adhesive backing
- RS-232 console cable
- One Cable Infinband 4X50CM
- One CD Kit for User's Guide/CLI/D-View module
- One CD Kit for D-View 5.1 Trial version.
- One Generic QIG
- One Hardware Installation and Getting Started Guide
- This Manual

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

Before You Connect to the Network

The site where you install the Switch may greatly affect its performance. Please follow these guidelines for setting up the Switch.

- Install the Switch on a sturdy, level surface that can support at least 6.6 lb. (3 kg) of weight. Do not place heavy objects on the Switch.
- The power outlet should be within 1.82 meters (6 feet) of the Switch.
- Visually inspect the power cord and see that it is fully secured to the AC power port.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch. Leave at least 10 cm (4 inches) of space at the front and rear of the Switch for ventilation.
- Install the Switch in a fairly cool and dry place for the acceptable temperature and humidity operating ranges.

- Install the Switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.

- When installing the Switch on a level surface, attach the rubber feet to the bottom of the device. The rubber feet cushion the Switch, protect the casing from scratches and prevent it from scratching other surfaces.

Installing the Switch Without the Rack

When installing the Switch on a desktop or shelf, the rubber feet included with the Switch should first be attached. Attach these cushioning feet on the bottom at each corner of the device. Allow enough ventilation space between the Switch and any other objects in the vicinity.
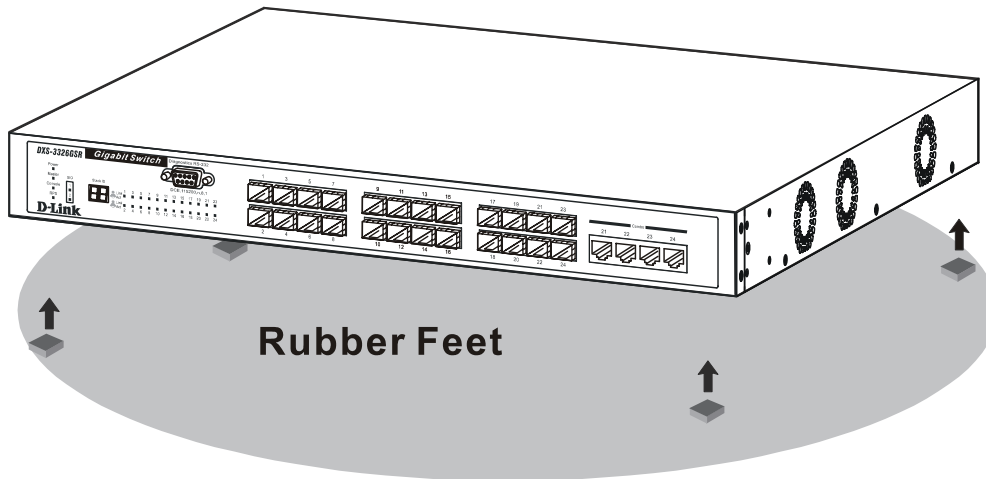
Figure 2- 1. Prepare Switch for installation on a desktop or shelf

Installing the Switch in a Rack

The Switch can be mounted in a standard 19" rack. Use the following diagrams to guide you.
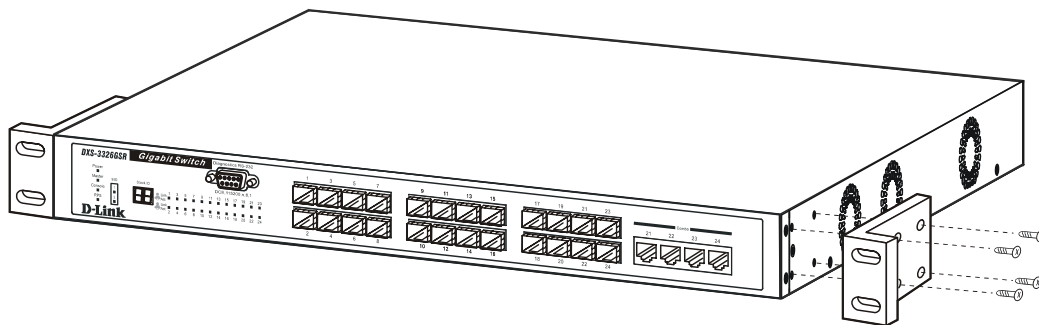

Figure 2- 2. Fasten mounting brackets to Switch

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
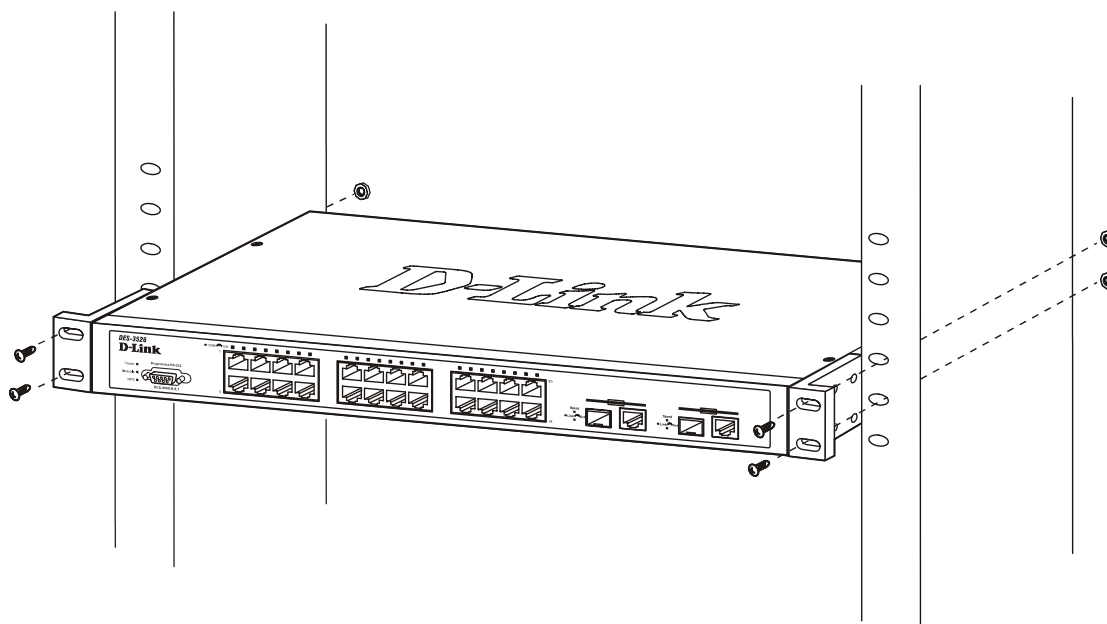
Figure 2- 3. Installing Switch in a rack

Power On

Plug one end of the AC power cord into the power connector of the Switch and the other end into the local power source outlet.

After the Switch is powered on, the LED indicators will momentarily blink. This blinking of the LED indicators represents a reset of the system.

Power Failure

As a precaution, in the event of a power failure, unplug the Switch. When power is resumed, plug the Switch back in.

Optional Module

At the rear of the DXS-3326GSR resides an optional module slot. This slot may be equipped with a 2-port 10GE XFP Uplink Module, sold separately. Adding the DEM-420X optional module will allow the administrator to add 2 fiber-optic ports which will transmit information at a rate of 10 gigabits a second. These two ports are compliant with standard IEEE 802.3ae, support full-duplex transmissions only and can be used with XFP MSA compliant transceivers. To install the module in the DXS-3326GSR, follow the simple steps listed below.

 CAUTION: Before adding the optional module, make sure to disconnect all power sources connected to the Switch. Failure to do so may result in an electrical shock that may cause damage, not only to the individual but to the Switch as well.

At the back of the Switch to the left is the slot for the optional module, as shown in Figure 2-4. This slot should be covered with a faceplate that can be easily removed by loosening the screws and pulling off the plate.

Optional Module Slot
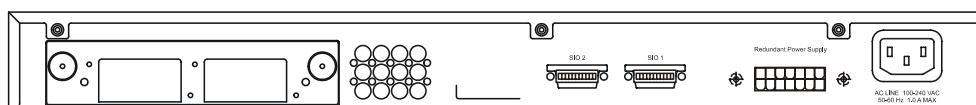
Figure 2- 4. Optional Module slot at the rear of the DXS-3326GSR

After removing the faceplate, remove the DEM-420X optional module from its box. The front panel should resemble the drawing represented in the following figure.
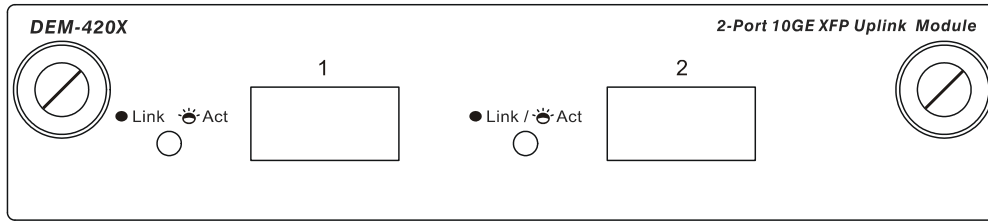
Figure 2- 5. Front Panel of the DEM-420X

Take the module and gently slide it in to the available slot at the rear of the Switch until it reaches the back, as shown in the following figure. At the back of the slot are two sets of plugs that must be connected to the module. Gently, but firmly push in on the module to secure it to the Switch. The module should fit snugly into the corresponding receptors.
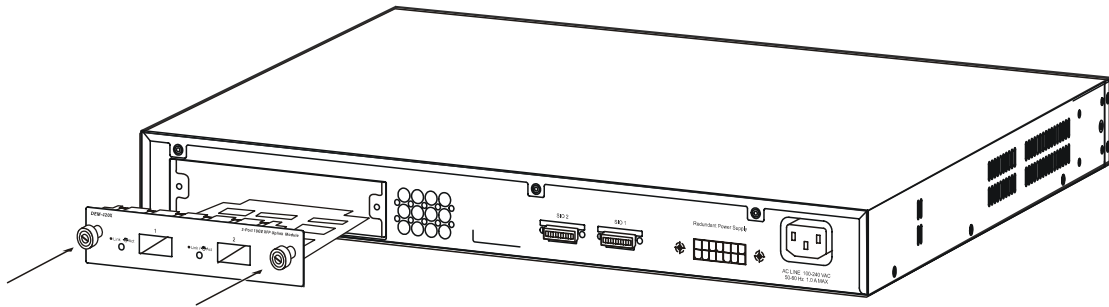
Figure 2- 6. Inserting the optional module into the DXS-3326GSR

Now tighten the two screws at adjacent ends of the module into the available screwholes on the Switch. The upgraded DXS-3326GSR is now ready for use.
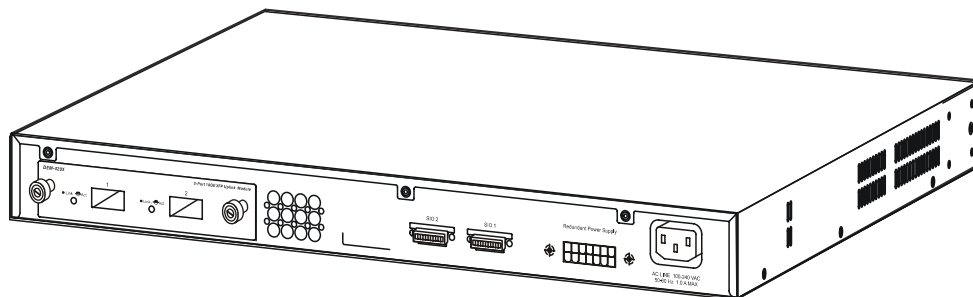
Figure 2- 7. DXS-3326GSR with optional module installed.

External Redundant Power System

The Switch supports an external redundant power system.

DXS-3326GSR

RPS connector

DPS-800 Case   DPS-500 Back Panel
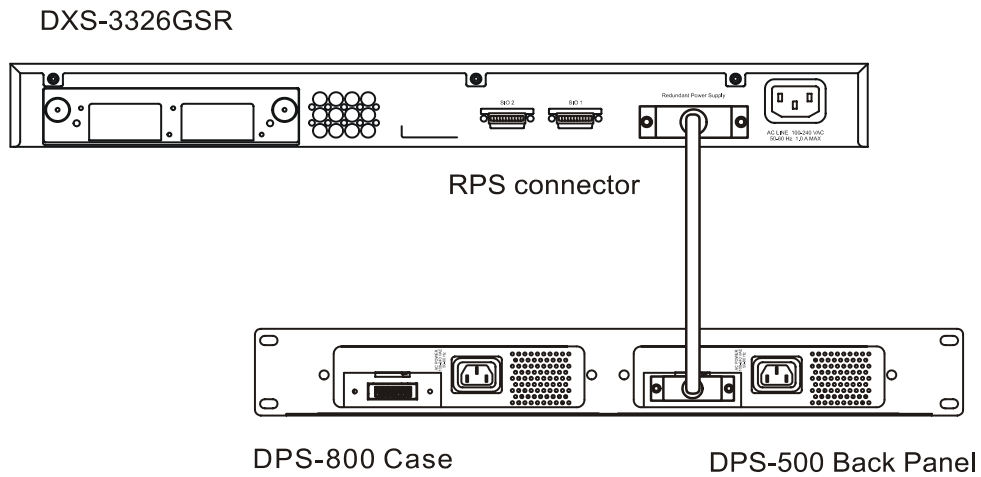
Figure 2- 8. The DXS-3326GSR with the DPS-500 Redundant External Power Supply

DXS-3326GSR

RPS connector

DPS-900 Chassis   DPS-500 Back Panel
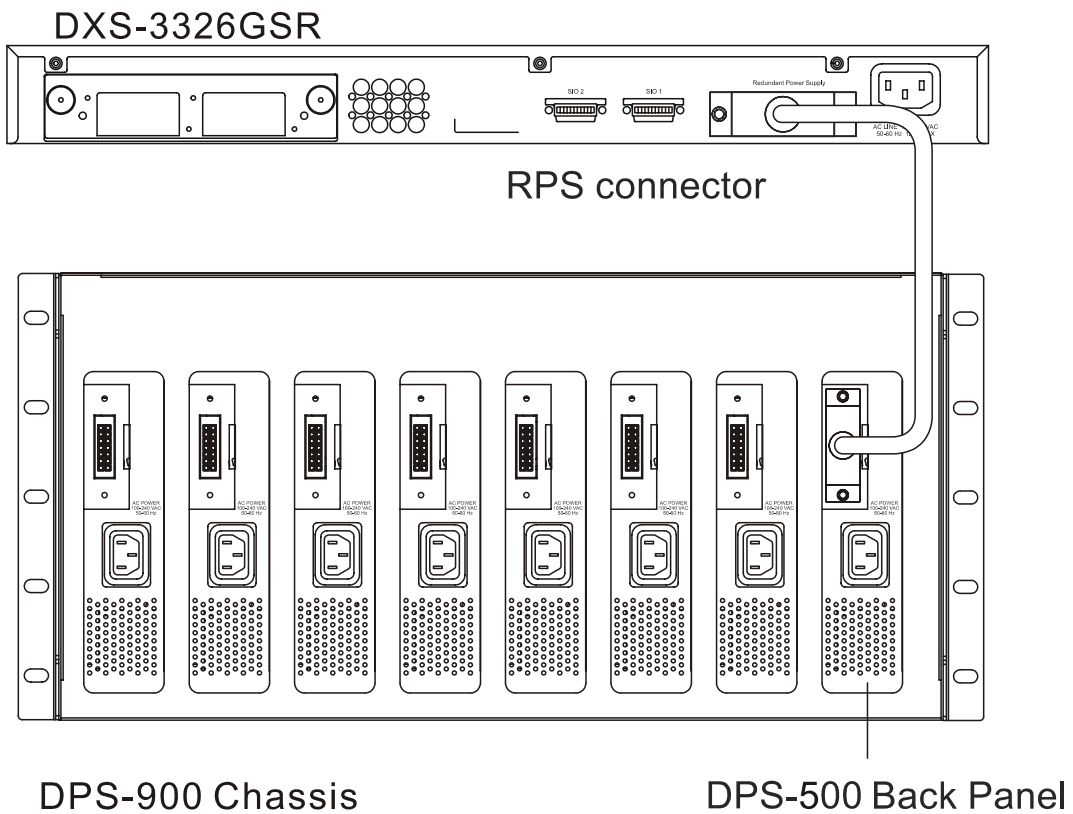
Figure 2- 9. The DXS-3326GSR with the DPS-900 chassis RPS

NOTE: See the DPS-500 documentation for more information.

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

<div align="right">

Section 3

</div>

Connecting the Switch

Switch To End Node

Switch To Hub or Switch

Connecting To Network Backbone or Server

Stacking and the DXS-3326GSR

NOTE: All 24 high-performance NWay Ethernet ports can support both MDI-II and MDI-X connections.

Switch To End Node

End nodes include PCs outfitted with a 10, 100 or 1000 Mbps RJ 45 Ethernet Network Interface Card (NIC) and most routers.

An end node can be connected to the Switch via a twisted-pair UTP/STP cable. The end node should be connected to any of the four 1000BASE-T ports of the Switch.

RJ-45 Connector
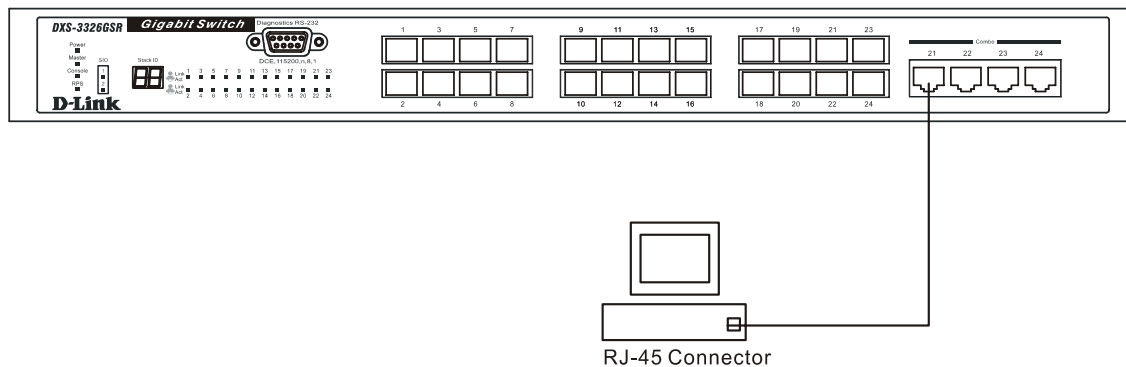
Figure 3- 1. Switch connected to an end node

The Link/Act LEDs for each UTP port will light green or amber when the link is valid. A blinking LED indicates packet activity on that port.

Switch To Hub or Switch

These connections can be accomplished in a number of ways using a normal cable.

- A 10BASE-T hub or switch can be connected to the Switch via a twisted-pair Category 3, 4 or 5 UTP/STP cable.

- A 100BASE-TX hub or switch can be connected to the Switch via a twisted -pair Category 5 UTP/STP cable.

- A 1000BASE-T switch can be connected to the Switch via a twisted pair Category 5e UTP/STP cable.

- A switch supporting a fibre optic uplink can be connected to the Switch's SFP ports via fiber-optic cabling.
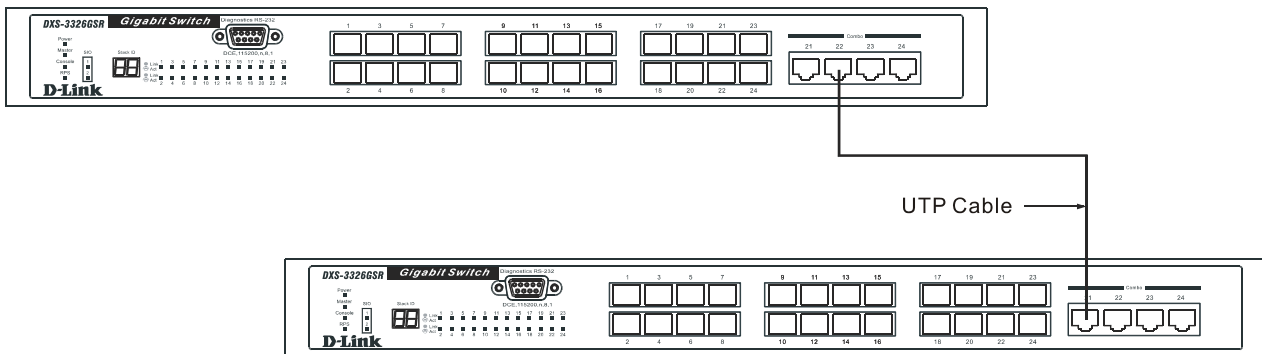
Figure 3- 2. Switch connected to a port on a hub or switch using either a straight or crossover cable-any normal cable is fine
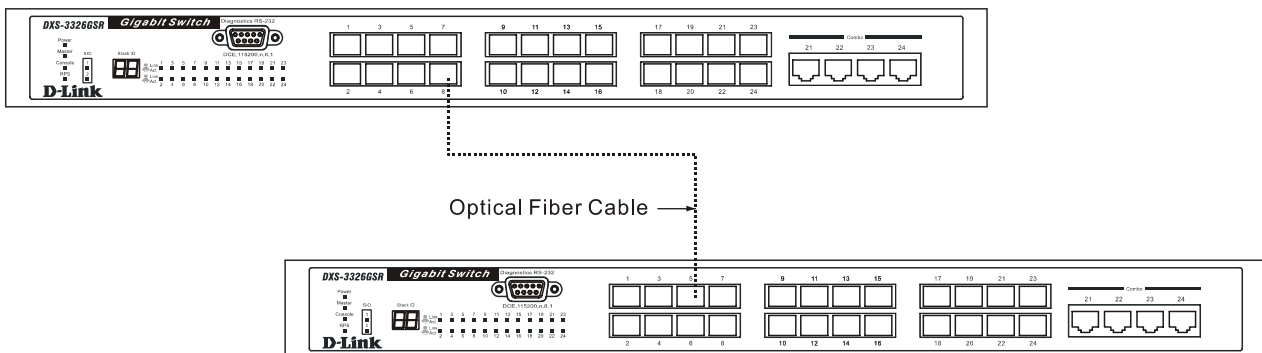
Figure 3- 3. Switch connected to switch using fiber-optic cabling

Connecting To Network Backbone or Server

The 24 SFP ports and the four combo 1000BASE-T ports are ideal for uplinking to a network backbone, server or server farm. The copper ports operate at a speed of 1000, 100 or 10Mbps in full or half duplex mode. The fiber-optic ports can operate at 1000Mbps in full duplex mode only.

Connections to the Gigabit Ethernet ports are made using fiber-optic cable or Category 5e copper cable, depending on the type of port. A valid connection is indicated when the Link LED is lit.
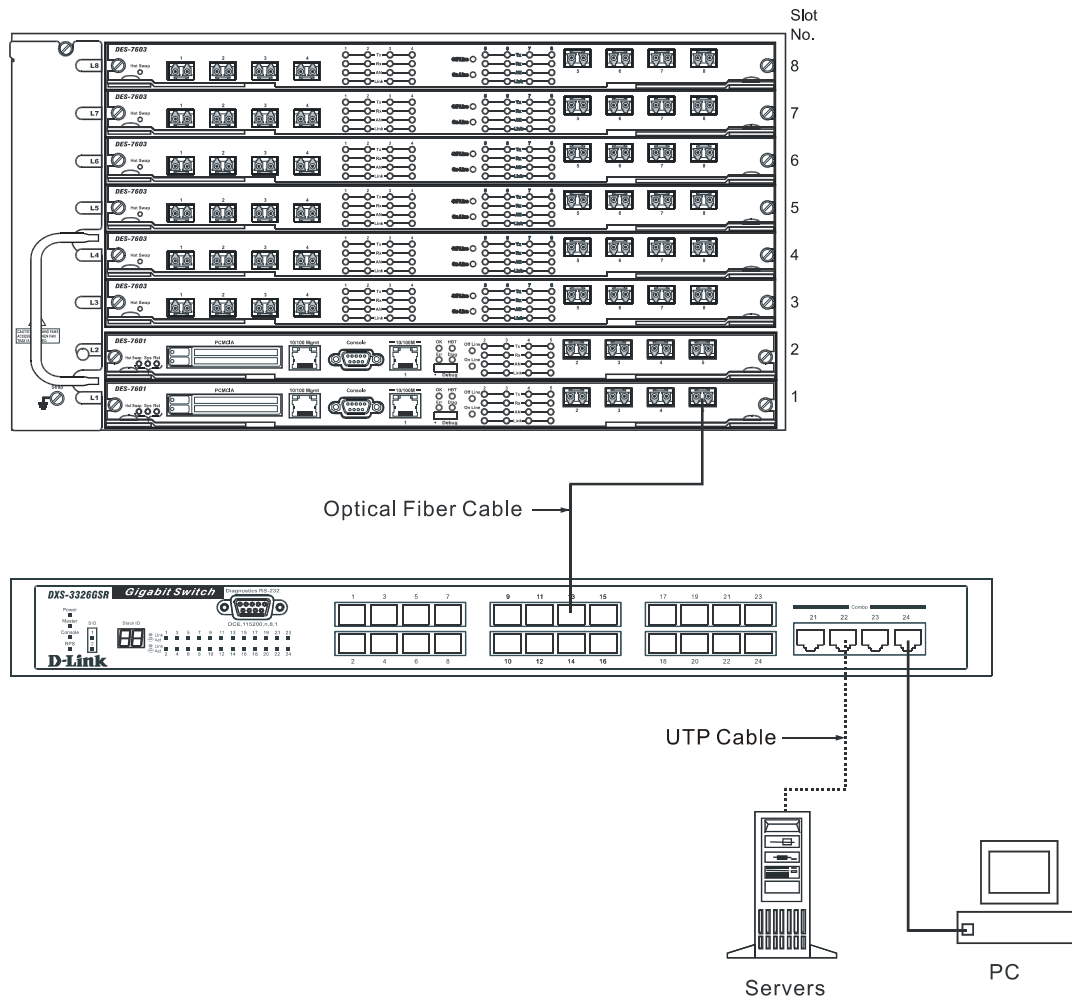
Figure 3- 4. Uplink Connection to a server, PC or switch stack.

Stacking and the DXS-3326GSR

The DXS-3326GSR is equipped with two 10-gigabit stacking ports at the rear of the Switch, as seen in the following figure. These stacking ports may be used to stack the DXS-3326GSR to a master switch to be used in a switch stack.
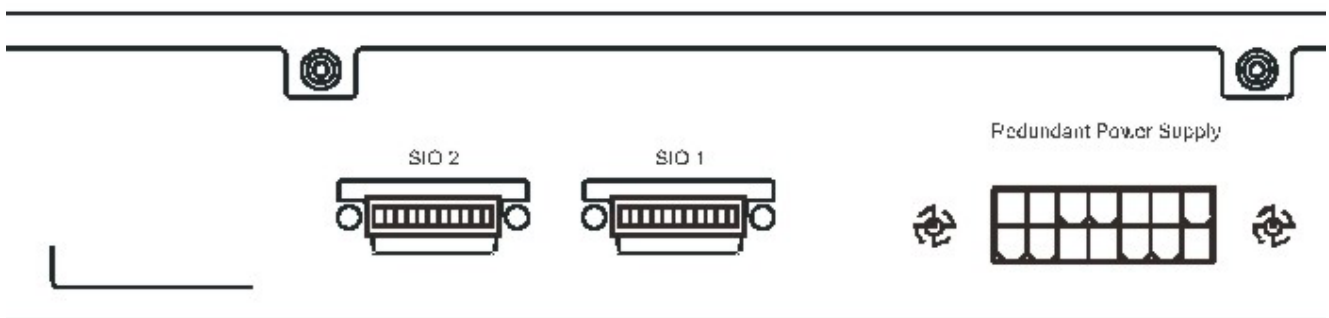
Figure 3- 5. SIO 1 and SIO 2 Stacking ports at the rear of the DXS-3326GSR

These two stacking ports, named SIO 1 and SIO 2 can be used with other stacking switches for a scalable stacking solution of up to 288 ports in a star or ring toplogy. These two stacking ports have corresponding LEDs at the front of the Switch, labeled SIO 1 and SIO 2 and will light solid green whenever the port is in use. The seven-segment LED Stack ID to the left of the SIO LEDs on the front of the Switch will display the Stack ID number of the Switch in a switch stack.
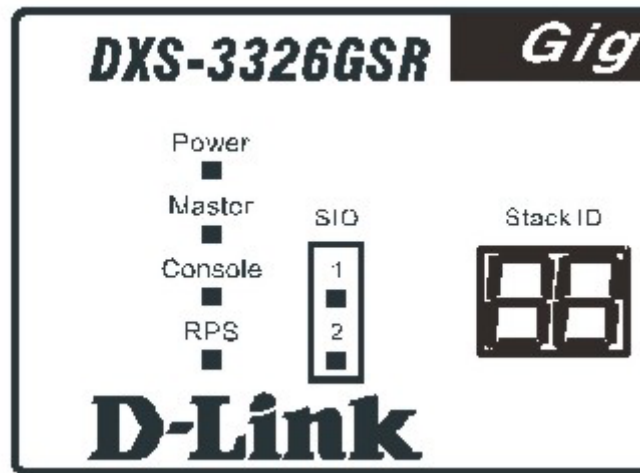
Figure 3- 6. Stacking LEDs at the front of the DXS-3326GSR

The Switch can be stacked in a star or ring topology, as previously mentioned. For a star architecture, only one of the two Gigabit stacking ports will be in use. This port will be connected to the master switch of the switch stack and will act as a slave switch of the stack. The administrator may use either of the two available stacking ports to achieve this arcitecture. See the following diagram for an example of stacking in a star architecture.
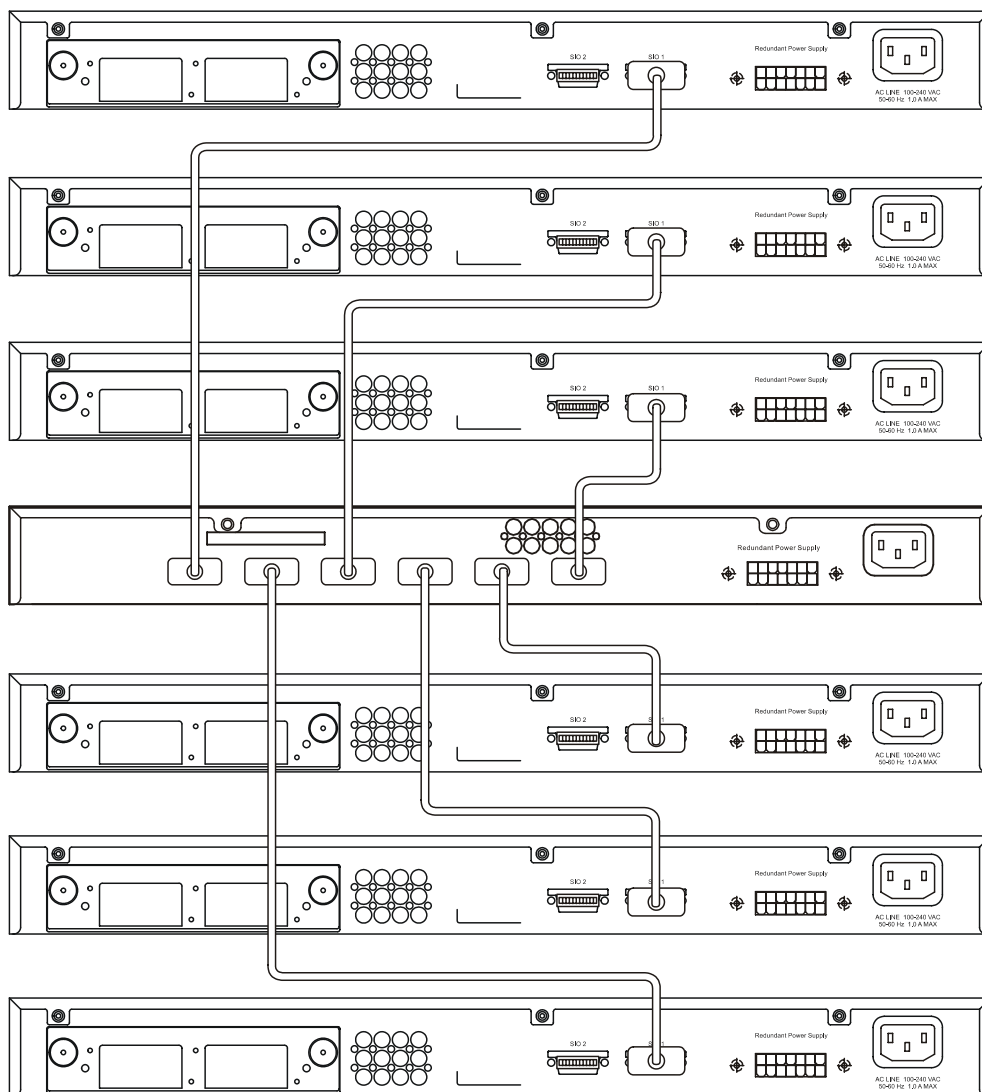
Figure 3- 7. Stacking in a Star Architecture

17

For stacking the in a ring architecture, both SIO ports will be in use, as shown in the following diagram. Up to 12 DXS-3326GSR switches may be stacked together in the ring architecture switch stack, though there are limitations on stacking, which will be discussed in the following section.
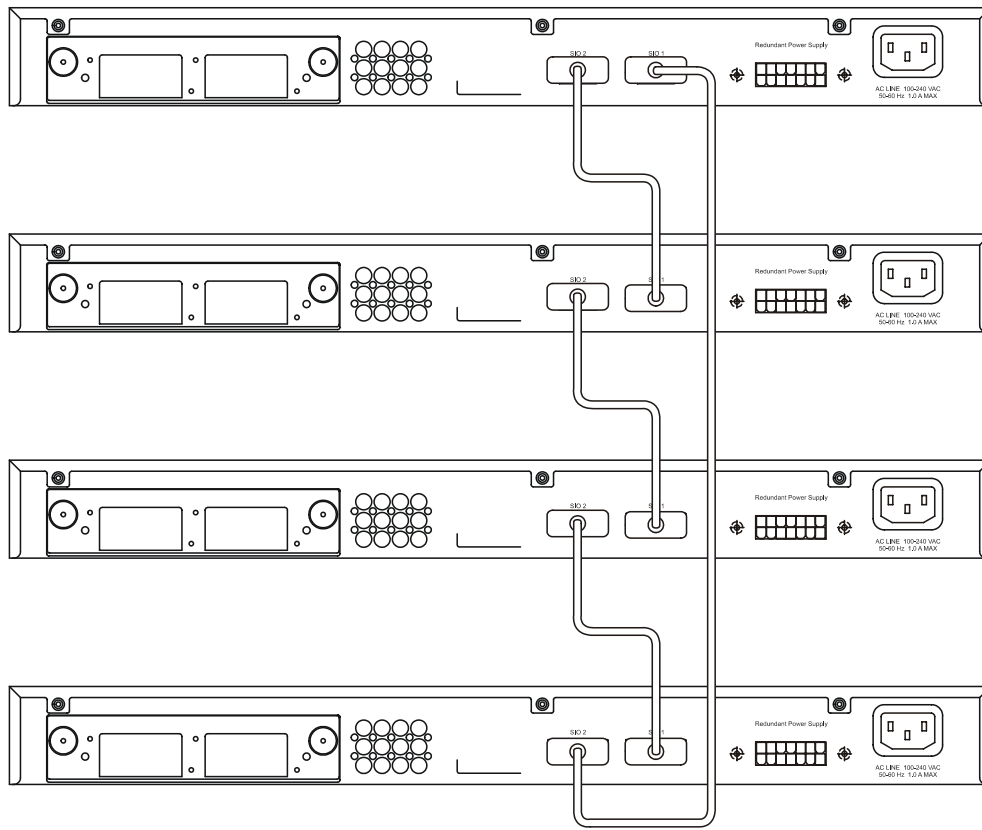
Figure 3- 8. Stacking in a Ring Architecture

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.

Stacking Limitations Utilizing a Ring or Star Toplogy

The Switches listed in the table below can all be stacked, but there is a limitation as to the number of Switches that can be included in a given stack. This limitation arises from a concept called a Token Cost. This Token Cost is used for communication between switches in a switch stack. Some of the switches have 2 as their token cost, while others are 4, and the 10G uplink ports have a Token Cost of 2. The maximum accumulated Token Cost in a given stack must be less than 32.

There is an additional limitation in that a maximum of 12 Switch boxes can be included in a given switch stack, using a ring topology.

In order to make the task of determining if a given set of Switches (from the table below) can be successfully stacked, use the following formula:

Token Cost * Number of Switches ≤32

Model Name	Token Cost
DGS-3324SRi	2
DGS-3324SR	2
DES-3352SR	2
DXS-3350SR	4
	6 (with 10G uplink)
DXS-3326GSR	2
	4 (with 10G uplink)

Table 3- 1. Switches and their corresponding token cost

Stacking In a Ring Topology

For example:

All of the stacked switches are identical.

You want to stack as many DXS-3326GSR switches as possible. The DXS-3326GSR switches do not have a 10G uplink, so their individual Token Cost is 2.

To calculate the maximum number of DXS-3326GSR switches in the ring stack, use the following formula:

Token Cost * Number of Switches ≤ 32

2 * Number of Switches ≤ 32

Number of Switches ≤ 32/2

Number of Switches ≤ 16

For this example, a maximum of 16 DXS-3326GSR switches (where all of these switches have a 10G uplink) can be ring stacked according to the previous calculations, but we must remember that there is a maximum limitation of 12 switches, so the actual maximum number of DXS-3326GSR switches that can be stacked together in the ring topology is twelve.

Remembering that our token cost cannot exceed 32, we realize that our current switch stack has a total token cost of 24 (12 * 2) and we still have a remainder of 8 left in our token cost. To maximize the usage of our switch stack, we decide to add the optional module to the rear of the Switch that has an individual token cost of 2. Since we have 8 left in our token cost, we are capable of adding four optional modules to any of the DXS-3326GSRs in the switch stack. (4 * 2 = 8) (8 + 24 ≤ 32)

To determine how many DXS-3326GSR switches (each with a 10G uplink port) could be stacked in a ring stack, you need to redo the calculation above using a Token Cost of 4 for each DXS-3326GSR switch.

To calculate the maximum number of DXS-3326GSR switches (with a 10G uplink port) in the ring stack, use the following formula:

Token Cost * Number of Switches ≤ 32

4 * Number of Switches ≤ 32

Number of Switches ≤ 32/4

Number of Switches ≤ 8

In this case, a maximum of eight DXS-3326GSR switches (where all of these switches have a 10G uplink) can be ring stacked.

Adding a different switch type to an existing stack

In this example, there are three different switch types, each with different token costs. There is one DGS-3324SR (Token Cost = 2), two DXS-3350SRs (Token Cost = 4), and three DXS-3326GSRs (Token Cost = 2). In this case the total Token Cost would be:

(1 * 2) + (2 * 4) + (3 * 2) = 16

If you then wanted to add the maximum number of DXS-3326GSR Switches (Token Cost = 2) to this stack:

(1*2 + 2 * 4 + 3 * 2) + Number of Switches * 2 ≤ 32

16 + Number of Switches * 2 ≤ 32

Number of Switches * 2 ≤32 – 16 = 16

Number of Switches ≤ 16/2 =8

So, in this case, you could add an extra eight DXS-3326GSR switches to this ring stack. The entire stack would then consist of eight DGS-3326GSRs, 1 DGS-3324SRs (Token Cost = 2), two DXS-3350SRs (Token Cost = 4), and three DXS-3326GSRs (Token Cost = 2). This gives a total Token Cost for the stack of:

1 * 2+ 8 * 2 + 2 *4 + 3 * 2 =32

Although the Token Cost is 32, the number of switch boxes is 14, which exceeds the maximum number of 12. Thus, only seven extra DXS-3326GSRs can be added to the ring stack.

For further examples, we can:

- Make a ring stack consisting of four DXS-3350SRs (one with module), three DGS-3324SRs, and three DXS-3326GSRs (no modules). Our switch count would equal 10 and our token cost would equal 32 (18 + 8+ 6 = 32 ≤ 32). Success!

- Make a ring stack consisting of four DGS-3324SRs, five DXS-3326GSRs (no modules), and three DXS-3350SRs (no modules). Our switch count would equal 12 and our token cost would equal 30 (8 + 10 + 12 = 30 ≤32). Success!

- Add four 10G modules to an existing ring stack (2+2+2+2=8). Using a stack consisting of six DGS-3324SRs and six DXS-3326GSRs (12 + 20 = 32). This is the maximum number of switch boxes allowed in a ring stack. Our switch count stay at 12 and our token cost becomes 32 (2 +2 + 2 +2+ 24 = 32 ≤ 32). Success!

Stacking In a Star Topology

In this case, the DGS-3324SRi is the Master Switch in a star topology. And up to six slave switches can be stacked with Master Stackable Switch. Check the following examples as a reference guide.

For examples, we can:

- Make a star stack consisting of one DGS-3324SRi (Master) and six DXS-3326GSRs (with modules). Our switch count would equal 6+1 and our token cost would equal 26 (2 + 24 = 26 ≤ 32). Success!

- Make a star stack consisting of one DGS-3324SRi (Master), one DGS-3324SR, two DXS-3326GSRs (no modules), and three DXS-3350SRs (one with module). Our switch count would equal 6+1 and our token cost would equal 22(2 + 2 + 4 + 14 = 22 ≤32). Success!

From these examples, we can see that there is a myriad of combinations possible for adding switches and modules to a given stack. Yet, you must keep in mind three very important points in configuring the stack:

1. **The total Token Cost of switches stacked must not exceed 32.**

2. **The total switch count of switches stacked in a ring topology cannot exceed 12.**

3. **The total switch count of switches stacked in a star topology cannot exceed 6+1.**

> **NOTE:** The total token cost of switches in a switch stack cannot exceed 32. Surpassing this token cost limitation will result in failure of the Switch stack and render the switches in it inoperable.

<div style="text-align: right; border: 1px solid black; display: inline-block; padding: 10px;">

Section 4

</div>

Introduction To Switch Management

> ***Management Options***
>
> ***Web-based Management Interface***
>
> ***SNMP-Based Management***
>
> ***Managing User Accounts***
>
> ***Command Line Console Interface Through The Serial Port***
>
> ***Connecting the Console Port (RS-232 DCE)***
>
> ***First Time Connecting to The Switch***
>
> ***Password Protection***
>
> ***SNMP Settings***
>
> ***IP Address Assignment***
>
> ***Connecting Devices to the Switch***

Management Options

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

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 Netscape Navigator (version 6.2 and higher) or Microsoft® Internet Explorer (version 5.0).

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.

Command Line Console Interface Through the Serial Port

You can also connect a computer or terminal to the serial console port to access the Switch. The command-line-driven interface provides complete access to all Switch management features.

Connecting the Console Port (RS-232 DCE)

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 female 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:

3. Select the appropriate serial port (COM port 1 or COM port 2).

4. Set the data rate to 115,200 baud.

5. Set the data format to 8 data bits, 1 stop bit, and no parity.

6. Set flow control to none.

7. Under Properties, select VT100 for Emulation mode.

8. Select Terminal keys for Function, Arrow, and Ctrl keys. Ensure that you select Terminal keys (not Windows keys).

> **NOTE:** 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 for information on Windows 2000 service packs.

9. 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.

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

11. 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.

12. 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 ***DXS-3326GSR Command Line Interface Reference Manual*** on the documentation CD for a list of all commands and additional information on using the CLI.

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

Make sure the terminal or PC you are using to make this connection is configured to match these settings.

If you are having problems making this connection on a PC, make sure the emulation is set to VT-100. You will be able to set the emulation by clicking on the File menu in you HyperTerminal window, clicking on Properties in the drop-down menu, and then clicking the Settings tab. This is where you will find the Emulation options. If you still do not see anything, try rebooting the Switch by disconnecting its power supply.

Once connected to the console, the screen below will appear on your console screen. This is where the user will enter commands to perform all the available management functions. The Switch will prompt the user to enter a user name and a password. Upon the initial connection, there is no user name or password and therefore just press Enter twice to access the command line interface.

```
                 DXS-3326GSR  Stackable Ethernet Switch
                           Command Line Interface

                          Firmware: Build 3.00-B16
          Copyright(C) 2004-2007 D-Link Corporation. All rights reserved.
UserName:_
```
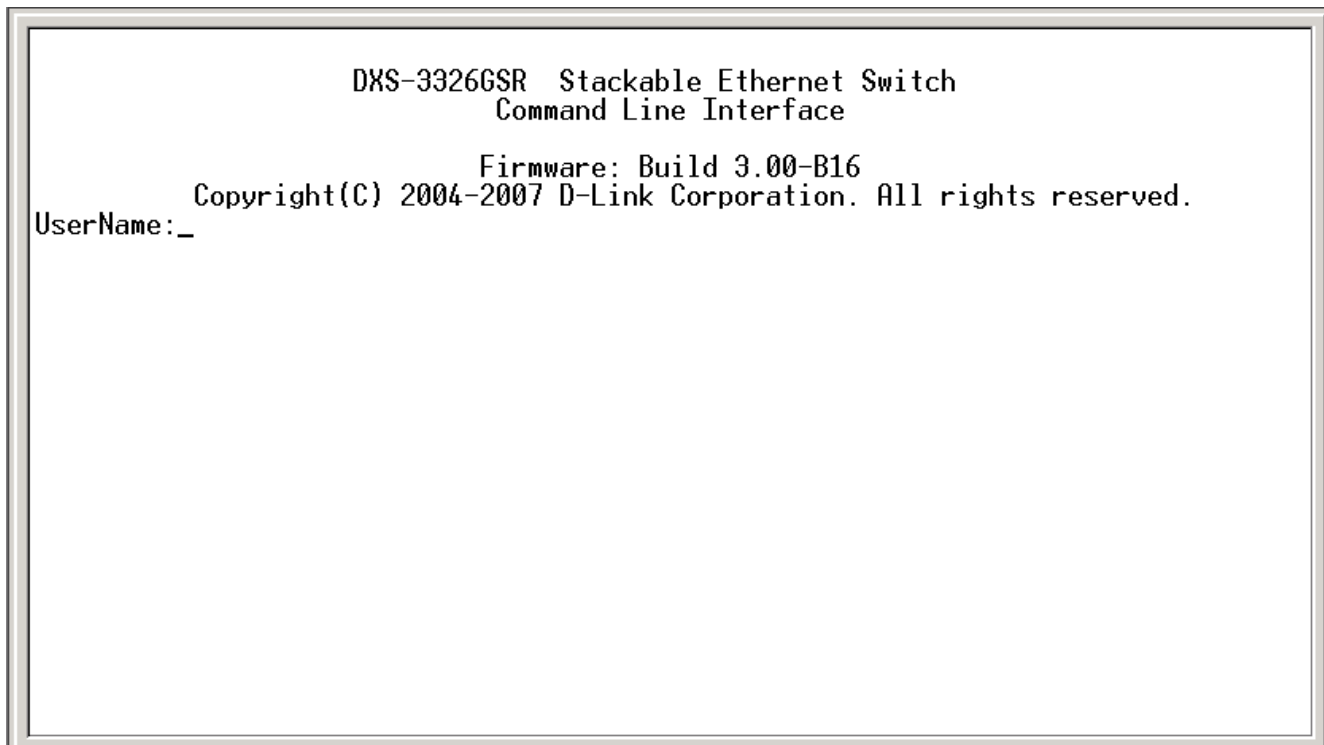
Figure 4- 1. Initial screen after first connection.

First Time Connecting to the Switch

The Switch supports user-based security that can allow you to prevent unauthorized users from accessing the Switch or changing its settings. This section tells how to log onto the Switch.

NOTE: The passwords used to access the Switch are case-sensitive; therefore, "S" is not the same as "s."

When you first connect to the Switch, you will be presented with the first login screen (shown above).

NOTE: Press Ctrl+R to refresh the screen. This command can be used at any time to force the console program in the Switch to refresh the console screen.

Press Enter in both the Username and Password fields. You will be given access to the command prompt **DXS-3326GSR:4#** shown below:

There is no initial username or password. Leave the **Username** and **Password** fields blank.

```
                DXS-3326GSR  Stackable Ethernet Switch
                        Command Line Interface

                        Firmware: Build 3.00-B16
         Copyright(C) 2004-2007 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DXS-3326GSR:4#_
```
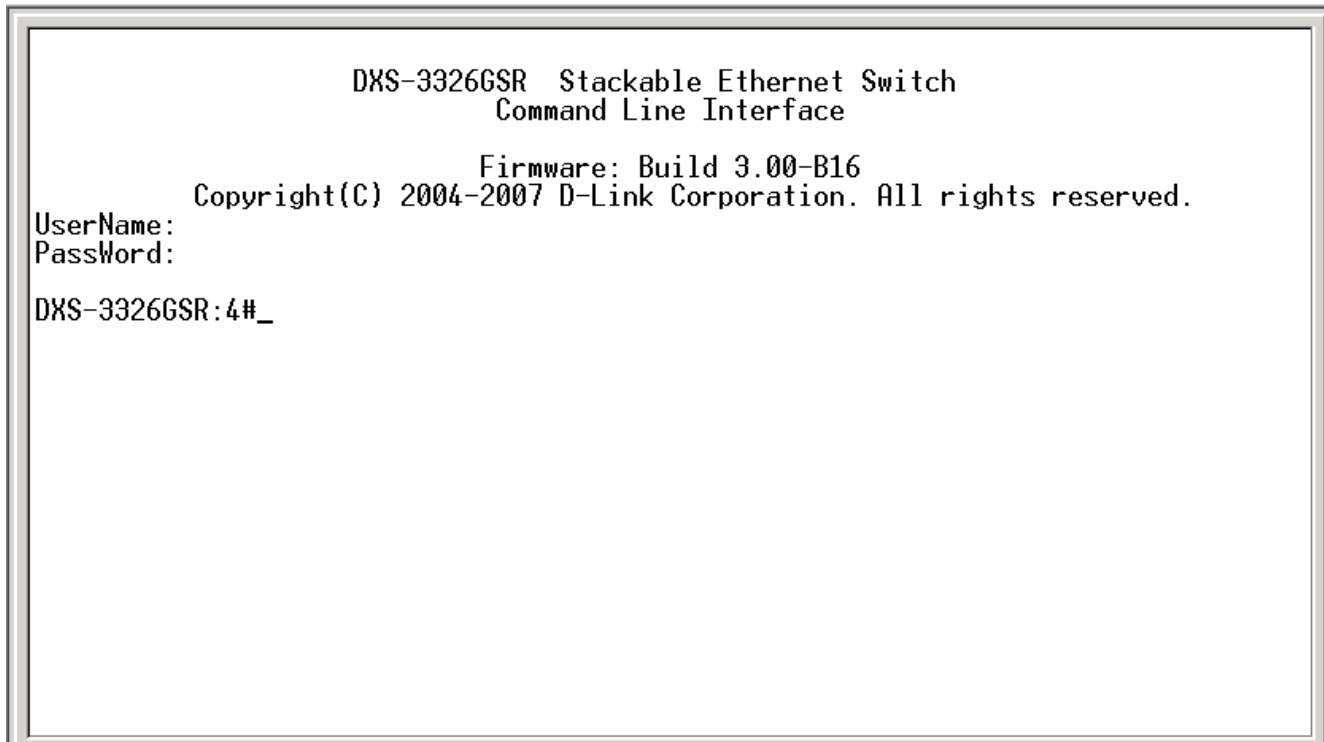
Figure 4- 2. Command Prompt

NOTE: The first user automatically gets Administrator level privileges. It is recommended to create at least one Admin-level user account for the Switch.

Password Protection

The DXS-3326GSR does not have a default user name and password. One of the first tasks when settings up the Switch is to create user accounts. If you log in using a predefined administrator-level user name, you have privileged access to the Switch's management software.

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

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

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

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

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

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

NOTE: Passwords are case sensitive. User names and passwords can be up to 15 characters in length.

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

DXS-3326GSR:4#create account admin newmanager

Command: create account admin newmanager

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


Success.


DXS-3326GSR: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 DXS-3326GSR supports SNMP versions 1, 2c, and 3. You can specify which version of 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 section entitled 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 by entering the command "show switch" into the command line interface, as shown below.

```
Device Type       : DXS-3326GSR Stackable Ethernet Switch
Unit ID           : 1
MAC Address       : 00-10-30-12-08-00
IP Address        : 10.24.22.9 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 2.00-B04
Firmware Version  : Build 3.00-B16
Hardware Version  : 2A1
Device S/N        :
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
RIP               : Disabled
DVMRP             : Disabled
PIM-DM            : Disabled
OSPF              : Disabled
TELNET            : Enabled (TCP 23)
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Figure 4- 3. Show switch command

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

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

The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy.** Where the x's represent the IP address to be assigned to the IP interface named System and the y's represent the corresponding subnet mask.

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

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

```
                DXS-3326GSR  Stackable Ethernet Switch
                        Command Line Interface

                        Firmware: Build 3.00-B16
              Copyright(C) 2004-2007 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DXS-3326GSR:4#config ipif System ipaddress 10.24.22.9/255.0.0.0
Command: config ipif System ipaddress 10.24.22.9/8

Success.

DXS-3326GSR:4#
```

Figure 4- 4. Assigning the Switch an IP Address

In the above example, the Switch was assigned an IP address of 10.24.22.9 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.

<div style="text-align: right; border: 1px solid black; display: inline-block;">

Section 5

</div>

Introduction to Web-based Switch Configuration

Login To Web manager

Web-Based User Interface

Basic Setup

Reboot

Basic Switch Setup

Network Management

Switch Utilities

Network Monitoring

IGMP Snooping Status

All software functions of the DXS-3326GSR can be 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.

Login to Web Manager

To begin managing your 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 page that opens, click on the following **Login** button:

Figure 5- 1. Login button

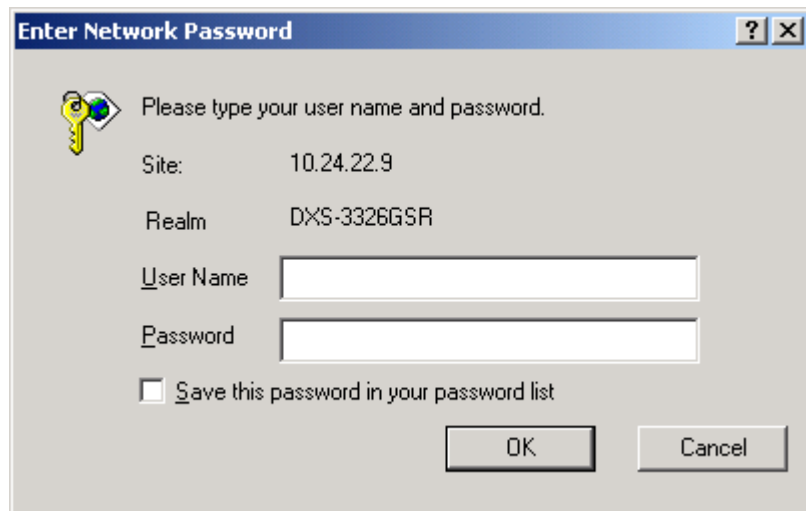This opens the management module's user authentication dialog box, as seen below.

Figure 5- 2. Enter Network Password dialog box

Leave both the User Name field and the Password field blank and click **OK**. This will open the Web-based user interface. The Switch management features available in the web-based manager are explained below.

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.
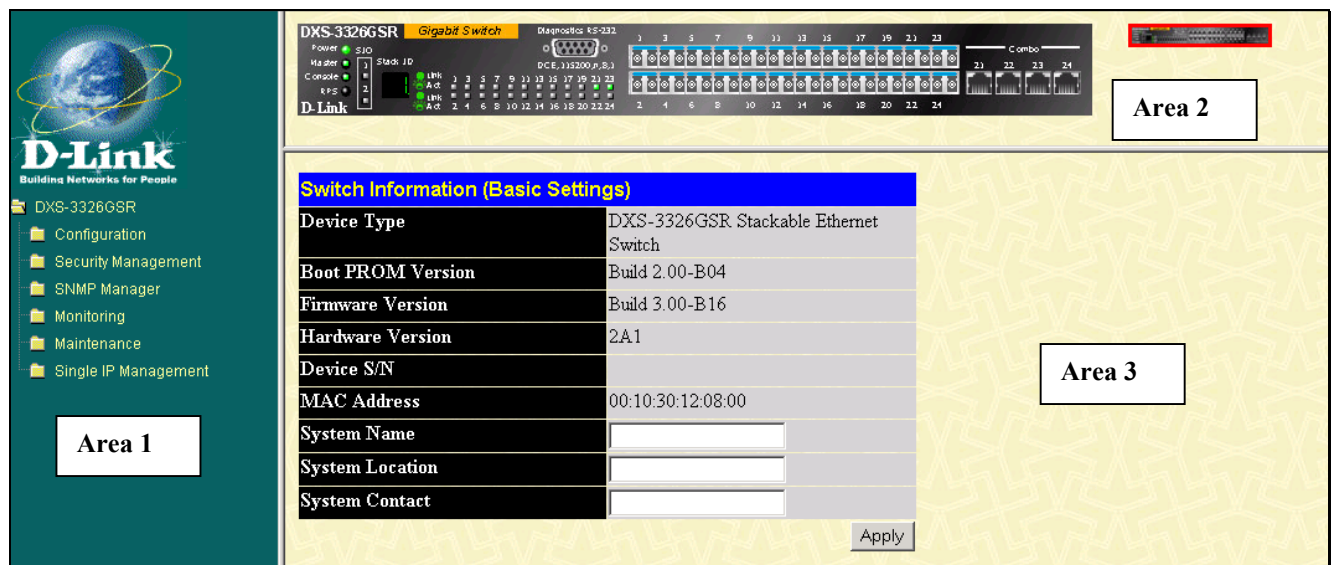
Figure 5- 3. Main Web-Manager page

Area	Function
Area 1	Select the folder or window to be displayed. The folder icons can be opened to display the hyperlinked windows and subfolders contained within them. Click the D-Link logo to go to the D-Link website.
Area 2	Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports and expansion modules, showing port activity, duplex mode, or flow control, depending on the specified mode.

	Various areas of the graphic can be selected for performing management functions, including port configuration.
Area 3	Presents switch information based on your selection and the entry of configuration data.

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

Web Pages

When you connect to the management mode of the Switch with a web browser, a login dialog box is displayed.

Enter a user name and password to access the Switch's management mode.

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

Configuration – Contains windows concerning configuration for Switch Information, IP Address, Box Information, Advanced Settings, Port Configuration, Port Description, Port Mirroring, Link Aggregation, LACP Port Setting, MAC Notification, IGMP Snooping, Spanning Tree, Forwarding & Filtering, VLANs, Traffic Control, Port Security, Port Lock Entries, QoS, System Log Server, SNTP Setting, Access Profile Table, and Port Access Entity.

Layer 3 IP Networking – Contains windows concerning configuration for L3 Global Advanced Settings, IP Interface Table, MD5 Key Table Configuration, Route Redistribution Settings, Static/Default Route, Route Preference Setting, Static ARP Settings, RIP, OSPF, DHCP/BOOTP Relay, DNS Relay, VRRP, and IP Multicast Routing Protocol, among others.

Security Management – Contains windows concerning configuration for Security IP, User Accounts, Access Authentication Control (TACACS), Secure Sockets Layer (SSL), and Secure Shell (SSH).

SNMP Manager – Contains windows concerning SNMP V3, including SNMP User Table, SNMP View Table, SNMP Group Table, SNMP Community Table, SNMP Host Table, and SNMP Engine ID.

Monitoring – Contains windows concerning monitoring the Switch, pertaining to Port Utilization, CPU Utilization, Packets, Errors, Size, Stacking Information, Device Status, MAC Address, IGMP Snooping Group, IGMP Snooping Forwarding, Router Port, Port Access Control, and Layer 3 Features.

Maintenance – Contains windows concerning configuration and information about Switch maintenance, including TFTP Services, Multiple Image Services, Ping Test, Save Changes, Reboot, and Logout.

Single IP Management – Contains windows concerning information on Single IP Management, including SIM Settings, Topology and Firmware/Configuration downloads.

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

Section 6

Configuration

Switch Information

IP Address

Box Information

Advanced Settings

Port Configuration

Port Description

Port Mirroring

Link Aggregation

LACP Port Setting

MAC Notification

MAC Notification Global Settings

MAC Notification Port Settings

IGMP Snooping

IGMP Snooping Settings

Static Router Port Settings

Spanning Tree

STP Bridge Global Settings

MST Configuration Table

MSTI Port Settings

STP Instance Settings

STP Port Settings

Forwarding & Filtering

Unicast Forwarding

Multicast Forwarding

VLANs

Static VLAN Entry

GVRP Setting

Traffic Control

Port Security

Port Lock Entries

QoS

Bandwith Control

QoS Scheduling Mechanism

QoS Output Scheduling

> ***802.1p Default Priority***
>
> ***802.1p User Priority***
>
> ***Traffic Segmentation***
>
> ***System Log Server***
>
> ***SNTP Setting***
>
> ***Time Setting***
>
> ***Time Zone and DST***
>
> ***Access Profile Table***
>
> ***Port Access Entity***
>
> ***Configure Authenticator***
>
> ***Local users***
>
> ***PAE System Control***
>
> ***Port Capability Settings***
>
> ***RADIUS Server***
>
> ***Authentic RADIUS Server***

Switch Information

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.

Click the **Switch Information** link in the **Configuration** folder.

Switch Information (Basic Settings)	
Device Type	DXS-3326GSR Stackable Ethernet Switch
Boot PROM Version	Build 2.00-B04
Firmware Version	Build 3.00-B16
Hardware Version	2A1
Device S/N	
MAC Address	00:10:30:12:08:00
System Name	
System Location	
System Contact	
	Apply

Figure 6- 1. Switch Information (Basic Settings) window

The **Switch Information (Basic Settings)** window shows the Switch's MAC Address (assigned by the factory and unchangeable), the Boot PROM, Firmware Version, and Hardware Version. This information is helpful to keep track of PROM and firmware updates and to obtain the Switch's MAC address for entry into another network device's address table, if necessary. The user may also enter a System Name, System Location and System Contact to aid in defining the Switch, to the user's preference.

IP Address

The IP Address 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 ***DXS-3326GSR Command Line Interface Manual*** or return to Section 4 of this manual for more information.

To change IP settings using the web manager you must access the IP Address menu located in the Configuration folder.

To configure the Switch's IP address:

Open the **Configuration** folder and click the **IP Address** menu link. The web manager will display the Switch's current IP settings in the IP configuration menu, as seen below.

Figure 6- 2. Switch IP Settings window

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

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

2. Enter the appropriate IP Address and Subnet Mask.

3. If you want to access the Switch from a different subnet from the one it is installed on, enter the IP address of the Default 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.

4. If no VLANs have been previously configured on the Switch, you can use the *default* VLAN Name. 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.

> **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 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 IP Address Settings options are:

Parameter	Description
BOOTP	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.
DHCP	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.
Manual	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.
Subnet Mask	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.
Default Gateway	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 gate-way. 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.
VLAN Name	This allows the entry of a VLAN Name 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 here 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 VLAN 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 a management VLAN is specified or Management Station IP Addresses are assigned.

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

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:
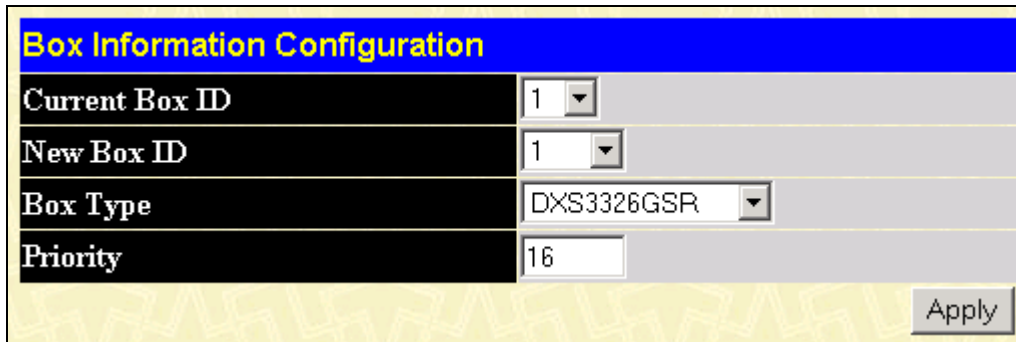
- Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/ yyy.yyy.yyy.yyy.** Where the x's represent the IP address to be assigned to the IP interface named System and the y's represent the corresponding subnet mask.

- 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 which 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.

Box Information

The **Box Information Configuration** window can be found in the **Configuration** folder under the heading **Box Information**:

Figure 6- 3. Box Information Configuration window

This window is used to configure the Master switch of a switch stack. The Master switch is the switch that will be used to configure the software applications regarding the switch stack.

Parameter	Description
Current Box ID	The current Box ID of the Master switch in the stack.
New Box ID	The new box ID of the Master switch in the stack.
Box Type	The user may choose the model name of the Master switch in a stack to be the main configuring switch of that stack.
Priority	Displays the priority ID of the Switch. The lower the number, the higher the priority. The box (switch) with the lowest priority number in the stack is the Master switch.

Information configured in this screen may be found in the **Monitoring** folder under **Stack Information**.

Advanced Settings

The **Switch Information (Advanced Settings)** window contains the main settings for all major functions for the Switch. To view this window, click its link in the **Configuration** folder. This will enable the following window to be viewed and configured.

Figure 6- 4. Switch Information (Advanced Settings) window

Parameter	Description
Serial Port Auto Logout Time	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*. The default setting is *10 minutes*.
Serial Port Baud Rate	The baud rate setting for the Switch is 115,200.
MAC Address Aging Time (10-1000000)	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). To change this, type in a different value representing the MAC address age-out time in seconds. The MAC Address Aging Tim**e** can be set to any value between *10* and *1,000,000* seconds. The default setting is *300* seconds.
IGMP Snooping	To enable system-wide IGMP Snooping capability select *Enabled*. IGMP snooping is *Disabled* 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 IGMP Snooping page under the **IGMP** folder.
Multicast router Only	Enable to support Multicast router only.
GVRP Status	Use this pull-down menu to enable or disable GVRP on the Switch.

Telnet Status	Telnet configuration is *Enabled* by default. If you do not want to allow configuration of the system through Telnet choose *Disabled*.
Telnet TCP Port Number (1-65535)	The Telnet TCP port number. TCP ports are numbered between *1* and *65535*. The "well-known" TCP port for the Telnet protocol is 23.
Web Status	Web-based management is *Enabled* by default. If you choose to disable this by selecting *Disabled*, you will lose the ability to configure the system through the web interface as soon as these settings are applied.
RMON Status	Remote monitoring (RMON) of the Switch is *Enabled* or *Disabled* here.
Link Aggregation Algorithm	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 *MAC Source*, *MAC Destination*, *MAC Src & Dest*, *IP Source, IP Destination* or *IP Src & Dest* (See the Link Aggregation section of this manual).
Switch 802.1x	The user may enable the 802.1x function by port or by MAC address. The default is *Disabled*.
Auth Protocol	The user may use the pull down menu to choose between *radius eap* and *radius pap* for the 802.1x authentication protocol on the Switch. The default setting is *radius eap*.
HOL Prevention	Enables or disables Head Of Line prevention.
Jumbo Frame	Enables or disables support for Jumbo Frames up to 9K bytes.
Syslog state	Enables or disables Syslog State; default is *Disabled*.

Click **Apply** to implement changes made.

Port Configuration

This section contains information for configuring various attributes and properties for individual physical ports, including port speed and flow control. Clicking on **Port Configuration** in the **Configuration** menu will display the following window for the user:

Figure 6- 5. Port Configuration window

To configure switch ports:

1. Choose the unit and the port or sequential range of ports using the Unit and From/To pull-down menus.

2. Use the remaining pull-down menus to configure the parameters described below:

Parameter	Description
State *<Enabled>*	Toggle the State field to either enable or disable a given port or group of ports.
Speed/Duplex *<Auto>*	Toggle the Speed/Duplex field to either select the speed and duplex/half-duplex state of the port. *Auto* denotes auto-negotiation between a range of devices, in 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 *Auto*, *10M/Half*, *10M/Full, 100M/Half, 100M/Full, 1000M/Full_M,* and *1000M/Full_S*. There is no automatic adjustment of port settings with any option other than Auto. The *master* and *slave* parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The *master* setting will allow the port to advertise capabilities related to duplex, speed and physical layer type. The *master* setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a *master* physical layer by a local source. The *slave* setting uses loop timing, where the timing comes form a data stream received from the *master*. If one connection is set for *1000M/Full_M*, the other side of the connection must be set for *1000M/Full_S*. Any other configuration will result in a link down status for both ports
Flow Control	Displays the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and *Auto* ports use an automatic selection of the two. The default is *Disabled*.
Learning	Enable or disable MAC address learning for the selected ports. When *Enabled*, destination and source MAC addresses are automatically listed in the forwarding table. When learning is *Disabled*, MAC addresses must be manually entered into the forwarding table. This is sometimes done for reasons of security or efficiency. See the section on Forwarding and Filtering for information on entering MAC addresses into the forwarding table. The default setting is *Disabled*.

Click **Apply** to implement the new settings on the Switch.

Port Description

The DXS-3326GSR supports a port description feature where the user may name various ports on the Switch. To assign names to various ports, click the **Port Description** on the **Configuration** menu:

Port Description Setting

Unit	From	To	Description	Apply
1 ▾	Port 1 ▾	Port 1 ▾		Apply

Port Description Table-Unit 1

Port	Description
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	

Figure 6- 6. Port Description Setting window

Use the Unit and From/To pull-down menus to choose a unit and port or range of ports to describe, and then enter a description of the port(s). Click **Apply** to set the descriptions in the Port Description Table.

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. This is useful for network monitoring and troubleshooting purposes. To view the **Port Mirroring** window, click **Port Mirroring** in the **Configuration** folder.

Figure 6- 7. Setup Port Mirroring window

To configure a mirror port:

- Select the Unit and Source Port from where you want to copy frames and the Target Port, which receives the copies from the source port.

- Select the Source Direction, Ingress, Egress, or Both and 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.

Link Aggregation

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline.

The DXS-3326GSR supports up to 32 port trunk groups with two to eight ports in each group. This includes link aggregation groups that spread over multiple switches in the switch stack.
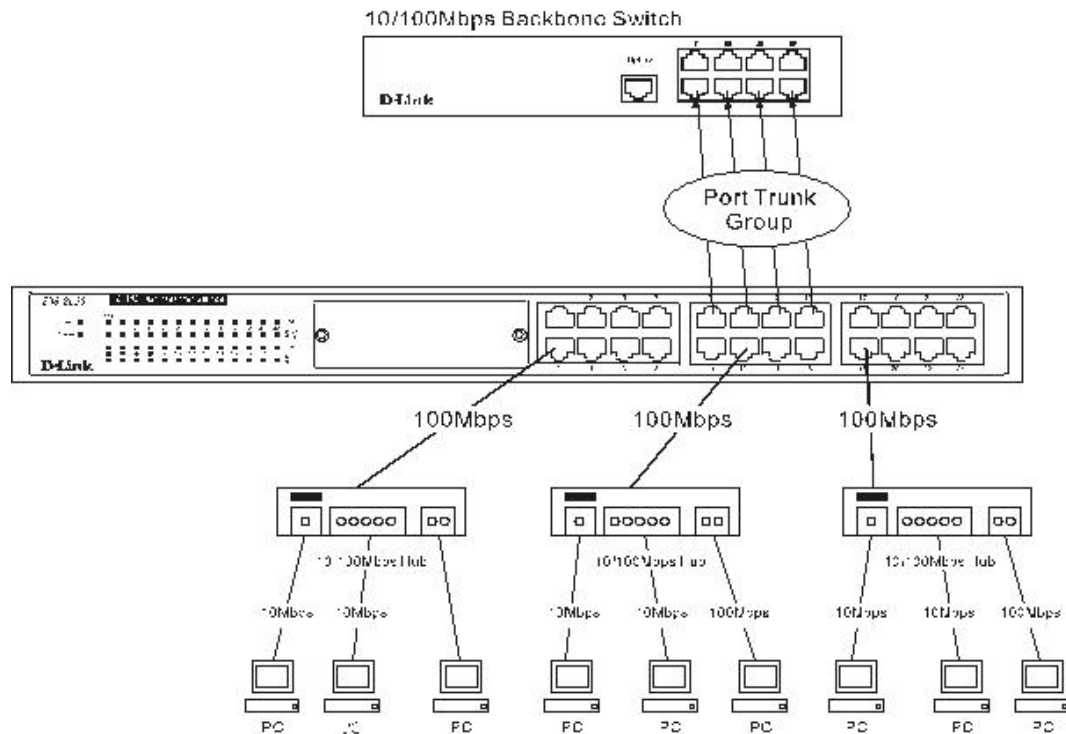
Figure 6- 8. Example of Port Trunk Group

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

> **NOTE:** If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load-shared among the other uplinked ports of the link aggregation group.

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

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

The Switch allows the creation of up to 32 link aggregation groups, each group consisting of 2 to 8 links (ports). All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control, traffic segmentation and 802.1p default priority configurations must be identical. Port locking, port mirroring and 802.1X must not be enabled on the trunk group. Further, the aggregated links must all be of the same speed and should be configured as full-duplex.

The Master Port of the group is to be configured by the user, 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 **Link Aggregation** hyperlink in the **Configuration** folder to bring up the **Port Link Aggregation Group** table:

Figure 6- 9. Current Link Aggregation Group Entries window

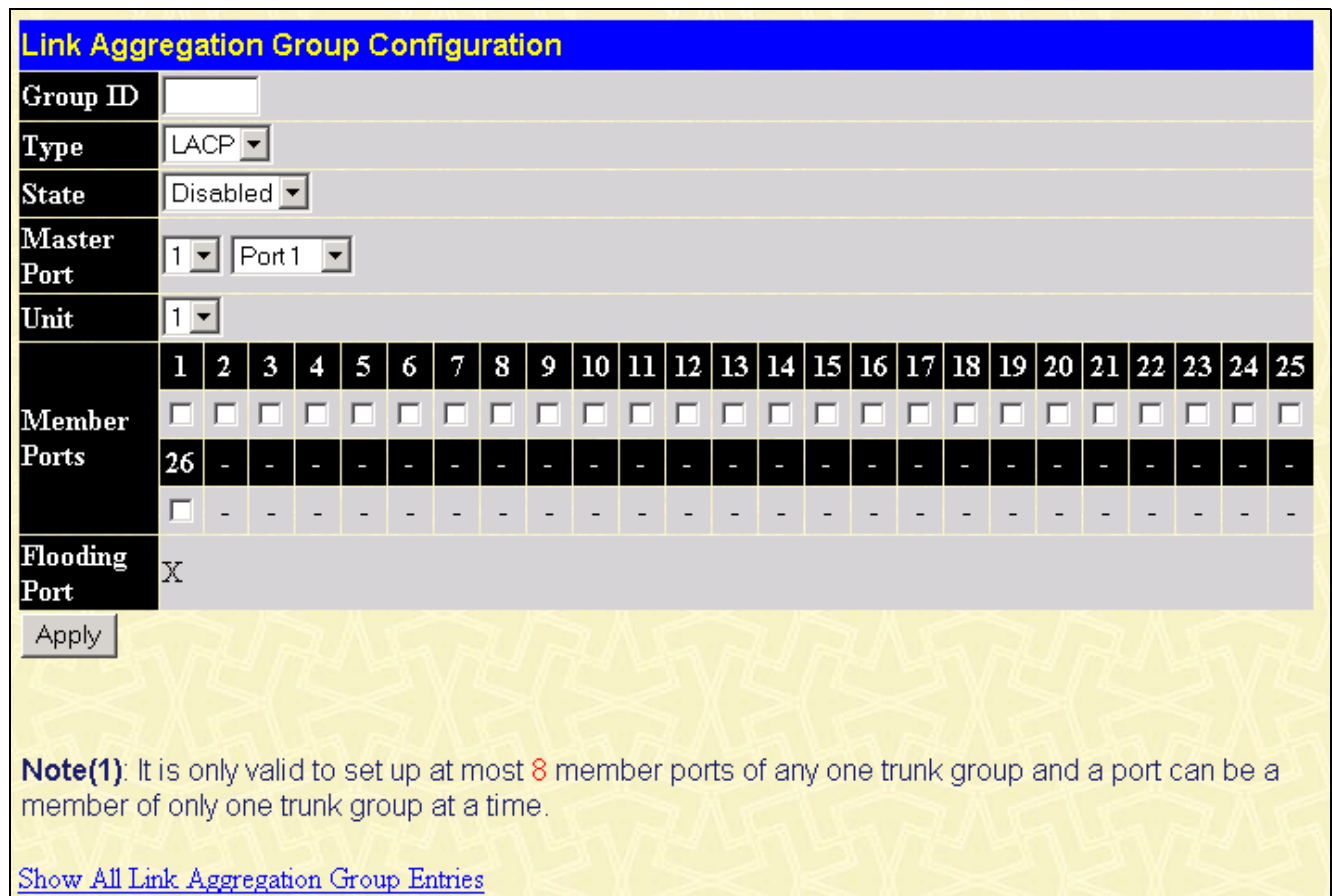To configure port trunk groups, click the **Add** button to add a new trunk group and use the **Link Aggregation Group Configuration** window (see example below) to set up trunk groups. To modify a port trunk group, click the **Modify** button corresponding to the entry you wish to alter. To delete a port trunk group, click the corresponding ✕ under the **Delete** heading in the Current Link Aggregation Group Entries table.

Figure 6- 10. Link Aggregation Group Configuration window

The user-changeable parameters are as follows:

Parameter	Description
Group ID	Select an ID number for the group.
Type	This pull-down menu allows you to select between *Static* and *LACP* (Link Aggregation Control Protocol). LACP allows for the automatic detection of links in a Port Trunking Group.
State	Trunk groups can be toggled between *Enabled* and *Disabled*. 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.

44

Master Port	Choose the Master Port for the trunk group using the pull-down menu.
Unit	Choose the Unit for the trunk group using the pull-down menu.
Member Ports	Choose the members of a trunked group. Up to 8 ports per group can be assigned to a group.
Flooding Port	A trunking group must designate one port to allow transmission of broadcasts and unknown unicasts.

After setting the previous parameters, click **Apply** to allow your changes to be implemented. Successfully created trunk groups will be shown in the **Current Link Aggregation Group Entries** window.

LACP Port Setting

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

Figure 6- 11. LACP Port Setting window

The user may set the following parameters:

Parameter	Description
Unit	Choose the desired Unit.
From/To	A consecutive group of ports may be configured starting with the selected port.
Mode	*Active* - 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. *Passive* - 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, one end of the connection must have "active" LACP ports (see above).

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.

MAC Notification

MAC Notification is used to monitor MAC addresses learned and entered into the forwarding database.

MAC Notification Global Settings

To globally set MAC notification on the Switch, open the following window by opening the **MAC Notification** folder and clicking the **MAC Notification Global Settings** link:

Figure 6- 12. Current MAC Notification Global Setting window

The following parameters may be modified:

Parameter	Description
State	Enable or disable MAC notification globally on the Switch
Interval (1-2147483647sec)	The time in seconds between notifications.
History size (1-500)	The maximum number of entries listed in the history log used for notification. Up to *500* entries can be specified.

MAC Notification Port Settings

To change MAC notification settings for a port or group of ports on the Switch, click **Port Settings** in the **MAC Notification** folder, which will display the following window:

MAC Notification Port Settings				
Unit	**From**	**To**	**State**	**Apply**
1 ▾	Port 1 ▾	Port 1 ▾	Disabled ▾	Apply

MAC Notification Port State Table-Unit 1	
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
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled

Figure 6- 13. MAC Notification Port Settings window

The following parameters may be set:

Parameter	Description
Unit	Choose the desired unit.
From…To	Select a port or group of ports to enable for MAC notification using the pull-down menus.
State	Enable MAC Notification for the ports selected using the pull-down menu.

Click **Apply** to implement changes made.

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can open or close a port to a specific device based on IGMP messages passing through the Switch.

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** link in the **Configuration** folder. 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 Settings

Use the first **IGMP Snooping Settings** window to view IGMP Snooping settings. To modify the settings, click the **Modify** button of the VLAN ID you want to change.

Figure 6- 14. first IGMP Snooping Settings window

Clicking the **Modify** button will open the second **IGMP Snooping Settings** window, shown below:

Figure 6- 15. second IGMP Snooping Settings window

The following parameters may be viewed or modified:

Parameter	Description
VLAN ID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to modify the IGMP Snooping Settings for.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to modify the IGMP Snooping Settings for.
Query Interval (1-65535 sec)	The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between *1* and *65535* seconds are allowed. Default = *125*.
Max Response Time (1-25 sec)	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). Default = *10*.
Robustness Value (1-255)	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Value should be increased to accommodate increased packet loss. This entry field allows an entry of *1* to *255*. Default = *2*.
Last Member Query Interval (1-25 sec)	This field specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. Default = *1*.
Host Timeout (1-16711450 sec)	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. Default = *260*.
Router Timeout (1-16711450)	This is the maximum amount of time in seconds a route is kept in the forwarding table without receiving a membership report. Default = *260*.

Leave Timer (1-16711450)	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.
Querier State	Choose *Enabled* to enable transmitting IGMP Query packets or *Disabled* to disable. The default is *Disabled*.
Querier Router Behavior	This indicates the current querier router behavior.
State	Select *Enabled* to implement IGMP Snooping. This field is *Disabled* by default.

Click **Apply** to implement the new settings. Click the Show All IGMP Group Entries link to return to the first **IGMP Snooping Settings** window.

Static Router Port Settings

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 a 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 or PIM-DM multicast packets are detected flowing into a port.

Open the **IGMP Snooping** folder and the click on the **Static Router Ports Settings** link to open the **Static Router Port Settings** window, as shown below.

Figure 6- 16. Static Router Port Settings window

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

Figure 6- 17. Static Router Ports Settings window

The following parameters can be set:

Parameter	Description
VID (VLAN ID)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN where the multicast router is attached.
VLAN Name	This is the name of the VLAN where the multicast router is attached.
Unit	This is the unit where the multicast router is attached.
Member Ports	There are the ports on the Switch that will have a multicast router attached to them.

Click **Apply** to implement the new settings, Click the Show All Static Router Ports Entries link to return to the **Static Router Port Settings** window.

Spanning Tree

This Switch supports three versions of the Spanning Tree Protocol; 802.1d STP, 802.1w Rapid STP, and 802.1s MSTP. 802.1d STP will be familiar to most networking professionals. However, since 802.1w RSTP and 802.1s MSTP 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, 802.1w RSTP and 802.1s MSTP.

802.1s MSTP

Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing any of the three spanning tree protocols (STP, RSTP or MSTP).

This protocol will also tag BDPU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs asscociated with them. These instances will be classified by an MSTI ID. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established

regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees.

Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

1. A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **Current MST Configuration Identification** window (**Configuration** > **Spanning Tree** > **MST Configuration Table**) in the Configuration Name field).

2. A configuration revision number (identified here as a Revision Level and found in the **Current MST Configuration Identification** window and;

3. A 4096-element table (defined here as a VID List in the **Current MST Configuration Identification** window which will associate each of the possible 4096 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

1. The Switch must be set to the MSTP setting (found in the **STP Bridge Global Settings** window in the STP Version field)

2. The correct spanning tree priority for the MSTP instance must be entered (defined here as a Priority in the **STP Instance Table** window (**Configuration** > **Spanning Tree** > **STP Instance Settings**) when configuring an MSTI ID settings).

3. VLANs that will be shared must be added to the MSTP Instance ID (defined here as a VID List in the **Current MST Configuration Identification** window when configuring an MSTI ID settings).

802.1w Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE 802.1s, 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 functions 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 three protocols is in the way ports transition to a forwarding state and in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. MSTP and RSTP combine 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/MSTP port state discarding, there is no functional difference, the port is not active in the network topology. Table 6-1 below compares how the three protocols differ regarding the port state transition.

All three 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 is sensitive to the status of the link. Ultimately this difference results in 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 MSTP	802.1w RSTP	802.1d STP	Forwarding	Learning
Discarding	Discarding	Disabled	No	No
Discarding	Discarding	Blocking	No	No
Discarding	Discarding	Listening	No	No
Learning	Learning	Learning	No	Yes
Forwarding	Forwarding	Forwarding	Yes	Yes

Table 6- 1. Comparing Port States

RSTP is capable of a 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/MSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

802.1d/802.1w/802.1s Compatibility

MSTP or RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1d format when necessary. However, any segment using 802.1d STP will not benefit from the rapid transition and rapid topology change detection of MSTP or 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 or MSTP.

The Spanning Tree Protocol (STP) operates on two levels:

1. On the switch level, the settings are globally implemented.

2. On the port level, the settings are implemented on a per user-defined group of ports basis.

STP Bridge Global Settings

To open the following window, open the **Spanning Tree** folder in the **Configuration** folder and click the **STP Bridge Global Settings** link.

Figure 6- 18. STP Bridge Global Settings window

The following parameters can be set:

Parameter	Description
STP Status	Use the pull-down menu to enable or disable STP globally on the Switch. The default is *Disabled*.
STP Version	Use the pull-down menu to choose the desired version of STP to be implemented on the Switch. There are three choices: *STP* - Select this parameter to set the Spanning Tree Protocol (STP) globally on the switch. *RSTP* - Select this parameter to set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *MSTP* - Select this parameter to set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.
Hello Time (1 - 10 Sec) *<2>*	The Hello Time can be set from *1* to *10* seconds. In STP, 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. In RSTP, this configuration message is sent by the Designated Port each Hello Time. This field will only appear here when STP or RSTP is selected for the STP Version. For MSTP, the Hello Time must be set on a port per port basis. See the MST Port Settings section for further details.
Max Age (6 - 40 Sec) *<20>*	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the 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. The user may choose a time between *6* and *40* seconds. The default value is *20*.
Forward Delay (4 - 30 Sec) *<15 >*	The Forward Delay can be from *4* to *30* seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the for-warding state.

Max Hops (1-20) *<20>*	Used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out. The user may set a hop count from *1* to *20*. The default is *20*.
TX Hold Count (1-10) *<3>*	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default is *3*.
Forwarding BPDU *<Enabled >*	This field can be *Enabled* or *Disabled.* When *Enabled,* it allows the forwarding of STP BPDU packets from other network devices. The default is *Enabled*.

Click **Apply** to implement changes made.

NOTE: The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur. Observe the following formulas when setting the above parameters:

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

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

MST Configuration Table

The following windows in the **Current MST Configuration Identification** window allow the user to configure a MSTI instance on the Switch. These settings will uniquely identify a multiple spanning tree instance set on the Switch. The Switch initially possesses one *CIST* or Common Internal Spanning Tree of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted. To view the **Current MST Configuration Identification** window, click **Configuration > Spanning Tree > MST Configuration Table**:

Figure 6- 19. Current MST Configuration Identification window

The window above contains the following information:

Parameter	Description
Configuration Name	A name that uniquely identifies the MSTI (Multiple Spanning Tree Instance). If a configuration name is not set, this field will show the MAC address to the device running MSTP.

Revision Level	This value, along with the Configuration Name, identifies the MSTP region configured on the Switch.
MSTI ID	This field shows the MSTI IDs currently set on the Switch. This field will always have the CIST MSTI, which may be configured but not deleted. Clicking the hyperlinked name will open a new window for configuring parameters associated with that particular MSTI.
VID List	This field displays the VLAN IDs associated with the specific MSTI.

Clicking the **Add** button will reveal the following window to configure:

Figure 6- 20. Instance ID Settings window

The user may configure the following parameters to create a MSTI in the Switch.

Parameter	Description
MSTI ID	Enter a number between *1* and *15* to set a new MSTI on the Switch.
Type	*Create* is selected to create a new MSTI. No other choices are available for this field when creating a new MSTI.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number *1* to *4094*.

Click **Apply** to implement changes made.

To configure the settings for the CIST, click on its hyperlinked name in the **Current MST Configuration Identification** window, which will reveal the following window to configure:

Figure 6- 21. Instance ID Settings window

The user may configure the following parameters to configure the CIST on the Switch.

Parameter	Description
MSTI ID	The MSTI ID of the CIST is 0 and cannot be altered.
Type	The type of configuration about to be processed. This window is used to add or delete VIDs to the configured MSTI or internal CIST. All other parameters are permanently set and therefore unchangeable.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number *1* to *4094*. This field is inoperable when configuring the CIST.

Click **Apply** to implement changes made.

To configure the parameters for a previously set MSTI, click on its hyperlinked MSTI ID number, which will reveal the following window for configuration.

Figure 6- 22. Instance ID Settings window

The user may configure the following parameters for a MSTI on the Switch.

Parameter	Description
MSTI ID	Displays the MSTI ID previously set by the user.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has two choices. • *Add VID* - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. • *Remove VID* - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch that the user wishes to add to this MSTI ID. Supported VIDs on the Switch range from ID number 1 to 4094. This parameter can only be utilized if the Type chosen is *Add VID* or *Remove VID*.

Click **Apply** to implement changes made.

MSTI Port Settings

This window displays the current MSTI configuration settings and can be used to update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest port number into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.

To view the following window, click **Configuration > Spanning Tree > MSTI Port Settings**:

Figure 6- 23. MSTI Port Information window

To view the MSTI settings for a particular port, select the Port number, located in the top left hand corner of the window and click **Apply**. To modify the settings for a particular MSTI Instance, click on its hyperlinked MSTI ID, which will reveal the following window.

Figure 6- 24. MSTI Settings window

Parameter	Description
Instance ID *<0>*	Displays the MSTI ID of the instance being configured. An entry of *0* in this field denotes the CIST (default MSTI).
Internal cost (0=Auto) *<200000>*	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is *0* (auto). There are two options: • *0 (auto)* - Selecting this parameter for the *internalCost* will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. • *value 1-2000000* - Selecting this parameter with a value in the range of 1-2000000 will set the quickest route when a loop occurs. A lower Internal cost represents a quicker transmission.
Priority *<128>*	Enter a value between *0* and *240* to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.

Click **Apply** to implement changes made.

STP Instance Settings

The following window displays MSTIs currently set on the Switch. To view the following table, click **Configuration > Spanning Tree > STP Instance Settings**:

Figure 6- 25. STP Instance Table window

The following information is displayed:

Parameter	Description
Instance Type	Displays the instance type(s) currently configured on the Switch. Each instance type is classified by an MSTI ID. CIST refers to the default MSTI configuration set on the Switch.
Instance Status	Displays the current status of the corresponding MSTI ID.
Instance Priority	Displays the priority of the corresponding MSTI ID. The lowest priority will be the root bridge.

Click **Apply** to implement changes made.

To make changes to entries on the **STP Instance Table** window, click **Modify**:

Figure 6- 26. Instance ID Settings window

The following information is displayed:

Parameter	Description
MSTI ID	Enter the Instance Type, which is classified by an MSTI ID.
Type	*Set Priority Only* is selected to create a new priority. No other choices are available for this field.
Priority (0-61440)	Select a value between *0* and *61440* to specify the priority for a specified MSTI for forwarding packets. The lower the value, the higher the priority. This entry must be divisible by 4094

STP Port Settings

STP can be set up on a port per port basis. To view the following window click **Configuration > Spanning Tree > STP Port Settings**:

STP Port Settings

Unit	From	To	External Cost (0=Auto)	Hello Time	Migrate	Edge	P2P	State
1 ▼	Port 1 ▼	Port 1 ▼	0		Yes ▼	False ▼	True ▼	Enabled ▼

Apply

STP Port Information Table-Unit 1

Port	External Cost	Hello Time	Edge	P2P	Port STP
1	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
2	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
3	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
4	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
5	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
6	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
7	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
8	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
9	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
10	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
11	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
12	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
13	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
14	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
15	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
16	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
17	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
18	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
19	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
20	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
21	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
22	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
23	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
24	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
25	AUTO/200000	2/2	No/No	Auto/Yes	Enabled
26	AUTO/200000	2/2	No/No	Auto/Yes	Enabled

Figure 6- 27. 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 based on 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:

Parameter	Description
Unit	Choose the desired unit.
From/To *<Port 1>*	A consecutive group of ports may be configured starting with the selected port.
External Cost *< 0 = Auto>*	External Cost - This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0(auto). • *0 (auto)* - Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. • *value 1-200000000* - Define a value between *1* and *200000000* to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.
Hello Time *<2>*	The time interval between the transmission of configuration messages by the designated port, to other devices on the bridged LAN, thus stating that the Switch is still functioning. The user may choose a time between *1* and *10* seconds. The default is 2 seconds. This field is only operable when the Switch is enabled for MSTP.
Migration *<Yes>*	Setting this parameter as "*yes*" will set the ports to send out BDPU packets to other bridges, requesting information on their STP setting If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP to 802.1w RSTP. If the Switch is configured for MSTP, the port is capable of migrating from 802.1d STP to 802.1s MSTP. RSTP and MSTP can coexist with standard STP, however the benefits of RSTP and MSTP are not realized on a port where an 802.1d network connects to an 802.1w or 802.1s enabled network. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP or 802.1s MSTP on all or some portion of the segment.
Edge *<False>*	Choosing the true parameter 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. Choosing the false parameter indicates that the port does not have edge port status.
P2P *<True>*	Choosing the *True* parameter indicates a point-to-point (P2P) shared link. P2P ports 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. A p2p value of *False* indicates that the port cannot have p2p status. *Auto* allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *False*. The default setting for this parameter is

	True.
State *<Disabled>*	This drop-down menu allows you to enable or disable STP for the selected group of ports. The default is *Enabled*.

Click **Apply** to implement changes made.

Forwarding & Filtering

Unicast Forwarding

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

Figure 6- 28. Setup Static Unicast Forwarding Table window

To add or edit an entry, define the following parameters and then click **Add/Modify**:

Parameter	Description
VLAN ID (VID)	The VLAN ID number of the VLAN on which the above Unicast MAC address resides.
MAC Address	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
Unit	Choose the desired Unit.
Port	Allows the selection of the port number on which the MAC address entered above resides.

Click **Apply** to implement the changes made. To delete an entry in the Static Unicast Forwarding Table, click the corresponding ✕ under the **Delete** heading.

Static 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 6- 29. Static Multicast Forwarding Settings window

This 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:

Figure 6- 30. Setup Static Multicast Forwarding Table window

The following parameters can be set:

Parameter	Description
Unit	Choose the desired unit.
VID	The VLAN ID of the VLAN the corresponding MAC address belongs to.
Multicast MAC Address	The MAC address of the static source of multicast packets. This must be a multicast MAC address.
Port Settings	Allows the selection of ports that will be members of the static multicast group. The options are: *None* - No restrictions on the port dynamically joining the multicast group. When *None* is chosen, the port will not be a member of the Static Multicast Group. *Egress* - The port is a static member of the multicast group.

Click **Apply** to implement the changes made. To delete an entry in the Static Multicast Forwarding Table, click the corresponding under the **Delete** heading. Click the Show All Multicast Forwarding Entries link to return to the **Static Multicast Forwarding Settings** window.

64

VLANs

Understanding IEEE 802.1p Priority

Priority tagging is a function defined by the IEEE 802.1p standard designed to provide a means of managing traffic on a network where many different types of data may be transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time critical data over congested networks. The quality of applications that are dependent on such time critical data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

Network devices that are in compliance with the IEEE 802.1p standard have the ability to recognize the priority level of data packets. These devices can also assign a priority label or tag to packets. Compliant devices can also strip priority tags from packets. This priority tag determines the packet's degree of expeditiousness and determines the queue to which it will be assigned.

Priority tags are given values from 0 to 7 with 0 being assigned to the lowest priority data and 7 assigned to the highest. The highest priority tag 7 is generally only used for data associated with video or audio applications, which are sensitive to even slight delays, or for data from specified end users whose data transmissions warrant special consideration.

The Switch allows you to further tailor how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows you to specify its relative priority to suit the needs of your network. There may be circumstances where it would be advantageous to group two or more differently tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 1, be reserved for data packets with a priority value of 7. Packets that have not been given any priority value are placed in Queue 0 and thus given the lowest priority for delivery.

A weighted round robin system is employed on the Switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 1, will clear 4 packets for every 1 packet cleared from Queue 0.

Remember, the priority queue settings on the Switch are for all ports, and all devices connected to the Switch will be affected. This priority queuing system will be especially beneficial if your network employs switches with the capability of assigning priority tags.

VLAN Description

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

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

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

Notes About VLANs on the DXS-3326GSR

No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.

The DXS-3326GSR supports IEEE 802.1Q VLANs and Port-Based VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.

The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."

The "default" VLAN has a VID = 1.

The member ports of Port-based VLANs may overlap, if desired.

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

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

VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will only deliver packets between stations that are members of the VLAN.

Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLANs allows 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-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

The IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN the receiving port is a member of.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns packets to VLANs by filtering.

- Assumes the presence of a single global spanning tree.

- Uses an explicit tagging scheme with one-level tagging.

- 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 whether to filter or forward the packet.

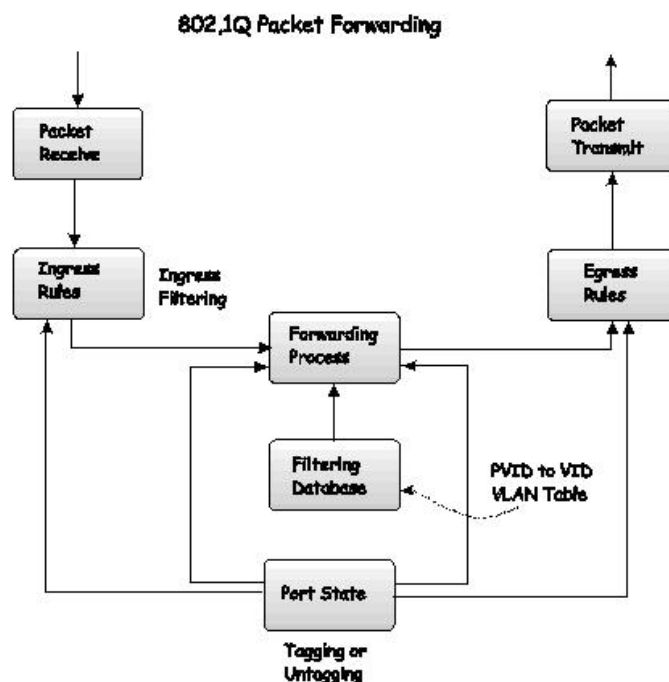- Egress rules - determines if the packet must be sent tagged or untagged.

Figure 6- 31. IEEE 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 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLANs can be identified.

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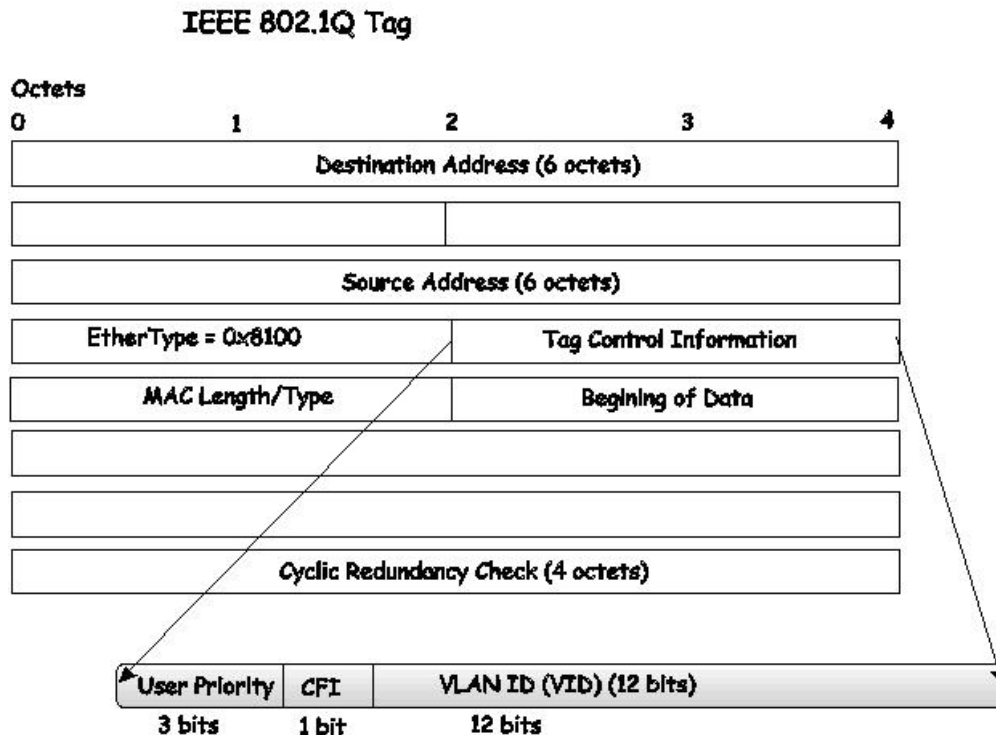

Figure 6- 32. IEEE 802.1Q Tag

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.
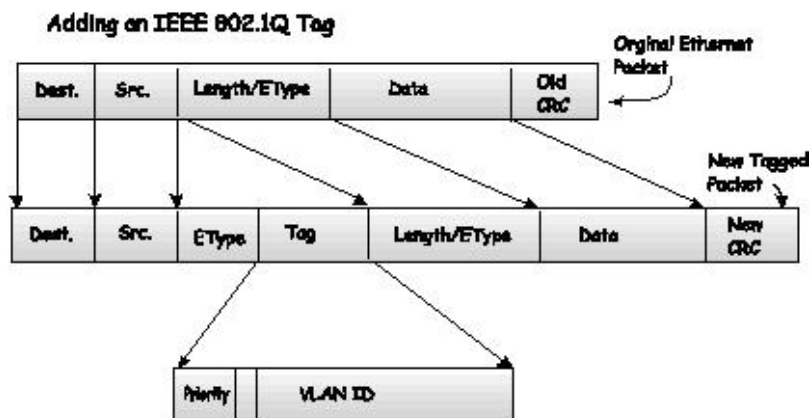

Figure 6- 33. Adding an IEEE 802.1Q Tag

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 of 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.

Default VLANs

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

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

NOTE: If no VLANs are configured on the Switch, then all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4

Table 6- 2. VLAN Example - Assigned Ports

Port-based VLANs

Port-based VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLANs, NICs do not need to be able to identify 802.1Q tags in packet headers. NICs send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet gets dropped by the Switch or delivered.

VLAN Segmentation

Take for example a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2. If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If Port 10 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2.

Network resources such as printers and servers however, can be shared across VLANs. This is achieved by setting up overlapping VLANs. That is ports can belong to more than one VLAN group. For example, setting VLAN 1 members to ports 1, 2, 3, and 4 and VLAN 2 members to ports 1, 5, 6, and 7. Port 1 belongs to two VLAN groups. Ports 8, 9, and 10 are not configured to any VLAN group. This means ports 8, 9, and 10 are in the same VLAN group.

VLAN and Trunk Groups

The members of a trunk group have the same VLAN setting. Any VLAN setting on the members of a trunk group will apply to the other member ports.

> **NOTE:** In order to use VLAN segmentation in conjunction with port trunk groups, you can first set the port trunk group(s), and then you may configure VLAN settings. If you wish to change the port trunk grouping with VLANs already in place, you will not need to reconfigure the VLAN settings after changing the port trunk group settings. VLAN settings will automatically change in conjunction with the change of the port trunk group settings.

Protocol VLANs

The DXS-3326SGR incorporates the idea of protocol-based VLANs. This standard, defined by the IEEE 802.1v standard maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. After assessing the protocol, the Switch will forward the packets to all ports within the protocol-assigned VLAN. This feature will benefit the administrator by better balancing load sharing and enhancing traffic classification. The Switch supports fifteen pre-defined protocols for configuration. The user may also choose a protocol that is not one of the fifteen defined protocols by properly configuring the *userDefined* protocol VLAN. The supported protocols for the protocol VLAN function on this switch include IP, IPX, DEC, DEC LAT, SNAP, NetBIOS, AppleTalk, XNS, SNA, IPv6, RARP and VINES.

The following is a list of type headers for each protocol listed for VLAN configuration.
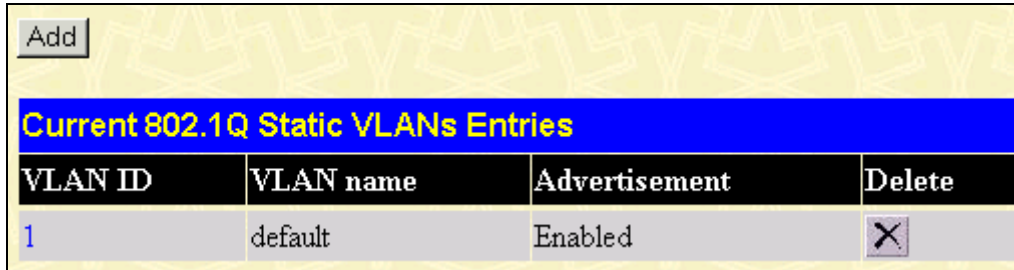
Protocol	Type Header in Hexidecimal Form
IP over Ethernet	0x0800
IPX 802.3	0xFFFF
IPX 802.2	0xE0E0
IPX SNAP	0x8137
IPX over Ethernet2	0x8137
decLAT	0x6000
decOther	0x6009
SNA 802.2	0x0404
netBios	0xF0F0
XNS	0x0600
VINES	0x0BAD
IPV6	0x86DD
AppleTalk	0x809B
RARP	0x8035

Table 6- 3. Protocol VLAN and the Corresponding Type Header

In configuring the user-defined protocol, the administrator must make sure that the pre-defined user type header does not match any other type header. A match may cause discrepancies within the local network and failure to define the VLAN to forward packets to.

Static VLAN Entry

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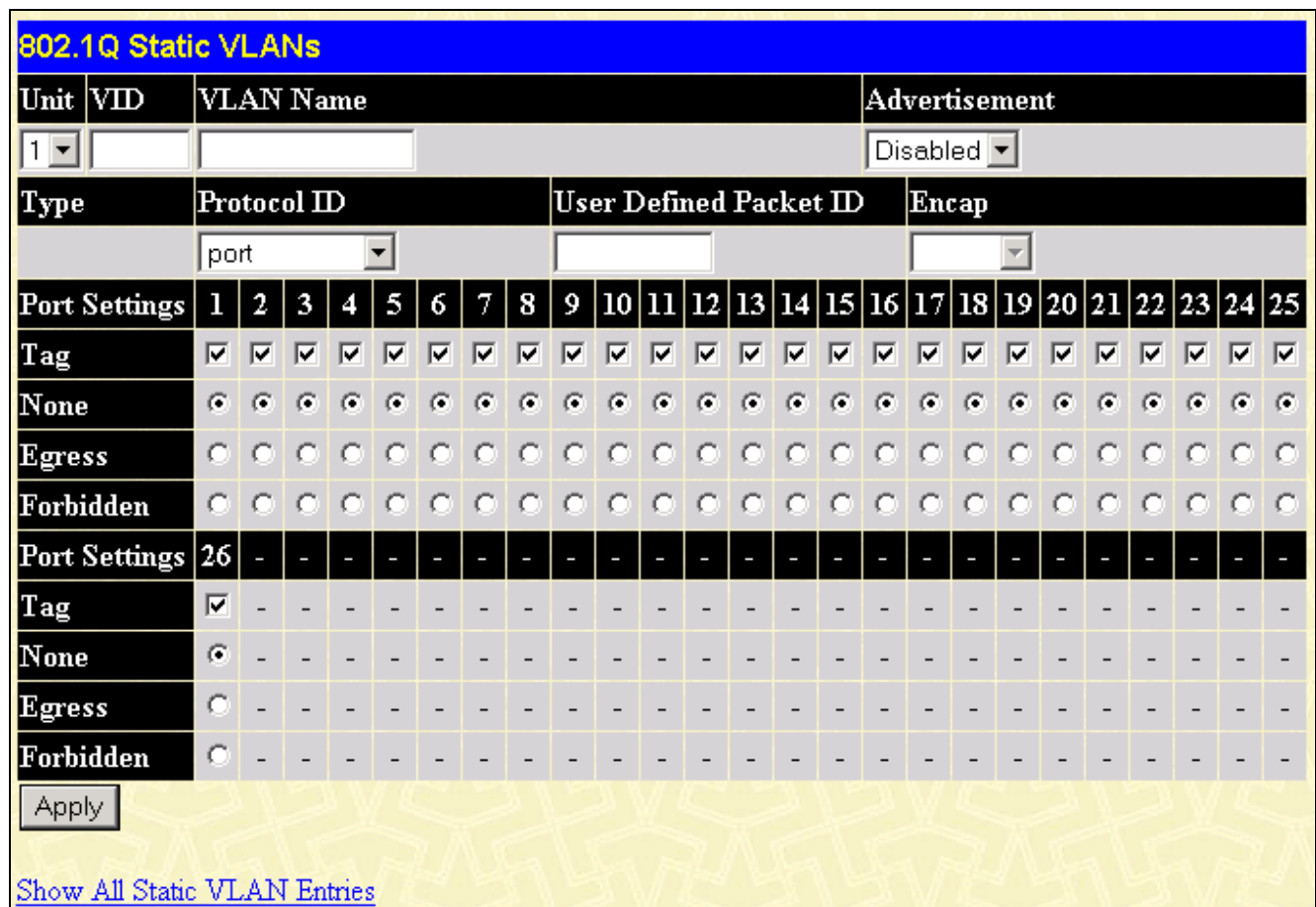

Figure 6- 34. Current 802.1Q Static VLANs Entries window

This window lists all previously configured VLANs by VLAN ID and VLAN Name. To delete an existing 802.1Q VLAN, click the corresponding ✕ button under the **Delete** heading.

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

Figure 6- 35. 802.1Q Static VLANs window

To return to the **Current 802.1Q Static VLANs Entries** window, click the Show All Static VLAN Entries link. To change an existing 802.1Q VLAN entry, click the **Modify** button of the corresponding entry you wish to modify. A new window will appear 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.

71

The following fields can then be set:

Parameter	Description
Unit	Choose the desired Unit.
VID (VLAN ID)	Allows the entry of a VLAN ID in the Add dialog box, or displays the VLAN ID of an existing VLAN in the Modify dialog box. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allows the entry of a name for the new VLAN in the Add dialog box, or for editing the VLAN name in the Modify dialog box.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Protocol ID	The following parameters allow for the creation of protocol-based VLANs. The switch supports 15 pre-configured protocol-based VLANs plus one user-defined protocol based VLAN where the administrator may configure the settings for the appropriate protocol and forwarding of packets (16 total). Selecting a specific protocol will indicate which protocol will be utilized in determining the VLAN ownership of a tagged packet. Pre-set protocol-based VLANs on the switch include: *port* – Using this parameter will allow the creation of a normal 802.1Q VLAN on the Switch. *ip* – Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is based on the Ethernet protocol. *rarp* - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Reverse Address Resolution (RARP) Protocol. *ipx802dot3* - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by Novell NetWare 802.3 (IPX - Internet Packet Exchange). *ipx802dot2* - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by Novell NetWare 802.2 (IPX - Internet Packet Exchange). *ipxSnap* - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by Novell and the Sub Network Access Protocol (SNAP). *ipxEthernet2* - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Ethernet Protocol. *appleTalk* - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the AppleTalk protocol. *decLAT* - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Digital Equipment Corporation (DEC) Local Area Transport (LAT) protocol. *decOther* - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Digital Equipment Corporation (DEC) Protocol. *sna802dot2* - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header

	information is defined by the Systems Network Architecture(SNA) 802.2 Protocol.
	netBios - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the NetBIOS Protocol.
	xns - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Xerox Network Systems (XNS) Protocol.
	vines - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Banyan Virtual Intergrated Network Service (VINES) Protocol.
	ipV6 - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Internet Protocol Version 6 (IPv6) Protocol.
	userDefined - Using this parameter will instruct the switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol defined by the user. This packet header information is defined by entering the following information:
User Defined Packet ID	Specifies that the VLAN will only accept packets with this hexadecimal 802.1Q Ethernet type value in the packet header. The user may define an entry, in the hexidecimal form (ffff) to define the packet identification. *(The user only need enter the final four integers of the hexidecimal format to define the packet ID – {hex 0x0 0xffff})* This field is only operable if *userDefined* is selected in the Protocol ID field.
Encap	Specifies that the switch will examine the octet of the packet header referring to one of the protocols listed (Ethernet, LLC or SNAP), looking for a match of the hexidecimal value previously entered. *All* will instruct the Switch to examine the total packet header. After a match is found, the Switch will forward the packet to this VLAN. This field is only operable if *userDefined* is selected in the Protocol ID field
Port Settings	Allows an individual port to be specified as member of a VLAN.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagged. Checking the box will designate the port as Tagged.
None	Allows an individual port to be specified as a non-VLAN member.
Egress	Select this to specify the port as a static member of the VLAN. Egress member ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.
Forbidden	Select this to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

Click **Apply** to implement changes made.

GVRP Setting

In the **Configuration** menu, open the **VLANs** folder and click **GVRP Setting**.

The **GVRP Settings** window, shown below, allows you to determine whether the Switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (GVRP) enabled switches. In addition, Ingress Checking can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port. Results can be seen in the table under the configuration settings, as seen below.

Figure 6- 36. GVRP Settings window

The following fields can be set:

Parameter	Description
Unit	Choose the desired unit.
From/To	These two fields allow you to specify the range of ports that will be included in the Port-based VLAN that you are creating using the **GVRP Settings** window.

	Port-based VLAN that you are creating using the **GVRP Settings** window.
GVRP	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is *Disabled* by default.
Ingress Check	This field can be toggled using the space bar between *Enabled* and *Disabled*. *Enabled* 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. *Disabled* disables ingress filtering. Ingress Checking is *Disabled* by default.
Acceptable Frame Type	This field denotes the type of frame that will be accepted by the port. The user may choose between *Tagged Only*, which means only VLAN tagged frames will be accepted, and *Admit_All*, which means both tagged and untagged frames will be accepted. *Admit_All* is enabled by default.
PVID	This field shows the current PVID assignment for each port, which may be manually assigned to a VLAN when created in the 802.1Q Port Settings table. The Switch's default is to assign all ports to the default VLAN with a VID of 1.The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If a packet is received by the port, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.

Click **Apply** to implement changes made.

Traffic Control

Use the **Traffic Control** 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. To view the following window, click **Configuration > Traffic Control**:

Traffic Control Settings							
Unit	From	To	Broadcast Storm	Multicast Storm	Destination Lookup Fail	Threshold	Apply
1 ▼	Port 1 ▼	Port 1 ▼	Disabled ▼	Disabled ▼	Disabled ▼	128	Apply

Traffic Control Table-Unit 1				
Port	Broadcast Storm	Multicast Storm	Destination Lookup Fail	Threshold
1	Disabled	Disabled	Disabled	128
2	Disabled	Disabled	Disabled	128
3	Disabled	Disabled	Disabled	128
4	Disabled	Disabled	Disabled	128
5	Disabled	Disabled	Disabled	128
6	Disabled	Disabled	Disabled	128
7	Disabled	Disabled	Disabled	128
8	Disabled	Disabled	Disabled	128
9	Disabled	Disabled	Disabled	128
10	Disabled	Disabled	Disabled	128
11	Disabled	Disabled	Disabled	128
12	Disabled	Disabled	Disabled	128
13	Disabled	Disabled	Disabled	128
14	Disabled	Disabled	Disabled	128
15	Disabled	Disabled	Disabled	128
16	Disabled	Disabled	Disabled	128
17	Disabled	Disabled	Disabled	128
18	Disabled	Disabled	Disabled	128
19	Disabled	Disabled	Disabled	128
20	Disabled	Disabled	Disabled	128
21	Disabled	Disabled	Disabled	128
22	Disabled	Disabled	Disabled	128
23	Disabled	Disabled	Disabled	128
24	Disabled	Disabled	Disabled	128
25	Disabled	Disabled	Disabled	128
26	Disabled	Disabled	Disabled	128

Figure 6- 37. Traffic Control Settings window

The purpose of broadcast, multicast or unknown unicast storm control is to limit too many broadcast, multicast or unknown unicast packets flooding in the network. Each port has a counter that tracks the number of broadcast packets received per second. The counter is cleared once per second. If the broadcast, multicast, or unknown unicast storm control is enabled, the port will discard all broadcast, multicast or unknown unicast packets received when the counter is greater or equal to the programmed Threshold.

Broadcast Storm, Multicast Storm and Destination Lookup Fail may be *Enabled* or *Disabled* for either group.

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*. The settings of each port may be viewed in the Traffic Control Table in the same window. Click **Apply** to implement changes made.

Port Security

A given port's (or a range of ports') 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**.

Port Security 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.

Figure 6- 38. Port Security Settings window

The following parameters can be set:

Parameter	Description
Unit	Choose the desired unit.
From/To	A consecutive group of ports may be configured starting with the selected port.
Admin State	This pull-down menu allows you to enable or disable Port Security (locked MAC address table for the selected ports).
Max. Addr (0-64)	The number of MAC addresses that will be in the MAC address forwarding table for the selected switch and group of ports.

	selected switch and group of ports.
Mode	This pull-down menu allows you to select how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are:
	• *Permanent* – The locked addresses will not age out after the aging timer expires.
	• *DeleteOnTimeout* – The locked addresses will age out after the aging timer expires.
	• *DeleteOnReset* – The locked addresses will not age out until the Switch has been reset.

Click **Apply** to implement changes made.

Port Lock Entries

The **Port Lock Entries Table** window is used to remove an entry from the port security entries learned by the Switch and entered into the forwarding database. To view the following window, click **Configuration > Port Lock Entries**.

Figure 6- 39. Port Lock Entries Table

This function is only operable if the Mode in the **Port Security** window is selected as *Permanent or DeleteOnReset***,** or in other words, only addresses that are permanently learned by the Switch can be deleted. Once the entry has been defined by entering the correct information into the window above, click the ✕ under the **Delete** heading of the corresponding MAC address to be deleted. Click the **Next** button to view the next page of entries listed in this table. This window displays the following information:

Parameter	Description
VID	The VLAN ID of the entry in the forwarding database table that has been permanaently learned by the Switch.
VLAN Name	The VLAN Name of the entry in the forwarding database table that has been permanaently learned by the Switch.
MAC Address	The MAC address of the entry in the forwarding database table that has been permanaently learned by the Switch.

80

Unit	The ID number of the Switch in the switch stack that has permanently learned the MAC address.
Port	The ID number of the port that has permanently learned the MAC address.
Type	The type of MAC address in the forwarding database table. Only entries marked Secured_Permanent can be deleted.
Delete	Click the ☒ in this field to delete the corresponding MAC address that was permanently learned by the Switch.

QoS

The DXS-3326GSR supports 802.1p priority queuing Quality of Service. The following section discusses the implementation of QoS (Quality of Service) and benefits of using 802.1p priority queuing.

Advantages of QoS

QoS is an implementation of the IEEE 802.1p standard that allows network administrators a method of reserving bandwidth for important functions that require a large bandwidth or have a high priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Not only can a larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and, in turn prioritized. View the following map to see how the DXS-3326GSR implements 802.1P priority queuing.
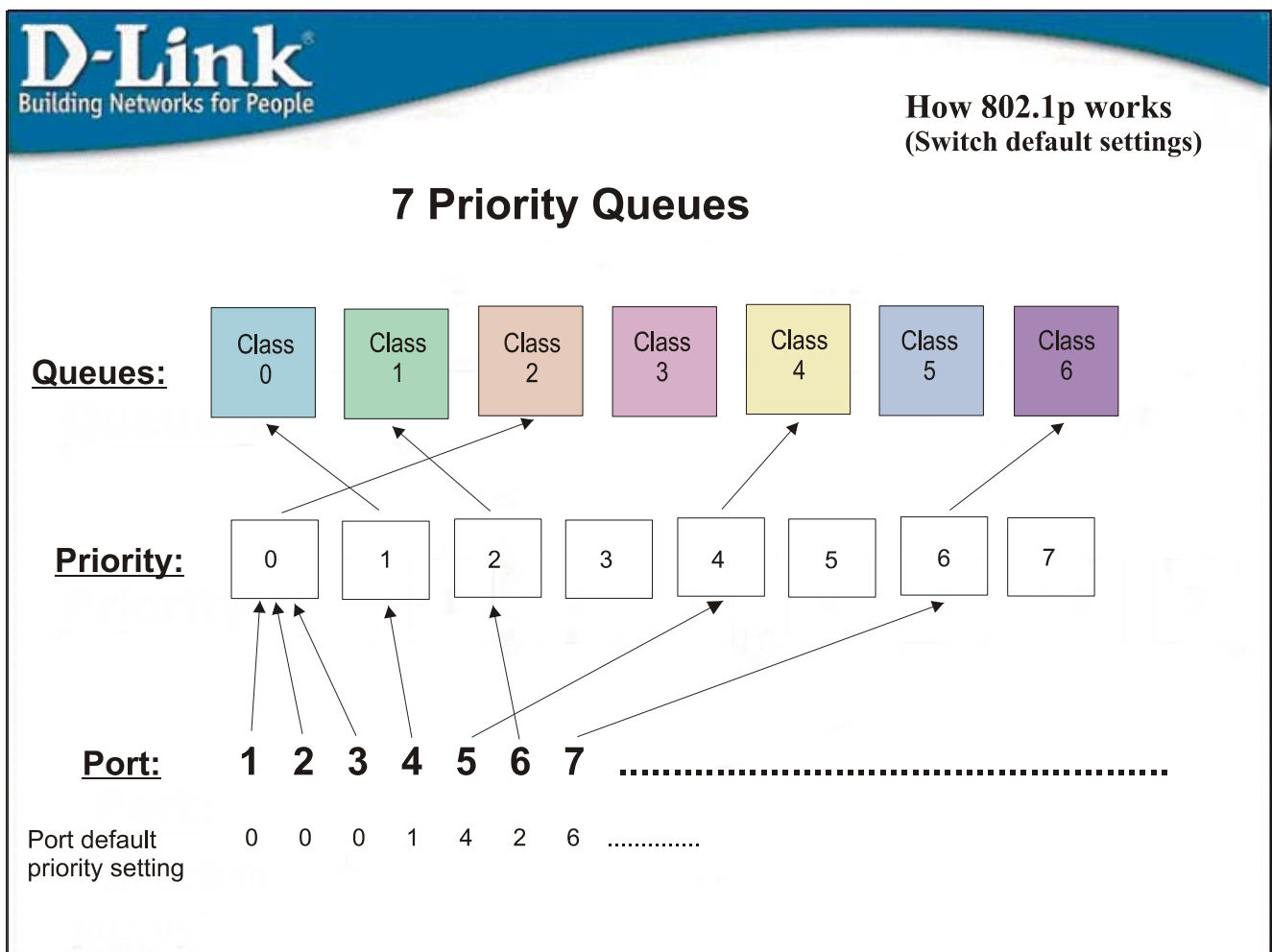
Figure 6- 40. Mapping QoS on the Switch

The picture above shows the default priority setting for the Switch. Class-6 has the highest priority of the eight priority queues on the Switch. In order to implement QoS, the user is required to instruct the Switch to examine the header of a packet to see if it has the proper identifying tag tagged. Then the user may forward these tagged packets to designated queues on the Switch where they will be emptied, based on priority.

For example, lets say a user wishes to have a video conference between two remotely set computers. The administrator can add priority tags to the video packets being sent out, utilizing the Access Profile commands. Then, on the receiving end, the administrator instructs the Switch to examine packets for this tag, acquires the tagged packets and maps them to a class queue on the Switch. Then in turn, the administrator will set a priority for this queue so that will be emptied before any other packet is forwarded. This results in the end user receiving all packets sent as quickly as possible, thus prioritizing the queue and allowing for an uninterrupted stream of packets, which optimizes the use of bandwidth available for the video conference.

Understanding QoS

The Switch has seven classes of service. These classes of services are labeled as 6, the highest class, to 0, the lowest class. The eight priority tags, specified in IEEE 802.1p are mapped to the Switch's classes of service as follows:

- Priority 0 is assigned to the Switch's Q2 queue.

- Priority 1 is assigned to the Switch's Q0 queue.

- Priority 2 is assigned to the Switch's Q1 queue.

- Priority 3 is assigned to the Switch's Q3 queue.

- Priority 4 is assigned to the Switch's Q4 queue.

- Priority 5 is assigned to the Switch's Q5 queue.

- Priority 6 is assigned to the Switch's Q6 queue.

- Priority 7 is assigned to the Switch's Q6 queue.

For strict priority-based scheduling, any packets residing in the higher priority queues are transmitted first. Multiple strict classes of service are emptied based on their priority tags. Only when these queues are empty, are packets of lower priority transmitted.

For weighted round-robin queuing, the number of packets sent from each class of service depends upon the assigned weight. For a configuration of eight CoS queues, A~H with their respective weight value: 8~1, the packets are sent in the following sequence: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

For weighted round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

For weighted round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common weighted round-robin scheme.

Remember that the DXS-3326GSR has seven classes of service for each port on the Switch.

Bandwidth Control

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port. In the **Configuration** folder, click **Port Bandwidth**, to view the window shown below.

Figure 6- 41. Bandwidth Settings window

The following parameters can be set or are displayed:

Parameter	Description
Unit	Choose the desired unit.
From/To	A consecutive group of ports may be configured starting with the selected port.
Type	This drop-down menu allows you to select between *RX* (receive,) *TX* (transmit,) and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving,

	transmitting, or both receiving and transmitting packets.
no_limit	This drop-down menu allows you to specify that the selected port will have no bandwidth limit. *Enabled* disables the limit.
Rate	This field allows you to enter the data rate, in Mbit/s, that will be the limit for the selected port.

Click **Apply** to set the bandwidth control for the selected ports. Results of configured Bandwidth Settings will be displayed in the Port Bandwidth Table.

QoS Scheduling Mechanism

This drop-down menu allows you to select between a Weight Fair and a Stric**t** mechanism for emptying the priority queues. In the **Configuration** folder, open the **QoS** folder and click **QoS Scheduling Mechanism**, to view the window shown below.

Figure 6- 42. Scheduling Mechanism Configuration window

The Scheduling Mechanism has the following parameters.

Parameter	Description
Strict	The highest queue is the first to process traffic. That is, the highest queue will finish before other queues empty.
Weight fair	Use the weighted round-robin (*WRR*) algorithm to handle packets in an even distribution in priority queues.

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

QoS Output Scheduling

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 classes of services is 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. In the **Configuration** folder open the **QoS** folder and click **QoS Output Scheduling**, to view the window shown below.

Figure 6- 43. QoS Output Scheduling Configuration window

You may assign the following values to the QoS classes to set the scheduling.

Parameter	Description
Max. Packets	Specifies the maximum number of packets the above specified hardware priority queue will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. A value between *0* and *15* can be specified.

Click **Apply** to implement changes made.

> **NOTE:** The settings you assign to the queues, numbers 0 to 7, represent the IEEE 802.1p priority tag number. Do not confuse these settings with port numbers.

> **NOTE:** Entering a 0 for the Max Packets field in the **QoS Ouput Scheduling Configuration** window above will create a Combination Queue. For more information on implementation of this feature, see the next section, **Configuring the Combination Queue.**

Configuring the Combination Queue

Utilizing the **QoS Output Scheduling Configuration** window shown above, the DXS-3326GSR can implement a combination queue for forwarding packets. This combination queue allows for a combination of strict and weight-fair (weighted round-robin *"WRR"*) scheduling. To set the combination queue, enter a *0* for the Max Packets entry of the corresponding priority queues listed in the window above. Priority queues that have a *0* in the Max Packet field will forward packets with strict priority scheduling. The remaining queues, that do not have a *0* in their Max Packet field, will follow a weighted round-robin (*WRR*) method of forwarding packets — as long as the priority queues with a *0* in their Max Packet field are empty. When a packet arrives in a priority queue with a *0* in its Max Packet field, this queue will automatically begin forwarding packets until it is empty. Once a priority queue with a *0* in its Max Packet field is empty, the remaining priority queues will reset the weighted round-robin (*WRR*) cycle of forwarding packets, starting with the highest available priority queue. Priority queues with an equal level of priority and equal entries in their Max Packet field will empty their fields based on hardware priority scheduling. The Max Packet parameter allows you to specify the maximum number of packets a given priority queue can transmit per weighted round-robin (*WRR*) scheduling cycle. This provides for a controllable CoS behavior while allowing other queues to empty as well. A value between *0* and *15* packets can be specified per priority queue to create the combination queue.

The example window below displays an example of the combination queue where Class-1 will have a strict priority for emptying its queue, while the other classes will follow a weight fair scheduling.

Figure 6- 44. QoS Output Scheduling Configuration window – Combination Queue Example

802.1p Default Priority

The Switch allows the assignment of a default 802.1p priority to each port on the Switch. In the **Configuration** folder open the **QoS** folder and click **802.1p Default Priority**, to view the window shown below.

Figure 6- 45. 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. Click **Apply** to implement your settings.

802.1p User Priority

The DXS-3326GSR allows the assignment of a class of service to each of the 802.1p priorities. In the **Configuration** folder open the **QoS** folder and click **802.1p User Priority**, to view the screen shown below.

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-6	
		Apply

Figure 6- 46. 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. Click **Apply** to set your changes.

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 (Single IP). 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.

In the **Configuration** folder open the **QoS** folder and click **Traffic Segmentation**, to view the window shown below.

Figure 6- 47. Current Traffic Segmentation Table window

This window allows you to view which port on a given switch will be allowed to forward packets to other ports on that switch.

The user may set the following parameters:

Parameter	Description
Unit	Choose the desired unit you wish to see the current traffic segmentation for.
Port	Choose the port you wish to see the current traffic segmentation for.

Click **Setup** to select which ports will be allowed to forward packets.

Figure 6- 48. Setup Forwarding ports window

This window allows you to determine which port on a given switch in a switch stack will be allowed to forward packets to other ports on that switch.

Configuring traffic segmentation on the Switch is accomplished in two parts. First, you specify a switch from a switch stack by using the Unit pull-down menu, and then a port from that switch, using the Port pull-down menu. Then you specify a second switch from the switch stack, and then you select which ports (or different ports on the same switch,) on that switch that you want to be able to receive packets from the switch and port you specified in the first part.

Clicking the **Apply** button will enter the combination of transmitting port and allowed receiving ports into the Switch's Traffic Segmentation table.

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

The Unit drop-down menu under the Setup Forwarding ports heading allows you to select a switch from a switch stack using that switch's Unit ID. The Forward Port click boxes allow you to select which of the ports on the selected switch will be able to forward packets. These are the ports that will be allowed to receive packets from the port specified above.

Click **Apply** to enter the settings into the Switch's Traffic Segmentation table.

System Log Server

The Switch can send Syslog messages to up to four designated servers using the System Log Server. In the **Configuration** folder, click **System Log Server**, to view the screen shown below.

Figure 6- 49. Current System Log Servers window

The parameters configured for adding and editing System Log Server settings are the same. To add a new Syslog Server, click the **Add** button. To modify a current entry, click the hyperlinked number of the server in the Index field. Both actions will result in the same window to configure. See the table below for a description of the parameters in the following window.

Figure 6- 50. Configure System Log Server-Add window

The following parameters can be set:

Parameter	Description
Index (1-4)	Syslog server settings index (1-4).
Server IP	The IP address of the Syslog server.
Severity	This drop-down menu allows you to select the level of messages that will be sent. The options are *Warning*, *Informational*, and *ALL*.
Facility	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 indicates the facility values that the Switch currently implements.

Numerical   Facility

Code

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 (514 or 6000-65535)	Type the UDP port number used for sending Syslog messages. The default is *514*.	
Status	Choose *Enabled* or *Disabled* to activate or deactivate.	

To set the System Log Server configuration, click **Apply**. To delete an entry from the **Current System Log Servers** window, click the corresponding ✕ under the **Delete** heading of the entry you wish to delete. To return to the **Current System Log Servers** window, click the Show All System Log Servers link.

SNTP Setting

Time Setting

To configure the time settings for the Switch, open the **Configuration** folder, then the **SNTP** folder and click on the **Current Time Setting** link, revealing the following window for the user to configure.

Figure 6- 51. Current Time window

The following parameters can be set or are displayed:

Parameter	Description
Current Time: Status	
System Boot Time	Displays the time when the Switch was initially started for this session.
Current Time	Displays the current time.
Time Source	Displays the time source for the system.
Current Time: SNTP Settings	
SNTP State	Use this pull-down menu to Enable or Disable SNTP.
SNTP Primary Server	This is the IP address of the primary server the SNTP information will be taken from.
SNTP Secondary Server	This is the IP address of the secondary server the SNTP information will be taken from.
SNTP Poll Interval in Seconds (30-99999)	This is the interval, in seconds, between requests for updated SNTP information.
Current Time: Set Current Time	

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

Click **Apply** to implement your changes.

Time Zone and DST

The following are windows used to configure time zones and Daylight Savings time settings for SNTP. Open the **Configuration** folder, then the **SNTP** folder and click on the **Time Zone and DST** link, to reveal the following window.

Figure 6- 52. Time Zone and DST Settings window

The following parameters can be set:

Parameter	Description
Time Zone and DST Settings	

94

Daylight Saving Time State	Use this pull-down menu to enable or disable the DST Settings.
Daylight Saving Time Offset in Minutes	Use this pull-down menu to specify the amount of time that will constitute your local DST offset - 30, 60, 90, or 120 minutes.
Time Zone Offset from GMT in +/- HH:MM	Use these pull-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)

DST Repeating Settings - 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.

From: Which Day	Enter the week of the month that DST will start.
From: Day of Week	Enter the day of the week that DST will start on.
From: Month	Enter the month DST will start on.
From: time in HH:MM	Enter the time of day that DST will start on.
To: Which Day	Enter the week of the month the DST will end.
To: Day of Week	Enter the day of the week that DST will end.
To: Month	Enter the month that DST will end.
To: time in HH:MM	Enter the time DST will end.

DST Annual Settings - Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified consisely. For example, specify to begin DST on April 3 and end DST on October 14.

From: Month	Enter the month DST will start on, each year.
From: Day	Enter the day of the month DST will start on, each year.
From: time in HH:MM	Enter the time of day DST will start on, each year.
To: Month	Enter the month DST will end on, each year.
To: Day	Enter the day of the month DST will end on, each year.
To: Time in HH:MM	Enter the time of day that DST will end on, each year.

Click **Apply** to implement changes made to the **Time Zone and DST Settings** window.

Access Profile Table

Configuring the 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 (the example shown below includes one of each type that have already been configured by clicking **Add** and then choosing the desired Type from the drop-down menu on the **Access Profile Configuration** window).

Figure 6- 53. 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 the Packet Content Mask. You can switch among the three **Access Profile Configuration** windows by using the Type drop-down menu. The window shown below is the **Access Profile Configuration** window for Ethernet.

Figure 6- 54. Access Profile Table (Ethernet) window

The following parameters can be set, for the **Ethernet** type:

Parameter	Description
Profile ID (1-8)	Type in a unique identifier number for this profile set. This value can be set from *1* to *8*.
Type	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 *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.
VLAN	Selecting this option instructs the Switch to examine the VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
Source MAC	Source MAC Mask - Enter a MAC address mask for the source MAC address.
Destination MAC	Destination MAC Mask - Enter a MAC address mask for the destination MAC address.
802.1p	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.
Ethernet type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.
Port	The user may set the Access Profile Table on a per-port basis by entering a port number in this field.

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

Figure 6- 55. Access Profile Configuration (IP) window

The following parameters can be set, for **IP**:

Parameter	Description
Profile ID (1-8)	Type in a unique identifier number for this profile set. This value can be set from *1* to *8*.
Type	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 *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.
VLAN	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.
Source IP Mask	Enter an IP address mask for the source IP address.

Destination IP Mask	Enter an IP address mask for the destination IP address.
DSCP	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.
Protocol	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: Select ICMP to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. • Select Type to further specify that the access profile will apply an ICMP type value, or specify Code to further specify that the access profile will apply an ICMP code value. Select IGMP to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. • Select Type to further specify that the access profile will apply an IGMP type value Select TCP to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish). • src port mask - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to deny. • dest port mask - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to deny. Select UDP to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. • src port mask - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff) that you want to filter. • dest port mask - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) that you want to filter. protocol id - Enter a value defining the protocol ID in the packet header to mask. Specify Layer 4 protocol masks in hex form (hex 0x0-0xffffffff). You can specify up to five of these masks.
Port	The user may set the Access Profile Table on a per-port basis by entering an entry 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.

Figure 6- 56. 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 Mask:

Parameter	Description
Profile ID (1-8)	Type in a unique identifier number for this profile set. This value can be set from *1* to *8*.
Type	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 *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.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified:
	• *value (0-15)* - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th 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 on a per-port basis by entering an entry in this field. Entering all will denote all ports on the Switch.

Click **Apply** to implement changes made.

To establish the rule for a previously created Access Profile:

In the **Configuration** folder, click the **Access Profile Table** link opening the **Access Profile Table** window. Under the heading Access Rule, clicking **Modify**, will open the following window.

Figure 6- 57. Access Rule Table window

To create a new rule set for an access profile click the **Add** button. A new window is displayed. To remove a previously created rule, click the corresponding ✕ button.

Figure 6- 58. Access Rule Configuration window (IP) window

Configure the following Access Rule Configuration settings:

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select Permit to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select Deny to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access. This value can be set from *1* to *50*.
Type	Selected profile based on Ethernet (MAC Address), IP address or Packet Content Mask. • *Ethernet* instructs the Switch to examine the layer 2 part of each packet header. • *IP* instructs the Switch to examine the IP address in each frame's header. • *Packet Content Mask* instructs the Switch to examine the packet header
Priority (0-7)	This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user. Replace priority with − Click the corresponding box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this window, before forwarding it on to the CoS queue mapped previously by the user. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues, and mapping for 802.1p, see the

	QoS section of this manual.
Replace DSCP (0-63)	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.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Source IP	Source IP Address - Enter an IP Address mask for the source IP address.
Destination IP	Destination IP Address- Enter an IP Address mask for the destination IP address.
DSCP (0-63)	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*.
Protocol	This field allows the user to modify the protocol used to configure the Access Rule Table, depending on which protocol the user has chosen in the Access Profile Table.

To view the settings of a previously correctly configured rule, click **View** in the Access Rule Table to view the following window:

Figure 6- 59. Access Rule Display window (IP) window

To configure the Access Rule for Ethernet, open the **Access Profile Table** window for Ethernet and click **Modify** for an Ethernet entry. This will open the following window:

Figure 6- 60. Access Rule Table window

To remove a previously created rule, select it and click the [X] button. To add a new Access Rule, click the **Add** button:

Figure 6- 61. Access Rule Configuration (Ethernet) window

To set the Access Rule for Ethernet, adjust the following parameters and click **Apply**.

Parameters	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select Permit to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select Deny to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access. This value can be set from *1* to *50*.
Type	Selected profile based on Ethernet (MAC Address), IP address or Packet Content Mask.

	Mask.
	• *Ethernet* instructs the Switch to examine the layer 2 part of each packet header.
	• *IP* instructs the Switch to examine the IP address in each frame's header.
	• *Packet Content Mask* instructs the Switch to examine the packet header
Priority (0-7)	This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.
	Replace priority with – Click the corresponding box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this window, before forwarding it on to the CoS queue mapped previously by the user. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
	For more information on priority queues, CoS queues, and mapping for 802.1p, see the QoS section of this manual.
Replace DSCP (0-63)	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.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Source MAC	Source MAC Address - Enter a MAC Address for the source MAC address.
Destination MAC	Destination MAC Address - Enter a MAC Address mask for the destination MAC address.
802.1p (0-7)	Enter a value from *0* to *7* to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type	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.

To view the settings of a previously correctly configured rule, click **View** in the Access Rule Table to view the following window:

Figure 6- 62. Access Rule Display (Ethernet) window

To configure the Access Rule for Packet Content Mask, open the **Access Profile Table** window and click **Modify** for a Packet Content Mask entry. This will open the following window:

Figure 6- 63. Access Rule Table (Packet Content Mask) window

To remove a previously created rule, select it and click the ✕ button. To add a new Access Rule, click the **Add** button:

Figure 6- 64. Access Rule Configuration (Packet Content Mask) window

To set the Access Rule for the Packet Content Mask, adjust the following parameters and click **Apply**.

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select Permit to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).

	Select Deny to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access. This value can be set from *1* to *50*.
Type	Selected profile based on Ethernet (MAC Address), IP address or Packet Content Mask. • *Ethernet* instructs the Switch to examine the layer 2 part of each packet header. • *IP* instructs the Switch to examine the IP address in each frame's header. • *Packet Content Mask* instructs the Switch to examine the packet header.
Priority (0-7)	This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user. Replace priority with – Click the corresponding box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this window, before forwarding it on to the CoS queue mapped previously by the user. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues, and mapping for 802.1p, see the QoS section of this manual.
Replace DSCP (0-63)	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.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified: • *value (0-15)* - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th 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.

To view the settings of a previously correctly configured rule, click **View** in the **Access Rule Table** to view the following window:

Access Rule Display

Profile ID	2
Access ID	1
Mode	Permit
Type	Packet Content
Priority	------
Replace Dscp	------
Offset	**Offset (0 - 15)** mask:0x00000000 mask:0x00000000 mask:0x00000000 mask:0x00000000 **Offset (16 - 31)** mask:0x00000000 mask:0x00000000 mask:0x00000000 mask:0x00000000 **Offset (32 - 47)** mask:0x00000000 mask:0x00000000 mask:0x00000000 mask:0x00000000 **Offset (48 - 63)** mask:0x00000000 mask:0x00000000 mask:0x00000000 mask:0x00000000

Show All Access Rule Entries

Figure 6- 65. Access Rule Display window (Packet Content Mask) window

Port Access Entity

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-Based Network Access Control.

Port-Based Network Access Control
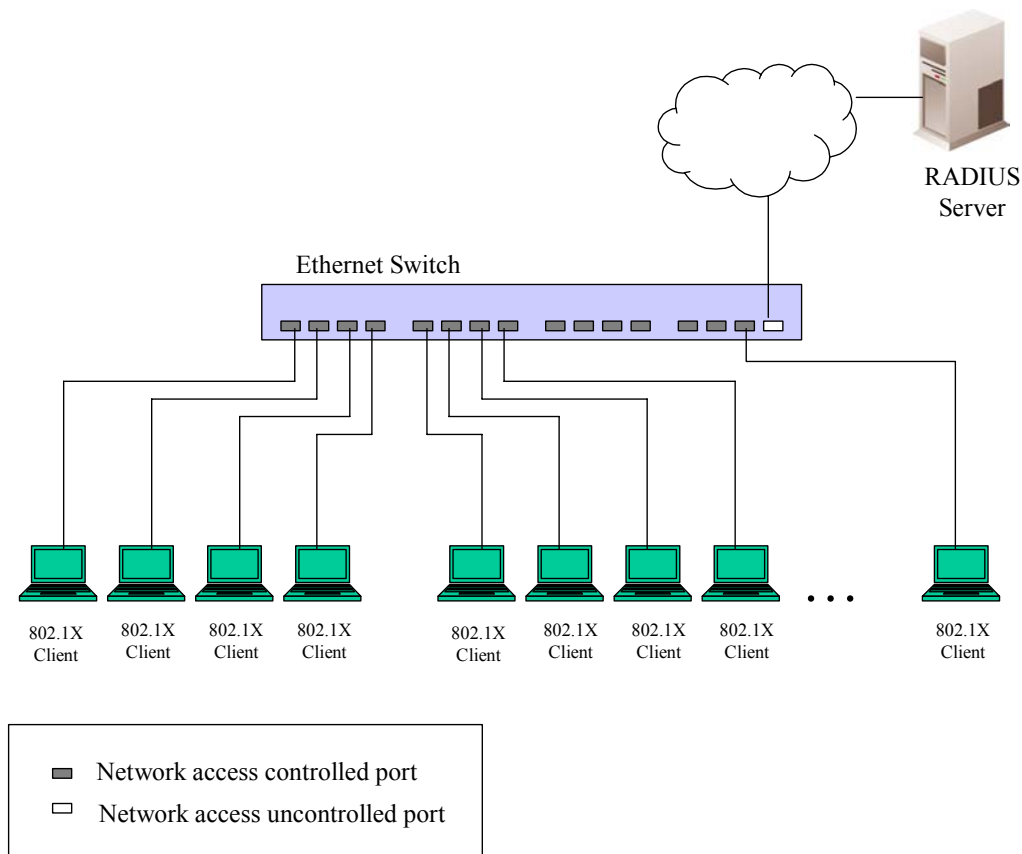
Figure 6- 66. Example of Typical Port-Based Configuration

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

MAC-Based Network Access Control
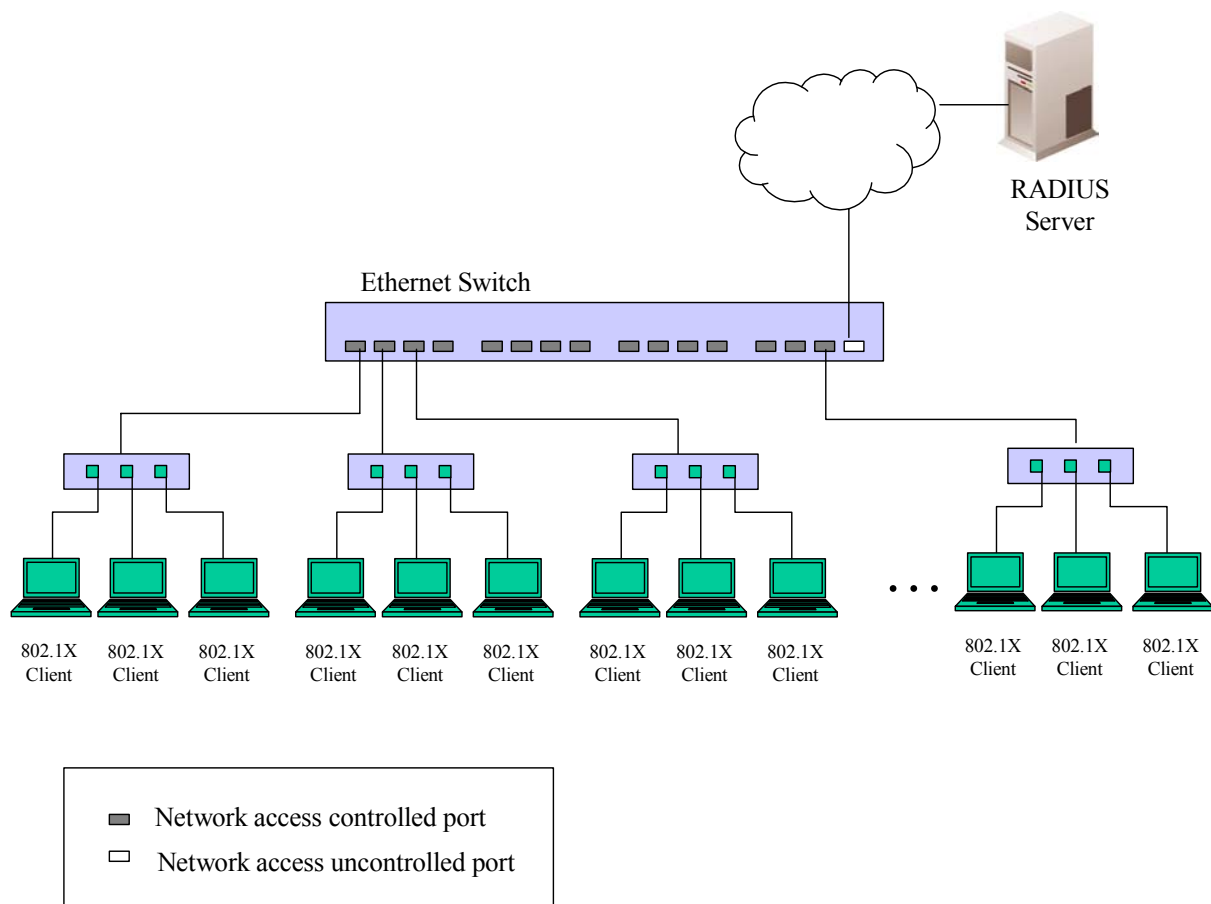
Figure 6- 67. Example of Typical MAC-Based Configuration

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create "logical" Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices' individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.

Configure Authenticator

To configure the 802.1X Authenticator Settings, click **Port Access Entity** > **Configure Authenticator**:

Unit: 1

Port	AdmDir	Port Control	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled
802.1X Authenticator Settings-Unit 1									
1	both	Auto	30	60	30	30	2	3600	No
2	both	Auto	30	60	30	30	2	3600	No
3	both	Auto	30	60	30	30	2	3600	No
4	both	Auto	30	60	30	30	2	3600	No
5	both	Auto	30	60	30	30	2	3600	No
6	both	Auto	30	60	30	30	2	3600	No
7	both	Auto	30	60	30	30	2	3600	No
8	both	Auto	30	60	30	30	2	3600	No
9	both	Auto	30	60	30	30	2	3600	No
10	both	Auto	30	60	30	30	2	3600	No
11	both	Auto	30	60	30	30	2	3600	No
12	both	Auto	30	60	30	30	2	3600	No
13	both	Auto	30	60	30	30	2	3600	No
14	both	Auto	30	60	30	30	2	3600	No
15	both	Auto	30	60	30	30	2	3600	No
16	both	Auto	30	60	30	30	2	3600	No
17	both	Auto	30	60	30	30	2	3600	No
18	both	Auto	30	60	30	30	2	3600	No
19	both	Auto	30	60	30	30	2	3600	No
20	both	Auto	30	60	30	30	2	3600	No
21	both	Auto	30	60	30	30	2	3600	No
22	both	Auto	30	60	30	30	2	3600	No
23	both	Auto	30	60	30	30	2	3600	No
24	both	Auto	30	60	30	30	2	3600	No
25	both	Auto	30	60	30	30	2	3600	No
26	both	Auto	30	60	30	30	2	3600	No

Figure 6- 68. first 802.1X Authenticator Settings window

To configure the settings by port, click on the hyperlinked port number under the Port heading, which will display the following table to configure:

Figure 6- 69. second 802.1X Authenticator Settings window

This window allows you to set the following features:

Parameter	Description
Unit	Choose the desired unit.
From [ ] To [ ]	Enter the port or ports to be set.
AdmDir *<both>*	Sets the administrative-controlled direction to either *in* or *both*. If *in* is selected, control is only exerted over incoming traffic through the port you selected in the first field. If *both* is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.
PortControl *< auto >*	This allows you to control the port authorization state. Select *forceAuthorized* 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 *forceUnauthorized* 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 *auto* is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

	The default setting is *Auto*.
TxPeriod *<30 >*	This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. The default setting is *30* seconds.
QuietPeriod *<60 >*	This allows you to set the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. The default setting is *60* seconds.
SuppTimeout *<30 >*	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is *30* seconds.
ServerTimeout *<30 >*	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is *30* seconds.
MaxReq *<2 >*	The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. The default setting is *2.*
ReAuthPeriod *<3600>*	A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default settijng is *3600* seconds.
ReAuth *<Disabled>*	Determines whether regular reauthentication will take place on this port. The default setting is *Disabled*.

Click **Apply** to implement your configuration changes. To view configurations for the 802.1X Authenticator Settings on a port-by-port basis, see the 802.1X Authenticator Settings table.

Local users

To configure an 802.1X local user, click **Port Access Entity** > **Local users**. This window will allow the user to set different local users on the Switch.

Figure 6- 70. 802.1X Local User Table Configuration window

Enter a User Name, Password, and confirmation of that password. Properly configured local users will be displayed in the 802.1x Local User Table in the lower half of the window.

PAE System Control

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

NOTE: By default, the Switch 802.1x is set to *Disabled*. Use the drop-down menu on the **Switch Information (Advanced Settings)** window to set Switch 802.1x to either *Port Base* or *MAC Base*.

Port Capability Settings

Click **Port Access Entity > PAE System Control > Port Capability Settings** to view the following window:

Figure 6- 71. 802.1x Capability Settings window

To set up the Switch's 802.1x port-based authentication, select which unit and ports are to be configured in the Unit and From/To fields. Next, enable the ports by selecting *Authenticator* from the drop-down menu under Capability. Click **Apply** to let your change take effect.

Configure the following 802.1x capability settings:

Parameter	Description
Unit	Unit being configured for 802.1x settings.
From and To	Ports being configured for 802.1x settings.
Capability	Two role choices can be selected: *Authenticator* - A user must pass the authentication process to gain access to the network. *None* - The port is not controlled by the 802.1x functions.

Initialize Ports

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

Click **Port Access Entity > PAE System Control > Initialize Port(s)** to open the **Initialize Port** window:

Initialize Port

Unit	From	To	Apply
1 ▾	Port 1 ▾	Port 1 ▾	Apply

Initialize Port Table-Unit 1

Port	Auth PAE State	Backend_State	Port Status
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized
13	ForceAuth	Success	Authorized
14	ForceAuth	Success	Authorized
15	ForceAuth	Success	Authorized
16	ForceAuth	Success	Authorized
17	ForceAuth	Success	Authorized
18	ForceAuth	Success	Authorized
19	ForceAuth	Success	Authorized
20	ForceAuth	Success	Authorized
21	ForceAuth	Success	Authorized
22	ForceAuth	Success	Authorized
23	ForceAuth	Success	Authorized
24	ForceAuth	Success	Authorized
25	ForceAuth	Success	Authorized
26	ForceAuth	Success	Authorized

Figure 6- 72. Initialize Port (Port-Based) window
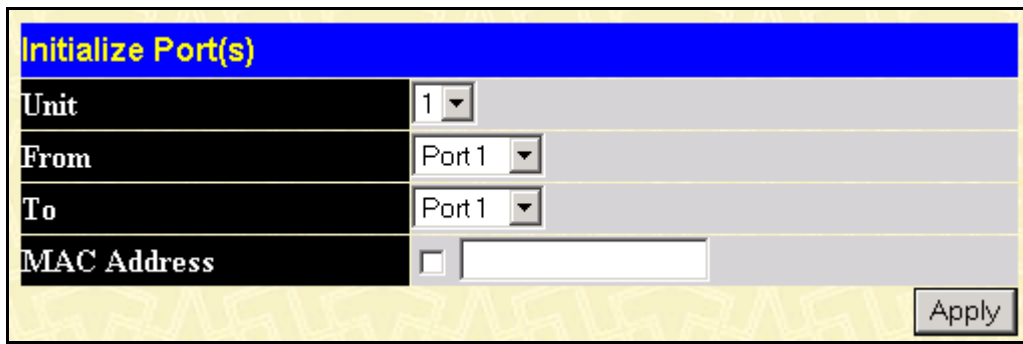
Figure 6- 73. Initialize Port(s) (MAC-Based) window

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

These windows display the following information:

Parameter	Description
Unit	Select desired unit.
From and To	Select ports to be initialized.
Port	A read only field indicating a port on the Switch.
MAC Address	Check the corresponding check box and enter a MAC address for which to initialize 802.1x for. This field is only for the **Initialize Port(s) (MAC-Based)** window.
Auth PAE State	The Authenticator PAE State will display one of the following: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth,* and *N/A.*
Backend State	The Backend Authentication State will display one of the following: *Request, Response, Success, Fail, Timeout, Idle, Initialize,* and *N/A.*
Port Status	The status of the controlled port can be *Authorized, Unauthorized,* or *N/A.*

NOTE: The user must first globally enable 802.1X in the **Switch Information (Advanced Settings)** window in the **Configuration** folder before initializing ports. Information in the Initialize Ports Table cannot be viewed before enabling 802.1X.

Reauthenticate Port(s)

These windows allow you to reauthenticate a port or group of ports by choosing a port or group of ports by using the pull-down menus Unit and From/To and clicking **Apply**. The Reauthenticate Port Table displays the current status of the reauthenticated port(s) once you have clicked **Apply.**

Click **Port Access Entity > PAE System Control > Reauthenticate Port(s)** to open one of the two following windows:

Figure 6- 74. Reauthenticate Port (Port-Based) window

Figure 6- 75. Reauthenticate Port (MAC-Based) window

These windows display the following information:

Parameter	Description
Unit	The unit where the reauthenticated port resides.
Port	The port number of the reauthenticated port.
MAC Address	Displays the physical address of the Switch where the port resides.
Auth State	The Authenticator State will display one of the following: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth,* and *N/A.*
BackendState	The Backend State will display one of the following: *Request, Response, Success, Fail, Timeout, Idle, Initialize,* and *N/A.*
OpenDir	Operational Controlled Directions are *both* and *in*.

PortStatus	The status of the controlled port can be *Authorized, Unauthorized,* or *N/A*.

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. The Web Manager offers three windows.

Click **Port Access Entity > RADIUS Server > Authentic RADIUS Server** to open the following window shown below:

Authentic RADIUS Server Setting

Succession	First ▼
RADIUS Server	0.0.0.0
Authentic Port	1812
Accounting Port	1813
Key	
Confirm Key	
Status	Valid ▼

Apply

Current RADIUS Server(s) Settings Table

Succession	RADIUS Server	Auth UDP Port	Acct UDP Port	Status	Key
First					
Second					
Third					

Figure 6- 76. Authentic RADIUS Server Setting window

This window displays the following information:

Parameter	Description
Succession *<First>*	Choose the desired RADIUS server to configure: *First, Second* or *Third*.
RADIUS Server *<0.0.0.0>*	Set the RADIUS server IP.
Authentic Port *<1812>*	Set the RADIUS authentic server(s) UDP port. The default port is *1812*.
Accounting Port *<1813>*	Set the RADIUS account server(s) UDP port. The default port is *1813*.
Key	Set the key the same as that of the RADIUS server.
Confirm Key	Confirm the shared key is the same as that of the RADIUS server.
Status	This allows you to set the RADIUS Server to *Valid* or *Invalid*.

Layer 3 IP Networking

L3 Global Advanced Settings

IP Interfaces Tables

MD5 Key Table Configuration

Route Redistribution Settings

Static/Default Route

Route Preference Setting

Static ARP Settings

RIP

RIP Global Settings

RIP Interface Settings

OSPF

OSPF Global Settings

OSPF Area ID Setting

OSPF Interface Settings

OSPF Virtual Interface Settings

OSPF Area Aggregation Settings

OSPF Host Route Settings

DHCP/BOOTP Relay

DHCP/BOOTP Global Settings

DHCP/BOOTP Relay Settings

DNS Relay

DNS Global Settings

DNS Relay Static Setting

VRRP

VRRP Global Settings

VRRP Configuration

IP Multicast Routing Protocol

IGMP Interface Settings

DVMRP Global Settings

DVMRP Interface Settings

PIM

PIM-DM Global Settings

PIM-DM Interface Settings

L3 Global Advanced Settings

The **L3 Global Advanced Settings** window allows the user to enable and disable Layer 3 settings and functions from a single window. The full settings and descriptions for these functions will appear later in this section. To view this window, open the **Configuration** folder and then the **Layer 3 IP Networking** folder and click on the **L3 Global Advanced Settings** link to access the following window.

Figure 7- 1. L3 Global Advanced Settings window

The user may set the following:

Parameter	Description
DVMRP State	The user may globally enable or disable the Distance Vector Multicast Routing Protocol (DVMRP) function by using the pull-down menu.
PIM-DM State	The user may globally enable or disable the Protocol Independent Multicast - Dense Mode (PIM-DM) function by using the pull-down menu.
RIP State	The user may globally enable or disable the Routing Information Protocol (RIP) function by using the pull-down menu.
OSPF State	The user may globally enable or disable the Open Shortest Path first (OSPF) function by using the pull-down menu.
ARP Aging Time (0-65535)	The user may globally set the maximum amount of time, in minutes, that an Address Resolution Protocol (ARP) entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table. The value may be set in the range of *0* to *65535* minutes with a default setting of *20* minutes.

IP Interfaces Table

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

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineer	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20

Sales	5	1, 2, 3, 4
Backbone	6	25, 26

Table 7- 1. VLAN Example - Assigned Ports

In this case, six IP interfaces are required, so a CIDR notation of 10.32.0.0/11 (or a 11-bit) addressing scheme will work. This addressing scheme will give a subnet mask of 11111111.11100000.00000000.00000000 (binary) or 255.224.0.0 (decimal).

Using a 10.xxx.xxx.xxx IP address notation, the above example would give six network addresses and six subnets.

Any IP address from the allowed range of IP addresses for each subnet can be chosen as an IP address for an IP interface on the switch.

For this example, we have chosen the next IP address above the network address for the IP interface's IP Address:

VLAN Name	VID	Network Number	IP Address
System (default)	1	10.32.0.0	10.32.0.1
Engineer	2	10.64.0.0	10.64.0.1
Marketing	3	10.96.0.0	10.96.0.1
Finance	4	10.128.0.0	10.128.0.1
Sales	5	10.160.0.0	10.160.0.1
Backbone	6	10.192.0.0	10.192.0.1

Table 7- 2. VLAN Example - Assigned IP Interfaces

The six IP interfaces, each with an IP address (listed in the table above), and a subnet mask of 255.224.0.0 can be entered into the **Setup IP Interface** window.

To setup IP Interfaces on the Switch:

Go to the **Configuration** folder, and click on the **Layer 3 IP Networking** folder, and then click on the **IP Interfaces Table** link to open the following window:

Figure 7- 2. IP Interface Table window

To setup a new IP interface, click the **Add** button. To edit an existing IP Interface entry, click on an entry under the Interface Name heading. Both actions will result in the same screen to configure, as shown below.

Figure 7- 3. IP Interface Configuration – Add window

Figure 7- 4. IP Interface Configuration – Edit 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 State pull-down menu to *Enabled* and click **Apply** to enter to make the IP interface effective. To view entries in the IP Interface Table, click the Show All IP Interface Entries hyperlink. Use the **Save Settings** window from the **Maintenance** folder to enter the changes into NV-RAM.

The following fields can be set:

Parameter	Description
Interface Name	This field displays the name for the IP interface. The default IP interface is named "System".
IP Address	This field allows the entry of an IP address to be assigned to this IP interface.
Subnet Mask	This field allows the entry of a subnet mask to be applied to this IP interface.
VLAN Name	This field allows the entry of the VLAN Name for the VLAN the IP interface belongs to.
Secondary	Use the pull-down menu to set the IP interface as *True* or *False*. *True* will set the interface as secondary and *False* will denote the interface as the primary interface of

	the VLAN entered above. *Secondary* interfaces can only be configured if a *primary* interface is first configured.
State *<Disabled>*	This field may be altered between *Enabled* and *Disabled* using the pull-down menu. This entry determines whether the interface will be active or not.
Link Status *<Link UP>*	This read-only field states the current status of the IP Interface on the Switch. *Link Up* denotes that the IP interface is up and running on the Switch. *Link Down* will denote that the IP interface is not currently set and/or enabled on the Switch.

Click **Apply** to implement changes made.

MD5 Key Table Configuration

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 can be used in the **OSPF Interface Configuration** window below.

To configure an MD5 Key, click the **MD5 Key Table Configuration** link to open the following window:

Figure 7- 5. MD5 Key Setting window

The following fields can be set:

Parameter	Description
Key ID (1-255)	A number from *1* to *255* used to identify the MD5 Key.
Key	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.

Click **Apply** to enter the new Key ID settings. To delete a Key ID entry, click the corresponding ✕ under the Delete heading.

Route Redistribution Settings

Route redistribution allows routers on the network, which 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 Switch 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 DXS-3326GSR switch is also redistributed.

Routing information source – OSPF and the Static Route table. Routing information will be redistributed to RIP. The following table lists the allowed values for the routing metrics and the types (or forms) of the routing information that will be redistributed.

Route Source	Metric	Type
OSPF	0 to 16	All Internal External ExtType1 ExtType2 Inter-E1 Inter-E2
RIP	0 to 16777214	Type 1 Type 2
Static	0 to 16777214	Type 1 Type 2
Local	0 to 16777214	Type 1 Type 2

Table 7- 3. Route Redistribution Source table

Entering the Type combination – internal type_1 type_2 is functionally equivalent to all. Entering the combination type_1 type_2 is functionally equivalent to external. Entering the combination internal external is functionally equivalent to all.

Entering the metric 0 specifies transparency.

This window will redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. To access the **Route Redistribution Settings** window, go to **Configuration > Layer 3 IP Networking > Route Redistribution Settings**:

Figure 7- 6. Route Redistribution Settings window

The following parameters may be set or viewed:

Parameter	Description
Dest Protocol	Allows for the selection of the protocol for the destination device. Choose between *RIP* and *OSPF.*
Src Protocol	Allows for the selection of the protocol for the source device. Choose between *RIP*, *OSPF, Static* and *Local*.
Type	Allows for the selection of one of six methods of calculating the metric value. The user may choose between *All*, *Internal*, *External*, *ExtType1*, *ExtType2*, *Inter-E1*, *Inter-E2*. See the table above for available metric value types for each source protocol.
Metric (0-16)	Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.

Click **Add/Modify** to implement changes made.

NOTE: The source protocol (Src Protocol) entry and the destination protocol (Dest Protocol) entry cannot be the same.

Static/Default Route

Entries into the Switch's forwarding table can be made using both MAC addresses and IP addresses. Static IP forwarding is accomplished by the entry of an IP address into the Switch's **Static IP Routing Table**.

Figure 7- 7. Static/Default Route Settings window

This window shows the following values:

Parameter	Description
IP Address	The IP address of the Static/Default Route.
Subnet Mask	The corresponding Subnet Mask of the IP address entered into the table.
Gateway	The corresponding Gateway of the IP address entered into the table.
Hops	Represents the metric value of the IP interface entered into the table. This field may read a number between 1-65535 for an OSPF setting, and 1-16 for a RIP setting.
Protocol	Represents the protocol used for the Routing Table entry of the IP interface. This field may read Static or Local.
Backup State	Represents the Backup state that this IP interface is configured for. This field may read Primary or Backup.
Delete	Click the ✕ if you would like to delete this entry from the Static/Default Route Settings table.

To enter an IP Interface into the Switch's **Static/Default Route Settings** window, click the **Add** button, revealing the following window:

Figure 7- 8. Static/Default Route Settings – Add window

The following fields can be set:

Parameter	Description
IP Address <*0.0.0.0*>	Allows the entry of an IP address that will be a static entry into the Switch's Routing Table.
Subnet Mask <*0.0.0.0*>	Allows the entry of a subnet mask corresponding to the IP address above.
Gateway IP <*0.0.0.0*>	Allows the entry of an IP address of a gateway for the IP address above.
Metric (1-65535) < *1* >	Allows the entry of a routing protocol metric representing the number of routers between the Switch and the IP address above.
Backup State <*Primary*>	The user may choose between *Primary* and *Backup.* If the Primary Static/Default Route fails, the Backup Route will support the entry. Please note that the Primary and Backup entries cannot have the same Gateway.

Click **Apply** to implement changes made.

Route Preference Setting

Route Preference is a way for routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. The majority of routing protocols are not compatible when used in conjunction with each other. This Switch supports and may be configured for many routing protocols, as a stand-alone switch or more importantly, in utilizing the stacking function and Single IP Managemant of the Switch. Therefore, the ability to exchange route information and select the best path is essential to optimal use of the Switch and its capabilities.

The first decision the Switch will make in selecting the best path is to consult the Route Preference Settings table of the switch. This table can be viewed by clicking **Configuration > Layer 3 IP Networking > Route Preference Settings**, and it holds the list of possible routing protocols currently implemented on the Switch, along with a Preference value which determines which routing protocol will be the most dependable to route packets. Below is a list of the default route preferences set on the Switch.

Route Type	Validity Range	Default Value
Local	0 - Permanently set on the switch and unconfigurable.	0
Static	1 - 999	60
OSPF Intra	1 - 999	80
OSPF Inter	1 - 999	90
RIP	1 - 999	100
OSPF ExtT1	1 - 999	110
OSPF ExtT2	1 - 999	115

As shown above, *Local* will always be the first choice for routing purposes and the next most reliable path is *Static* due to the fact that its has the next lowest value. To set a higher reliability for a route, change its value to a number less than the value of a route preference that has a greater reliability value using the **Current Route Preference Settings** window fields. For example, if the user wishes to make RIP the most reliable route, the user can change its value to one that is less than the lowest value (Static - 60) or the user could change the other route values to more than 100.

The user should be aware of three points before configuring the route preference:

1. No two route preference values can be the same. Entering the same route preference may cause the switch to crash due to indecision by the switch.

2. If the user is not fully aware of all the features and functions of the routing protocols on the switch, a change in the default route preference value may cause routing loops or black holes.

3. After changing the route preference value for a specific routing protocol, that protocol needs to be restarted because the previously learned routes have been dropped from the switch. The switch must learn the routes again before the new settings can take affect.

To view the **Current Route Preference Settings** window, click **Configuration > Layer 3 IP Networking > Route Preference Settings:**

Figure 7- 9. Current Route Preference Settings window

The following fields can be viewed or set:

Parameter	Description
RIP (1-999)	Enter a value between *1* and *999* to set the route preference for RIP. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is *100*.
OSPF Intra (1-999)	Enter a value between *1* and *999* to set the route preference for OSPF Intra-area route. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is *80*.
Static (1-999)	Enter a value between *1* and *999* to set the route preference for Static route. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is *60*.
OSPF Inter (1-999)	Enter a value between *1* and *999* to set the route preference for OSPF Inter-area route. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is *90*.
OSPF ExtT1 (1-999)	Enter a value between *1* and *999* to set the route preference for OSPF AS external route type 1. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is *110*.

OSPF ExtT2 (1-999)	Enter a value between *1* and *999* to set the route preference for OSPF AS external route type 2. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is *115*.

Click **Apply** to implement changes made.

Static ARP Settings

The Address Resolution Protocol (ARP) is a TCP/IP protocol that converts IP addresses into physical addresses. This table allows network managers to view, define, modify and delete ARP information for specific devices.

Static entries can be defined in the ARP Table. When static entries are defined, a permanent entry is entered and is used to translate IP address to MAC addresses.

To open the **Static ARP Settings** window, open the **Configuration** folder, and then open the **Layer 3 IP Networking** folder and click on the **Static ARP Table** link.

Figure 7- 10. Static ARP Settings window

To add a new entry, click the Add button, revealing the following window to configure:

Figure 7- 11. Static ARP Table – Add a New Entry window

The following fields can be set:

Parameter	Description
IP Address	The IP address of the ARP entry.
MAC Address	The MAC address of the ARP entry.

After entering the IP Address and MAC Address of the Static ARP entry, click **Apply** to implement the new entry. To completely clear the Static ARP Settings, click the **Clear All** button.

RIP

The Routing Information Protocol is a distance-vector routing protocol. There are two types of network devices running RIP - active and passive. Active devices advertise their routes to others through RIP messages, while passive devices listen to these messages. Both active and passive routers update their routing tables based upon RIP messages that active routers exchange. Only routers can run RIP in the active mode.

Every 30 seconds, a router running RIP broadcasts a routing update containing a set of pairs of network addresses and a distance (represented by the number of hops or routers between the advertising router and the remote network). So, the vector is the network address and the distance is measured by the number of routers between the local router and the remote network.

RIP measures distance by an integer count of the number of hops from one network to another. A router is one hop from a directly connected network, two hops from a network that can be reached through a router, etc. The more routers between a source and a destination, the greater the RIP distance (or hop count).

There are a few rules to the routing table update process that help to improve performance and stability. A router will not replace a route with a newly learned one if the new route has the same hop count (sometimes referred to as 'cost'). So learned routes are retained until a new route with a lower hop count is learned.

When learned routes are entered into the routing table, a timer is started. This timer is restarted every time this route is advertised. If the route is not advertised for a period of time (usually 180 seconds), the route is removed from the routing table.

RIP does not have an explicit method to detect routing loops. Many RIP implementations include an authorization mechanism (a password) to prevent a router from learning erroneous routes from unauthorized routers.

To maximize stability, the hop count RIP uses to measure distance must have a low maximum value. Infinity (that is, the network is unreachable) is defined as 16 hops. In other words, if a network is more than 16 routers from the source, the local router will consider the network unreachable.

RIP can also be slow to converge (to remove inconsistent, unreachable or looped routes from the routing table) because RIP messages propagate relatively slowly through a network.

Slow convergence can be solved by using split horizon update, where a router does not propagate information about a route back to the interface on which it was received. This reduces the probability of forming transient routing loops.

Hold down can be used to force a router to ignore new route updates for a period of time (usually 60 seconds) after a new route update has been received. This allows all routers on the network to receive the message.

A router can 'poison reverse' a route by adding an infinite (16) hop count to a route's advertisement. This is usually used in conjunction with triggered updates, which force a router to send an immediate broadcast when an update of an unreachable network is received.

RIP Version 1 Message Format

There are two types of RIP messages: routing information messages and information requests. Both types use the same format.

The Command field specifies an operation according the following table:

Command	Meaning
1	Request for partial or full routing information
2	Response containing network-distance pairs from sender's routing table
3	Turn on trace mode (obsolete)
4	Turn off trace mode (obsolete)
5	Reserved for Sun Microsystem's internal use
9	Update Request
10	Update Response
11	Update Acknowledgement

RIP Command Codes

The field Version contains the protocol version number (1 in this case), and is used by the receiver to verify which version of RIP the packet was sent.

RIP 1 Message

RIP is not limited to TCP/IP. Its address format can support up to 14 octets (when using IP, the remaining 10 octets must be zeros). Other network protocol suites can be specified in the Family of Source Network field (IP has a value of 2). This will determine how the address field is interpreted.

RIP specifies that the IP address, 0.0.0.0, denotes a default route.

The distances, measured in router hops are entered in the Distance to Source Network, and Distance to Destination Network fields.

RIP 1 Route Interpretation

RIP was designed to be used with classed address schemes, and does not include an explicit subnet mask. An extension to version 1 does allow routers to exchange subnetted addresses, but only if the subnet mask used by the network is the same as the subnet mask used by the address. This means the RIP version 1 cannot be used to propagate classless addresses.

Routers running RIP version 1 must send different update messages for each IP interface to which it is connected. Interfaces that use the same subnet mask as the router's network can contain subnetted routes, other interfaces cannot. The router will then advertise only a single route to the network.

RIP Version 2 Extensions

RIP version 2 includes an explicit subnet mask entry, so RIP version 2 can be used to propagate variable length subnet addresses or CIDR classless addresses. RIP version 2 also adds an explicit next hop entry, which speeds convergence and helps prevent the formation of routing loops.

RIP2 Message Format

The message format used with RIP2 is an extension of the RIP1 format:

RIP version 2 also adds a 16-bit route tag that is retained and sent with router updates. It can be used to identify the origin of the route.

Because the version number in RIP2 occupies the same octet as in RIP1, both versions of the protocols can be used on a given router simultaneously without interference.

RIP Global Settings

To setup RIP for the IP interfaces configured on the Switch, the user must enable RIP and then configure RIP settings for the individual IP interfaces. To globally enable RIP on the Switch, open the **Configuration** folder to **Layer 3 Networking** and then open the **RIP** folder and click on the **RIP Configuration** link to access the following window:

Figure 7- 12. RIP Global Settings window

To enable RIP, simply use the pull-down menu, select *Enabled* and click **Apply**.

RIP Interface Settings

RIP settings are configured for each IP interface on the Switch. Click the **RIP Interface Settings** link in the **RIP** 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 Interface Name. To view the next page of RIP Interface Settings, click the **Next** button.

Figure 7- 13. RIP Interface Settings window

Click the hyperlinked name of the interface you want to set up for RIP, which will give access to the following window:

Figure 7- 14. RIP Interface Settings - Edit window

Refer to the table below for a description of the available parameters for RIP interface settings.

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

Parameter	Description
Interface Name	The name of the IP interface on which RIP is to be setup. This interface must be previously configured on the Switch.
IP Address	The IP address corresponding to the Interface Name showing in the field above.
TX Mode *<Disabled>*	Toggle among *Disabled*, *v1 Only*, *v1 Compatible*, and v*2 Only*. This entry specifies which version of the RIP protocol will be used to transmit RIP packets. *Disabled* prevents the transmission of RIP packets.
RX Mode *<Disabled>*	Toggle among *Disabled*, *v1 Only*, *v2 Only*, and *v1 or v2*. This entry specifies which version of the RIP protocol will be used to interpret received RIP packets. *Disabled* prevents the reception of RIP packets.
Authentication	Toggle between *Disabled* and *Enabled* to specify that routers on the network should us the Password above to authenticate router table exchanges.
Password	A password to be used to authenticate communication between routers on the network.
State	Toggle between *Disabled* and *Enabled* to disable or enable this RIP interface on the switch.

Interface Metric	A read-only field that denotes the Metric value of the current IP Interface setting.

Click **Apply** to implement changes made.

OSPF

The Open Shortest Path First (OSPF) routing protocol 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 is 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:

- 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.

- 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.

- 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.

- 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:

Cost = 100,000,000 / 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.
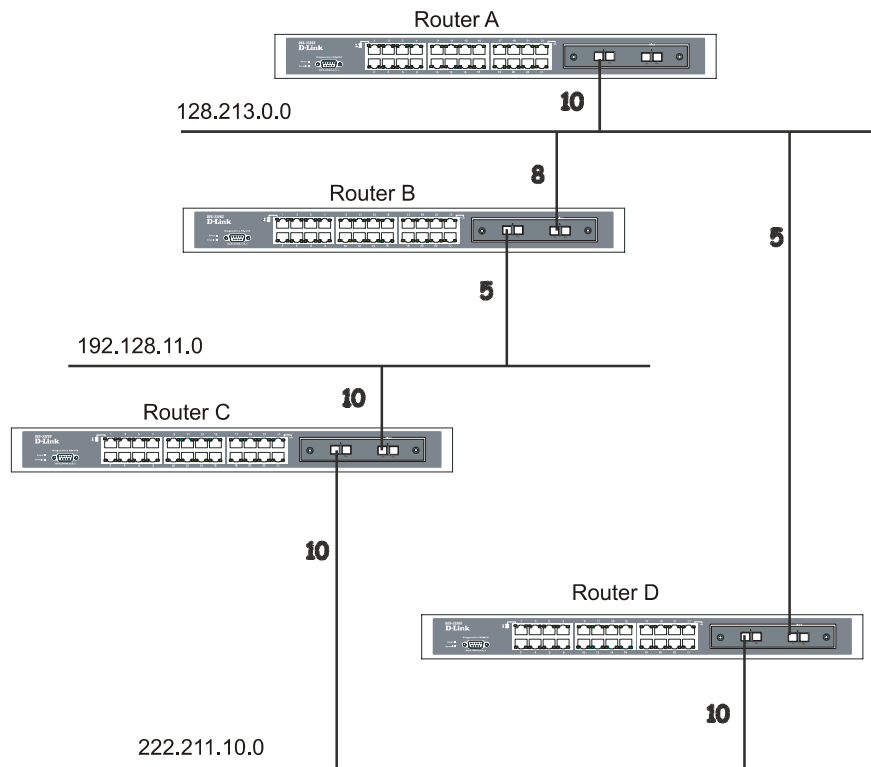
Figure 7- 15. Constructing a Shortest Path Tree
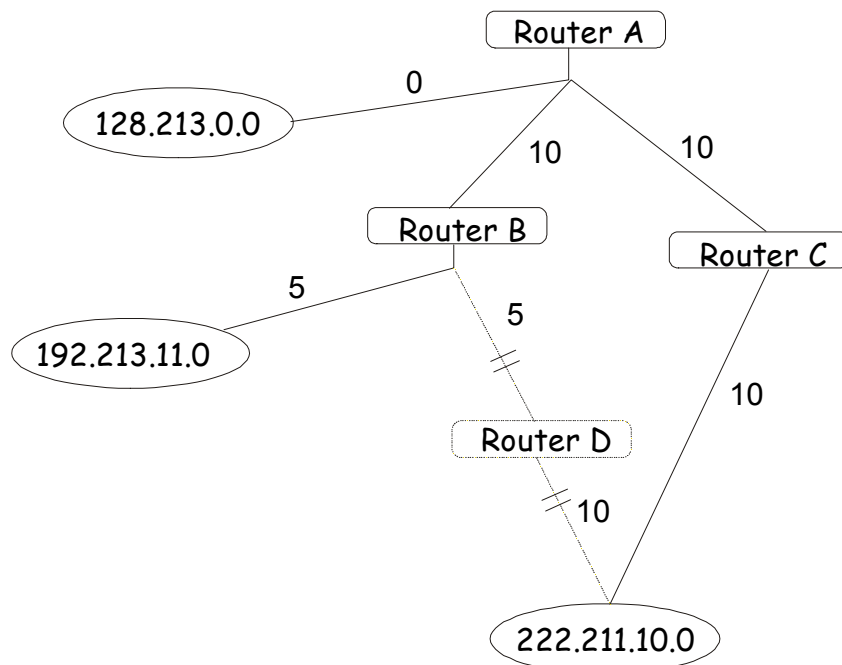
Figure 7- 16. Constructing a Shortest Path Tree

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:
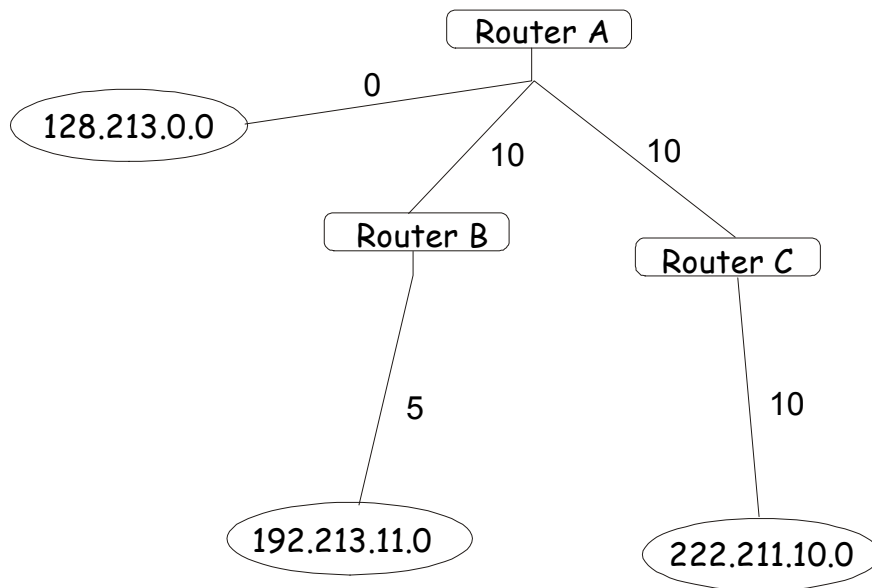
Figure 7- 17. Constructing a Shortest Path Tree - Completed

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 a number of different types of link-state packets, four of which 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:

- Linking an area that does not have a physical connection to the backbone.
- 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 is 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 the 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

- 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 OSPP packet header is shown below:
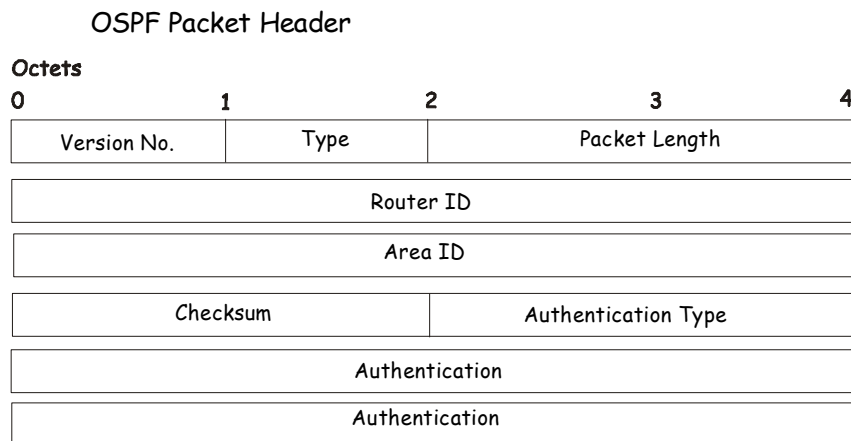
OSPF Packet Header

Figure 7- 18. OSPF Packet Header Format

Field	Description
Version No.	The OSPF version number
Type	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
Packet Length	The length of the packet in bytes. This length includes the 24-byte header.
Router ID	The Router ID of the packet's source.
Area ID	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

Checksum	A standard IP checksum that includes all of the packet's contents except for the 64-bit authentication field.
Authentication Type	The type of authentication to be used for the packet.
Authentication	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:
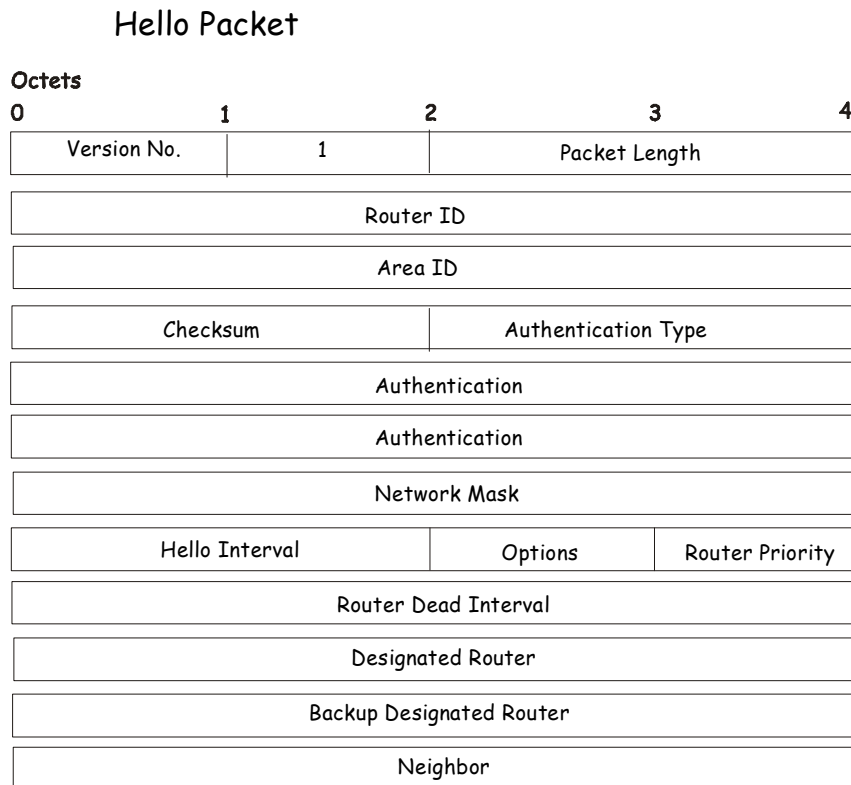
Hello Packet

Figure 7- 19. Hello Packet

Field	Description
Network Mask	The network mask associated with this interface.
Options	The optional capabilities supported by the router.
Hello Interval	The number of seconds between this router's Hello packets.
Router Priority	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 to become the DR or the BDR.

Router Dead Interval	The number of seconds that must pass before declaring a silent router as down.
Designated Router	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.
Backup Designated Router	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.
Field	Description
Neighbor	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 seconds 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.
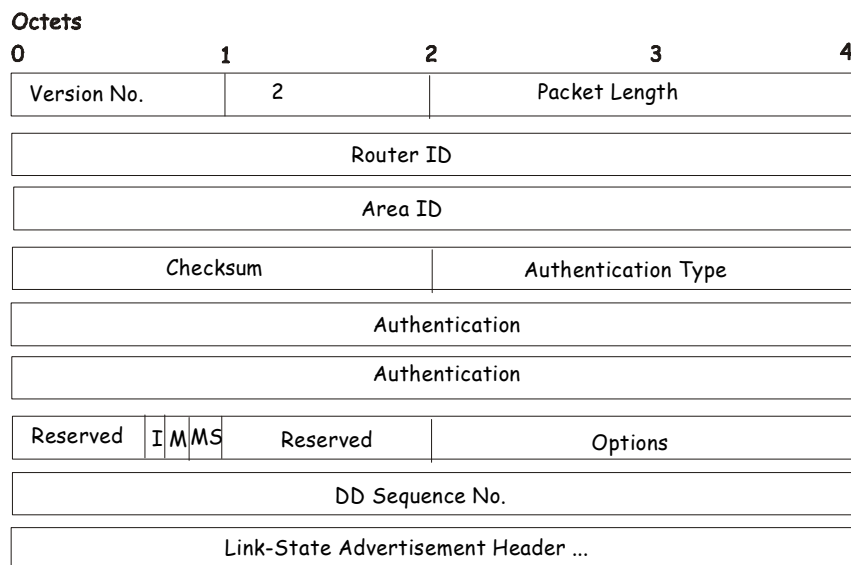
Figure 7- 20. Database Description Packet

Field	Description
Options	The optional capabilities supported by the router.
I - bit	The Initial bit. When set to 1, this packet is the first in the sequence of Database Description packets.
M - bit	The More bit. When set to 1, this indicates that more Database Description packets will follow.
MS - bit	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.

DD Sequence Number	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:

Link-State Request Packet

Figure 7- 21. 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:

Link-State Update Packet
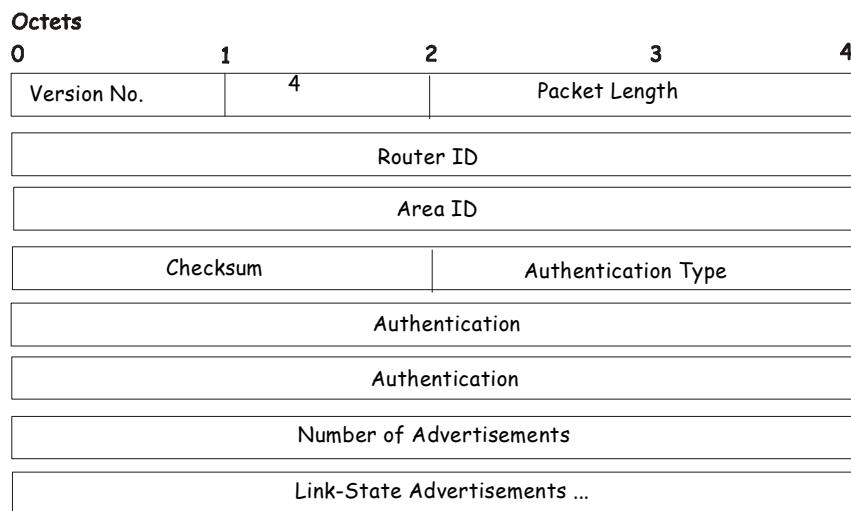
Figure 7- 22. Link-State Update Packet

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 folding 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:

Link-State Acknowledgment Packet
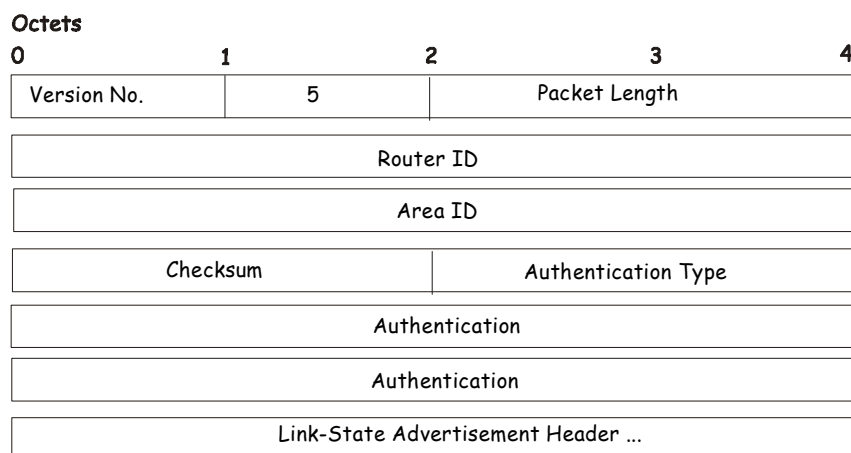
Figure 7- 23. Link State Acknowledge Packet

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:

Link-State Advertisement Header
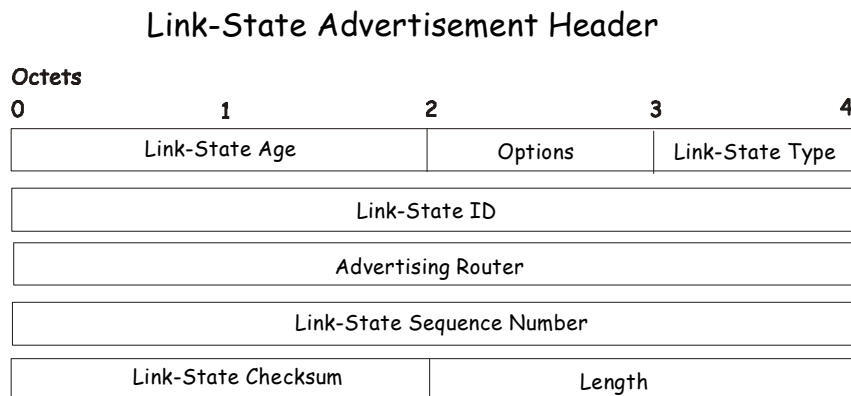
Figure 7- 24. Link State Advertisement Header

Field	Description
Link State Age	The time is seconds since the link state advertisement was originated.
Options	The optional capabilities supported by the described portion of the routing domain.
Link State Type	The type of the link state advertisement. Each link state type has a separate advertisement format.
	The link state type are as follows: Router Links, Network Links, Summary Link (IP Network), Summary Link (ASBR), AS External Link.
Link State ID	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.

Advertising Router	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.
Link State Sequence Number	Detects old or duplicate link state advertisements. Successive instances of a link state advertisement are given successive Link State Sequence numbers.
Link State Checksum	The Fletcher checksum of the complete contents of the link state advertisement, including the link state advertisement header by accepting the Link State Age field.
Length	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:
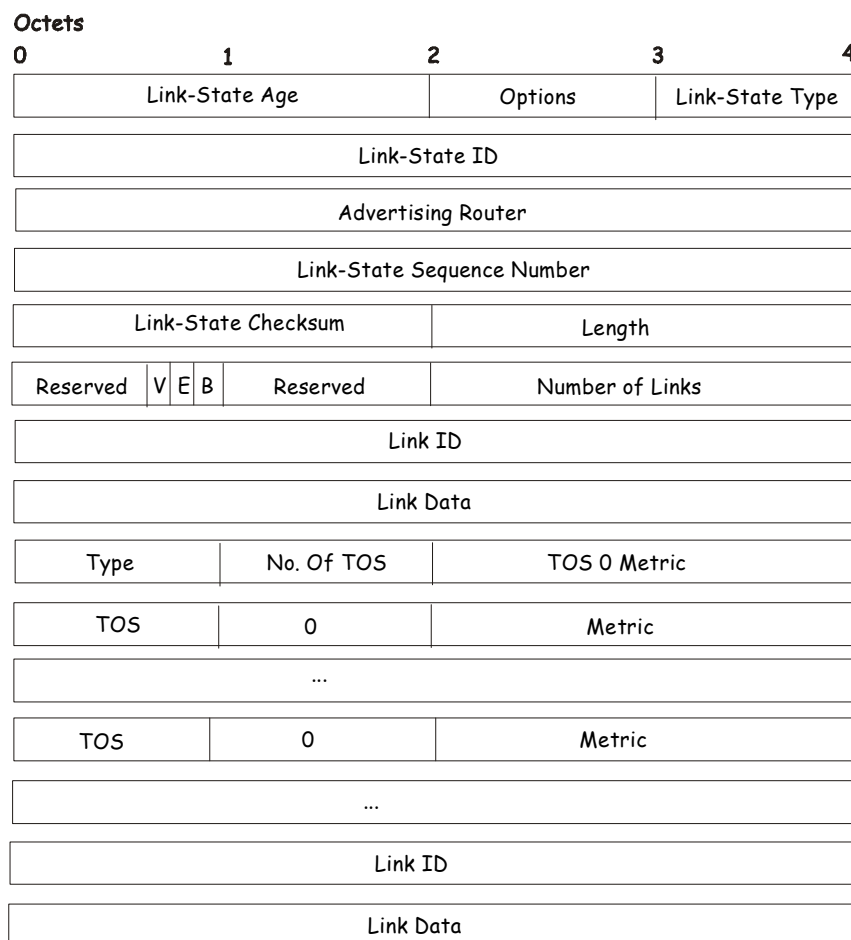
Routers Links Advertisements

Figure 7- 25. Routers Links Advertisements

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
V - bit	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).
E - bit	When set, the router is an Autonomous System (AS) boundary router (E is for External).
B - bit	When set, the router is an area border router (B is for Border).
Number of Links	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
Type	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. Virtual link.
Link ID	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. IP network/subnet number. Neighboring router's Router ID
Link Data	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.
No. of TOS	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.
TOS 0 Metric	The cost of using this router link for TOS 0.

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.

Field	Description
TOS	IP Type of Service that this metric refers to.
Metric	The cost of using this outbound router link, for traffic of the specified TOS.

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 form 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:
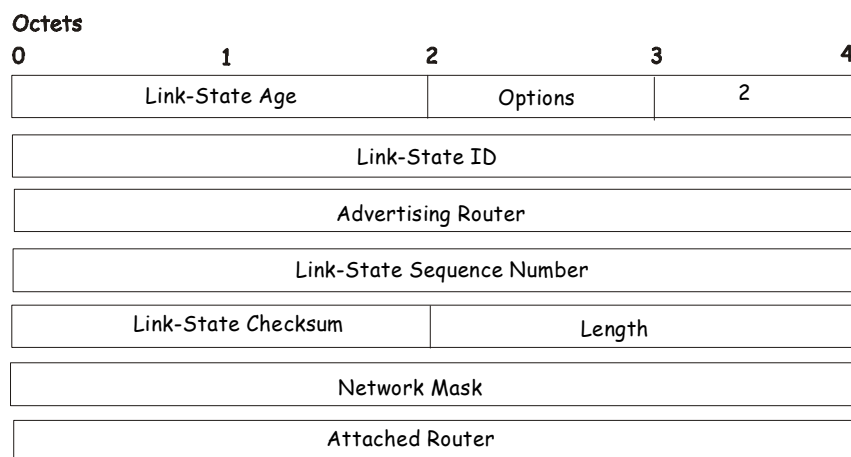
Network Link Advertisements

Figure 7- 26. Network Link Advertisements

Field	Description
Network Mask	The IP address mask for the network.
Attached Router	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 that the difference in the Link State ID field, the format of Type 3 and 4 link state advertisements is identical.

Summary Link Advertisements

```
Octets
0              1              2              3              4
┌────────────────────────────┬──────────────┬──────────────┐
│       Link-State Age        │   Options    │      2       │
├────────────────────────────┴──────────────┴──────────────┤
│                       Link-State ID                       │
├───────────────────────────────────────────────────────────┤
│                     Advertising Router                    │
├───────────────────────────────────────────────────────────┤
│                 Link-State Sequence Number                │
├────────────────────────────┬──────────────────────────────┤
│     Link-State Checksum     │            Length            │
├────────────────────────────┴──────────────────────────────┤
│                       Network Mask                        │
├──────────────────┬────────────────────────────────────────┤
│       TOS        │                 Metric                 │
└──────────────────┴────────────────────────────────────────┘
```

Figure 7- 27. 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
Network Mask	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
TOS	The Type of Service that the following cost is relevant to.
Metric	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:
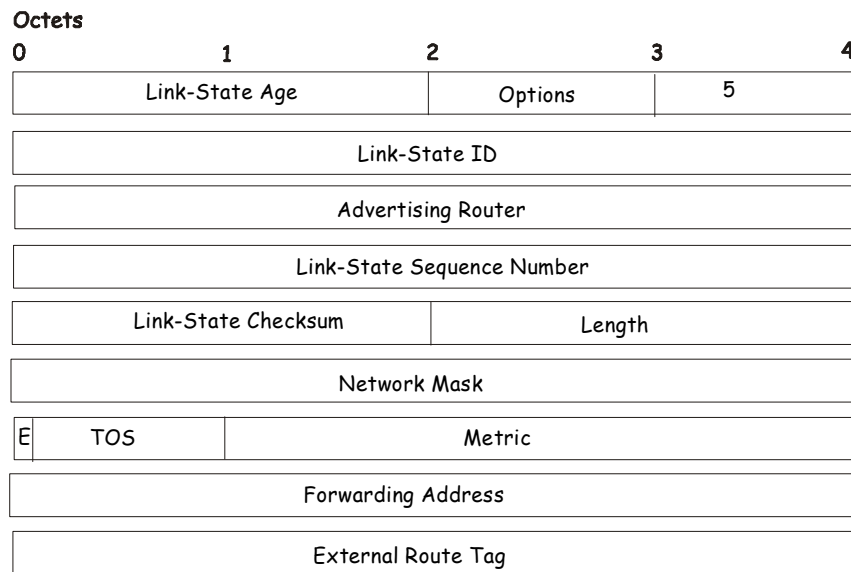
AS External Link Advertisements

Figure 7- 28. AS External Link Advertisements

Field	Description
Network Mask	The IP address mask for the advertised destination.
E - bit	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.
Forwarding Address	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.
TOS	The Type of Service that the following cost is relevant to.
Metric	The cost of this route. The interpretation of this metric depends on the external type indication (the E - bit above).
External Route Tag	A 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

OSPF Global Settings

This 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** folder and click on the **OSPF Global Settings** 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 7- 29. OSPF Global Settings window

The following parameters are used for general OSPF configuration:

Parameter	Description
OSPF Route ID	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 10.53.13.189, 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.
Current Route ID	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.
State	Allows OSPF to be enabled or disabled globally on the Switch without changing the OSPF configuration.

OSPF Area ID Setting

This menu 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. 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 **Configuration > Layer 3 IP Networking > OSPF > OSPF Area ID Settings** link to open the following window:

Figure 7- 30. OSPF Area ID 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 ✕ 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.

Figure 7- 31. OSPF Area ID Setting Example window

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

The Area ID settings are as follows:

Parameter	Description
Area ID	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.
Type	This field can be toggled between Normal and Stub using the space bar. When it is toggled to Stub, additional fields appear – Stub Import Summary LSA, and Default Cost.
Stub Import Summary LSA	Displays whether or not the selected Area will allow Summary Link-State Advertisements (Summary LSAs) to be imported into the area from other areas.
Stub Default Cost	Displays the default cost for the route to the stub of between *0* and *65,535*. The default is *1*.

OSPF Interface Settings

To set up OSPF interfaces, click **Configuration > Layer 3 IP Networking > OSPF > OSPF Interface Settings** 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 window for that interface.

Figure 7- 32. OSPF Interface Settings window

Figure 7- 33. OSPF Interface Settings – Edit window

Configure each IP interface individually using the **OSPF Interface Settings - Edit** menu. Click the **Apply** button when you have entered the settings. The new configuration appears listed in the **OSPF Interface Settings** window. To return to that 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
Interface Name	Displays the of an IP interface previously configured on the Switch.
Area ID	Allows the entry of an OSPF Area ID configured above.
Router Priority (0-255)	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.
Hello Interval (1-65535)	Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between *1* 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.
Dead Interval (1-65535)	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 *1* and *65535* seconds can be specified. The Dead Interval must be evenly

153

	divisible by the Hello Interval.
State	Allows the OSPF interface to be disabled for the selected area without changing the configuration for that area.
Auth. Type	This field can be toggled between *None*, *Simple*, and *MD5* using the space bar. This allows a choice of authorization schemes for OSPF packets that may be exchanged over the OSPF routing domain. *None* specifies no authorization. *Simple* uses a simple password to determine if the packets are from an authorized OSPF router. When *Simple* 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. *MD5* uses a cryptographic key entered in the **MD5 Key Setting** window. When *MD5* 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.
Auth. Key ID	Enter a Key ID of up to 5 characters to set the Auth. Key ID for either the Simple Auth Type or the MD5 Auth Type, as specified in the previous parameter.
Metric (1-65535)	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*.
DR State	A read-only field describing the Designated Router state of the IP interface. This field many read DR if the interface is the designated router, or Backup DR if the interface is the Backup Designated Router. The highest IP address will be the Designated Router and is determined by the OSPF Hello Protocol of the Switch.
DR Address	The IP address of the aforementioned Designated Router.
Backup DR Address	The IP address of the aforementioned Backup Designated Router.
Transmit Delay	A read-only field that denotes the estimated time to transmit a Link State Update Packet over this interface, in seconds.
Retransmit Time	A read-only field that denotes the time between LSA retransmissions over this interface, in seconds.

OSPF Virtual Interface Settings

Click the **OSPF Virtual Interface Setting**s 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 one used to add a new set. To eliminate an existing configuration, click the ✕ in the Delete column.

Figure 7- 34. OSPF Virtual Interface Configuration

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

Figure 7- 35. OSPF Virtual Link Setting – Add window

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

Parameter	Description
Transit Area ID	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.
Neighbor Router ID	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.
Hello Interval (1-65535)	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.
Dead Interval (1-65535)	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.
Auth Type	If using authorization for OSPF routers, select the type being used. MD5 key authorization must be set up in the **MD5 Key Setting** window.
Password/Auth. Key ID	Enter a case-sensitive password for simple authorization or enter the MD5 key you set in the MD5 Key settings menu.
Transmit Delay	The number of seconds required to transmit a link state update over this virtual link. Transit delay takes into account transmission and propagation delays. This field is fixed at 1 second.
RetransInterval	The number of seconds between link state advertisement retransmissions for adjacencies belonging to this virtual link. This field is fixed at 5 seconds.

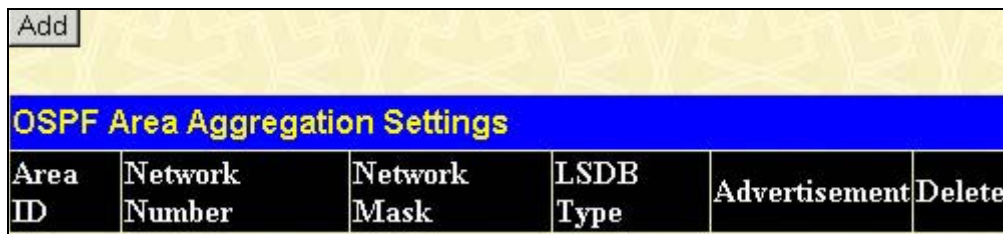Click **Apply** to implement changes made.

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 menu. 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 one used to add
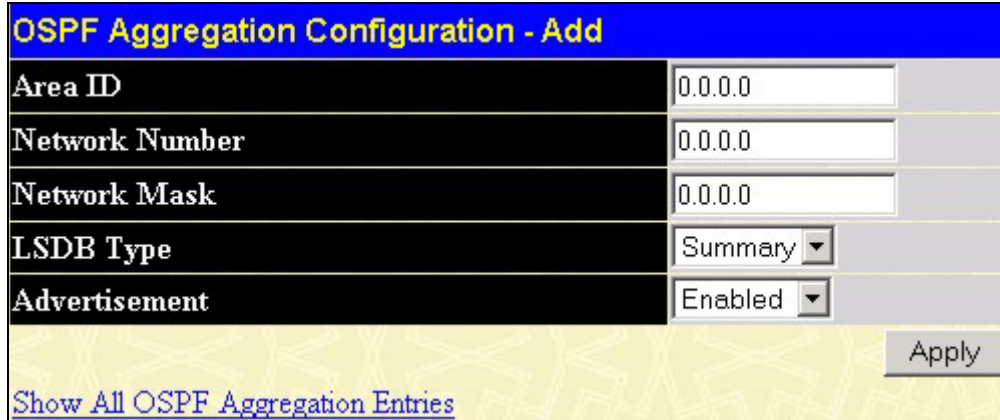
a new configuration. To eliminate an existing configuration, click the ✕ in the Delete column for the configuration being removed.

Figure 7- 36. OSPF Area Aggregation Settings window

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

Figure 7- 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 this table 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
Area ID	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.
Network Number	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.

Network Mask	The corresponding network mask for the Network Number specified above.
LSDB Type	Specifies the type of address aggregation, which is set at *Summary*.
Advertisement	Select *Enabled* or *Disabled* to determine whether the selected OSPF Area will advertise it's 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 window 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.
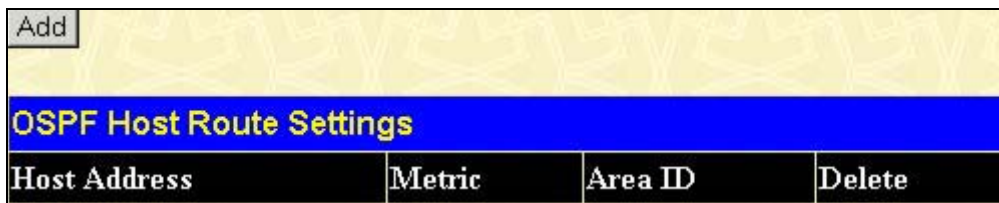

Figure 7- 38. OSPF Host Route Settings window

Use the menu below to set up OSPF host routes.

Figure 7- 39. OSPF Host Route Setting – 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. 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
Host Address	The IP address of the OSPF host.
Metric	A value between *1* and *65535* that will be advertised for the route.
Area ID	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

The BOOTP hops count limit allows the maximum number of hops (routers) that the BOOTP messages can be relayed through to be set. If a packet's hop count is more than the hop count limit, the packet is dropped. The range is between 1 and 16 hops, with a default value of 4. The relay time threshold sets the minimum time (in seconds) that the Switch will wait before forwarding a BOOTP request packet. If the value in the seconds field of the packet is less than the relay time threshold, the packet will be dropped. The range is between 0 and 65,535 seconds, with a default value of 0 seconds.

DHCP/BOOTP Global Settings

To enable and configure BOOTP or DHCP on the Switch, click **Configuration** > **DHCP/BOOTP Relay** > **DHCP/BOOTP Global Settings**:

Figure 7- 40. DHCP/Bootp Global Settings window

The following fields can be set:

Parameter	Description
BOOTP Relay Status *<Disabled>*	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the BOOTP/DHCP Relay service on the Switch. The default is *Disabled*
BOOTP HOPS Count Limit (1-16) *<4 >*	This field allows an entry between *1* and *16* to define the maximum number of router hops BOOTP messages can be forwarded across. The default hop count is *4*.
BOOTP Relay Time Threshold (0-65535) *<0>*	Allows an entry between *0* and *65535* seconds, and defines the maximum time limit for routing a BOOTP/DHCP packet. If a value of *0* is entered, the Switch will not process the value in the seconds field of the BOOTP or DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given BOOTP or DHCP packet.

DHCP/BOOTP Relay Settings

The DHCP/BOOTP Relay settings allow the user to set up a server, by IP address, for relaying DHCP/BOOTP information to the Switch. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP/BOOTP server using the following window. Properly configured settings will be displayed in the BOOTP Relay Table at the bottom of the following window, once the user clicks the **Add** button. The user may add up to four Server IPs per IP interface on the Switch. Entries may be deleted by clicking its corresponding ✕.

Figure 7- 41. DHCP/BOOTP Relay Settings window

The following parameters may be configured or viewed.

Parameter	Description
Interface	The IP interface on the Switch that will be connected directly to the Server.
Server IP	Enter the IP address of the DHCP/BOOTP server. Up to four Server IPs can be configured per IP Interface

DNS Relay

Computer users usually prefer to use text names for computers they may want to open a connection with. Computers themselves, require 32-bit IP addresses. Somewhere, a database of network devices' text names and their corresponding IP addresses must be maintained.

The Domain Name System (DNS) is used to map names to IP addresses throughout the Internet and has been adapted for use within intranets.

For two DNS servers to communicate across different subnets, the DNS Relay of the Switch must be used. The DNS servers are identified by IP addresses.

Mapping Domain Names to Addresses

Name-to-address translation is performed by a program called a Name server. The client program is called a Name resolver. A Name resolver may need to contact several Name servers to translate a name to an address.

The Domain Name System (DNS) servers are organized in a somewhat hierarchical fashion. A single server often holds names for a single network, which is connected to a root DNS server - usually maintained by an ISP.

Domain Name Resolution

The domain name system can be used by contacting the name servers one at a time, or by asking the domain name system to do the complete name translation. The client makes a query containing the name, the type of answer required, and a code specifying whether the domain name system should do the entire name translation, or simply return the address of the next DNS server if the server receiving the query cannot resolve the name.

When a DNS server receives a query, it checks to see if the name is in its sub domain. If it is, the server translates the name and appends the answer to the query, and sends it back to the client. If the DNS server cannot translate the name, it determines what type of name resolution the client requested. A complete translation is called recursive resolution and requires the server to contact other DNS servers until the name is resolved. Iterative resolution specifies that if the DNS server cannot supply an answer, it returns the address of the next DNS server the client should contact.

Each client must be able to contact at least one DNS server, and each DNS server must be able to contact at least one root server.

The address of the machine that supplies domain name service is often supplied by a DHCP or BOOTP server, or can be entered manually and configured into the operating system at startup.

DNS Global Settings

To configure the DNS function on the Switch, open the **Configuration** folder and click the **DNS Relay** folder. In this folder, click the **DNS Global Settings** link to open the following window.

Figure 7- 42. DNS Global Settings window

The following fields can be set:

Parameter	Description
DNS Relay Status *<Disabled>*	This field can be toggled between *Disabled* and *Enabled* using the pull-down menu, and is used to enable or disable the DNS Relay service on the Switch.
Primary Name Server *<0.0.0.0>*	Allows the entry of the IP address of a primary domain name server (DNS).
Secondary Name Server *<0.0.0.0>*	Allows the entry of the IP address of a secondary domain name server (DNS).
DNSR Cache Status *<Disabled>*	This can be toggled between *Disabled* and *Enabled.* This determines if a DNS cache will be enabled on the Switch.
DNS Static Table Status *<Disabled>*	This field can be toggled using the pull-down menu between *Disabled* and *Enabled.* This determines if the static DNS table will be used or not.

DNS Relay Static Setting

To view the DNS Relay Static Settings, open the **DNS Relay** folder in the **Configuration** folder and click the **DNS Relay Static Setting** link, which will open the following window.

Figure 7- 43. DNS Relay Static Settings window

To add an entry into the **DNS Relay Static Table**, simply enter a Domain Name with its corresponding IP address and click **Apply**. A successful entry will be presented in the table below, as shown in the example above. To erase an entry from the table, click the ✕ corresponding of the entry you wish to delete.

VRRP

VRRP or Virtual Routing Redundancy Protocol 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 Global Settings

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

Figure 7- 44. VRRP Global Settings window

The following fields can be set:

Parameter	Description
Global VRRP	Use the pull-down menu to enable or disable VRRP globally on the Switch. The default is *Disabled*.
Non-owner response PING	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 *Disabled* by default.

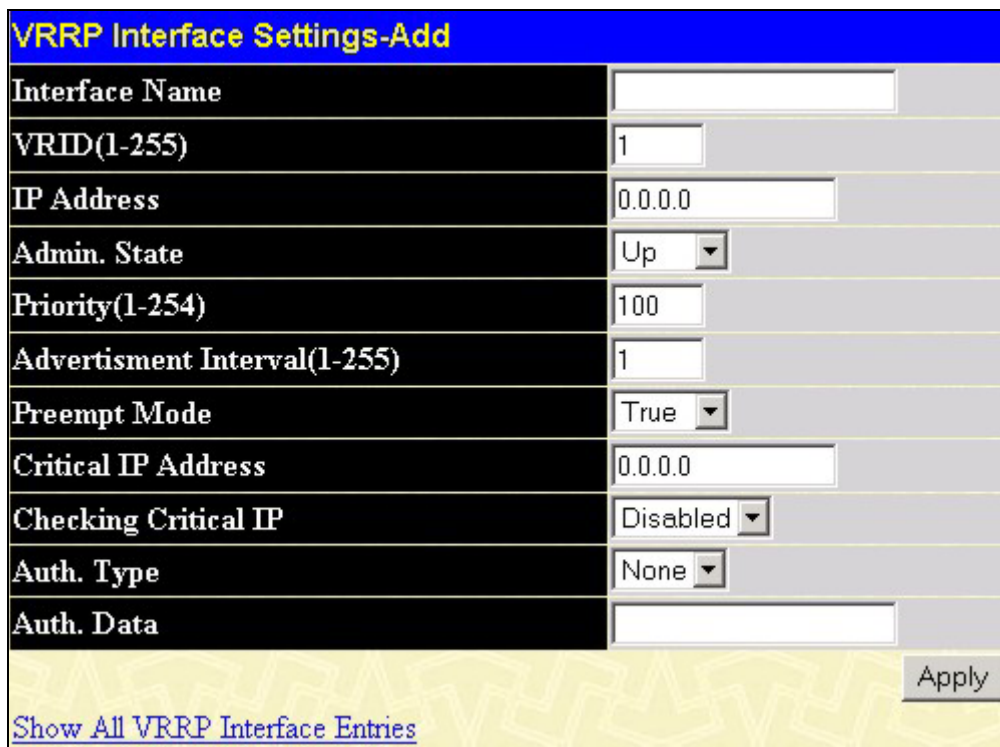Click **Apply** to implement changes made.

VRRP Configuration

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

Figure 7- 45. VRRP Configuration window

The following fields are displayed in the window above:

Parameter	Description
Interface Name	An IP interface name that has been enabled for VRRP. This entry must have been previously set in the **IP Interface Table** window.
Authentication type	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.
VRID	Displays the virtual router ID set by the user. This will uniquely identify the VRRP Interface on the network.
Display	Click the View button to display the settings for this particular VRRP entry.
Delete	Click the X to delete this VRRP entry.

Click the **Add** button to display the following window to configure a VRRP interface.

Figure 7- 46. VRRP Interface Settings – Add window

Or, the user may click the hyperlinked Interface Name to view the same window:

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

Parameter	Description
Interface Name	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.

	This IP interface must be assigned to a VLAN on the Switch.
VRID (1-255)	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 VRID value. This value MUST be different from other VRRP groups set on the Switch.
IP Address	Enter the IP address that will be assigned to the VRRP router. 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.
Admin. State	Used to enable (*Up*) and disable (*Down*) the VRRP IP interface on the Switch.
Priority (1-254)	Enter a value between *1* and *254* 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*. (The value of *255* is reserved for the router that owns the IP address associated with the virtual router and is therefore set automatically.)
Advertisement Interval (1-255)	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. The default is *1* second.
Preempt Mode	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 *True* 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 *False* 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 *True*.
Critical IP Address	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, the virtual router will be disabled automatically. A new Master should be elected from the back routers participating in the VRRP group. 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.
Checking Critical IP	Use the pull-down menu to enable or disable the Critical IP address entered above.
Auth. Type	Specifies the type of authentication used. The Auth. Type must be consistent with all routers participating within the VRRP group. The choices are: • *None* - Selecting this parameter indicates that VRRP protocol exchanges will not be authenticated. • *Simple* - 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. • *IP* - 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.
Auth. Data	This field is only valid if the user selects *Simple* or *IP* in the Auth. Type field. *Simple*

	will require the user to enter an alphanumeric string of no more than 8 characters to identify VRRP packets received by a router. *IP* will require the user to enter a MD5 message digest for authentication in comparing VRRP messages received by the router. The Authentication Type and Data must be identical for each IP interface.

Click **Apply** to implement changes made.

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

VRRP Interface Entry Display	
Interface Name	Darren
Authentication type	No Authentication
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	10.53.13.126
Checking Critical IP	Disabled
Advertisement Interval	1
Preempt Mode	True
Virtual Router Up Time	0

Show All VRRP Interface Entries

Figure 7- 47. VRRP Interface Entry Display window

This window displays the following information:

Parameter	Description
Interface Name	An IP interface name that has been enabled for VRRP. This entry must have been previously set in the IP Interface Settings table.
Authentication type	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.
VRID	Displays the virtual router ID set by the user. This will uniquely identify the VRRP Interface on the network.

	Interface on the network.
Virtual IP Address	The IP address of the Virtual router configured on the Switch.
Virtual MAC Address	The MAC address of the device that holds the Virtual router.
Virtual Router State	Displays the current status of the virtual router. Possible states include *Initialize*, *Master* and *Backup.*
Admin. State	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.
Priority	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.
Master IP Address	Displays the IP address of the Master router for the VRRP function.
Critical IP Address	Displays the critical IP address of the VRRP function. This address will judge if a virtual router is qualified to be a master router.
Checking Critical IP	Displays the status of the Critical IP address. May be enabled or disabled.
Advertisement Interval	Displays the time interval, in seconds, that VRRP messages are sent out to the network.
Preempt Mode	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.
Virtual Router Up Time	Displays the time, in minutes, since the virtual router has been initialized

IP Multicast Routing Protocol

The functions supporting IP multicasting are added under the **IP Multicast Routing Protocol** folder, from the **Layer 3 IP Networking** folder.

IGMP Snooping, **DVMRP**, and **PIM-DM** can be enabled or disabled on the Switch without changing the individual protocol's configuration.

IGMP Interface Settings

The Internet Group Multicasting Protocol (IGMP) can be configured on the Switch on a per-IP interface basis. To view the **IGMP Interface Table** window, open the **IP Multicast Routing Protocol** folder under **Configuration** and click **IGMP Interface Settings**. Each IP interface configured on the Switch is displayed in the below **IGMP Interface Table** window.

Figure 7- 48. IGMP Interface Table window

To configure IGMP for a particular interface, click the corresponding hyperlink for that IP interface. This will open the **IGMP Interface Configuration** window:

Figure 7- 49. IGMP Interface Configuration window

This window allows the configuration of IGMP for each IP interface configured on the Switch. IGMP can be configured as Version 1 or 2 by toggling the Version field using the pull-down menu. The length of time between queries can be varied by entering a value between 1 and 65,535 seconds in the Query Interval field. The maximum length of time between the receipt of a query and the sending of an IGMP response report can be varied by entering a value in the Max Response Time field.

The Robustness Variable field allows IGMP to be 'tuned' for sub-networks that are expected to lose a lot of 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.

The following fields can be set:

Parameter	Description
Interface Name <*System*>	Displays the name of the IP interface that is to be configured for IGMP. This must be a previously configured IP interface.
IP Address	Displays the IP address corresponding to the IP interface name above.
Version <*2*>	Enter the IGMP version (*1* or *2*) that will be used to interpret IGMP queries on the interface.
Query Interval (1-65535) <*125*>	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.

Max Response Time (1-25) <*10*>	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.
Robustness Variable (1-255) <*2*>	A tuning variable to allow for subnetworks that are expected to lose a large number of packets. A value between *2* and *255* can be entered, with larger values being specified for subnetworks that are expected to lose larger numbers of packets.
Last Member Query Interval (1-25) <*1*>	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. A value between *1* and *25*. The default is *1* second.
State <*Disabled*>	This field can be toggled between *Enabled* and *Disabled* and enables or disables IGMP for the IP interface. The default is *Disabled*.

DVMRP Global Settings

To enable DVMRP globally on the Switch, open the **IP Multicast Routing Protocol** folder in the **Configuration** folder, and click the **DVMR Configuration** link. This will give the user access to the following screen:

Figure 7- 50. DVMRP Global Settings window

Use the pull-down menu, choose *Enabled*, and click **Apply** to implement the DVMRP function on the Switch.

DVMRP Interface Settings

The Distance Vector Multicast Routing Protocol (DVMRP) is a hop-based method of building multicast delivery trees from multicast sources to all nodes of a network. Because the delivery trees are 'pruned' and 'shortest path', DVMRP is relatively efficient. Because multicast group membership information is forwarded by a distance-vector algorithm, propagation is slow. DVMRP is optimized for high delay (high latency) relatively low bandwidth networks, and can be considered as a 'best-effort' multicasting protocol.

DVMRP resembles the Routing Information Protocol (RIP), but is extended for multicast delivery. DVMRP builds a routing table to calculate 'shortest paths' back to the source of a multicast message and defines "route cost" (it is similar to, but not defined as, the hop count in RIP) as a relative number that represents the real cost of using this route in the construction of a multicast delivery tree to calculate which branches of a multicast delivery tree should be 'pruned' - once the delivery tree is established.

When a sender initiates a multicast, DVMRP initially assumes that all users on the network will want to receive the multicast message. When an adjacent router receives the message, it checks its unicast routing table to determine the interface that gives the shortest path (lowest cost) back to the source. If the multicast was received over the shortest path, then the adjacent router enters the information into its tables and forwards the message. If the message is not received on the shortest path back to the source, the message is dropped.

Route cost is a relative number that is used by DVMRP to calculate which branches of a multicast delivery tree should be 'pruned'. The 'cost' is relative to other costs assigned to other DVMRP routes throughout the network.

The higher the route cost, the lower the probability that the current route will be chosen to be an active branch of the multicast delivery tree (not 'pruned') - if there is an alternative route.

To view the **DVMRP Interface Settings** window, open the **IP Multicast Routing Protocol** folder under **Configuration** and click **DVMRP Interface Settings**. This window allows the Distance-Vector Multicast Routing Protocol (DVMRP) to be configured for each IP interface defined on the Switch. Each IP interface configured on the Switch is displayed in the below **DVMRP Interface Settings** window. To configure DVMRP for a particular interface, click the corresponding hyperlink for that IP interface. This will open the **DVMRP Interface Settings** window:

DVMRP Interface Settings

Interface Name	IP Address	Neighbor Timeout	Probe	Metric	State
System	10.24.22.9	35	10	1	Disabled

Figure 7- 51. first DVMRP Interface Settings window

DVMRP Interface Settings

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

Apply

Show All DVMRP Interface Entries

Figure 7- 52. second DVMRP Interface Settings window

The following fields can be set:

Parameter	Description
Interface Name *<System>*	Displays the name of the IP interface for which DVMRP is to be configured. This must be a previously defined IP interface.
IP Address	Displays the IP address corresponding to the IP Interface name entered above.
Neighbor Timeout Interval (1-65535 sec) *<35>*	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.
Probe Interval (1-65535 sec) *<10>*	This field allows an entry between *1* and *65,535* seconds and defines the interval between 'probes'. The default is *10*.
Metric (1-31) *<1>*	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*.
State *<Disabled>*	This field can be toggled between *Enabled* and *Disabled* and enables or disables DVMRP for the IP interface. The default is *Disabled*.

PIM

The Protocol Independent Multicast - Dense Mode (PIM-DM) protocol should be used in networks with a low delay (low latency) and high bandwidth as PIM-DM is optimized to guarantee delivery of multicast packets, not to reduce overhead.

The PIM-DM multicast routing protocol is assumes that all downstream routers want to receive multicast messages and relies upon explicit prune messages from downstream routers to remove branches from the multicast delivery tree that do not contain multicast group members.

PIM-DM has no explicit 'join' messages. It relies upon periodic flooding of multicast messages to all interfaces and then either waiting for a timer to expire (the Join/Prune Interval) or for the downstream routers to transmit explicit 'prune'

messages indicating that there are no multicast members on their respective branches. PIM-DM then removes these branches ('prunes' them) from the multicast delivery tree.

Because a member of a pruned branch of a multicast delivery tree may want to join a multicast delivery group (at some point in the future), the protocol periodically removes the 'prune' information from its database and floods multicast messages to all interfaces on that branch. The interval for removing 'prune' information is the Join/Prune Interval.

PIM-DM Global Settings

To enable PIM-DM globally on the Switch, go to **Configuration > IP Multicast Routing Protocol > PIM > PIM-DM Configuration**. This will give the user access to the following screen:
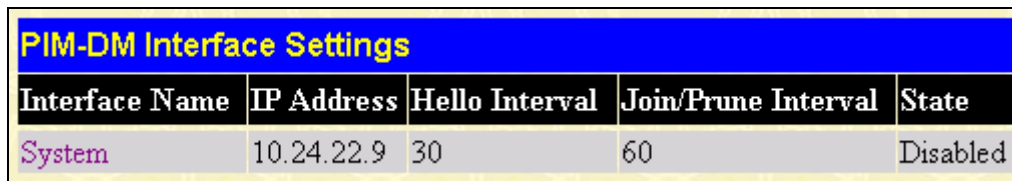
Figure 7- 53. PIM-DM Global Settings window

Use the pull down menu, choose *Enabled*, and click **Apply** to set the PIM-DM function on the Switch.

PIM-DM Interface Settings

To view the first **PIM-DM Interface Settings** window, open the **IP Multicast Routing Protocol** folder under **Configuration** and click **PIM-DM Interface Settings**. This window allows the PIM-DM to be configured for each IP interface defined on the Switch. Each IP interface configured on the Switch is displayed in the below first **PIM-DM Interface Settings** window.
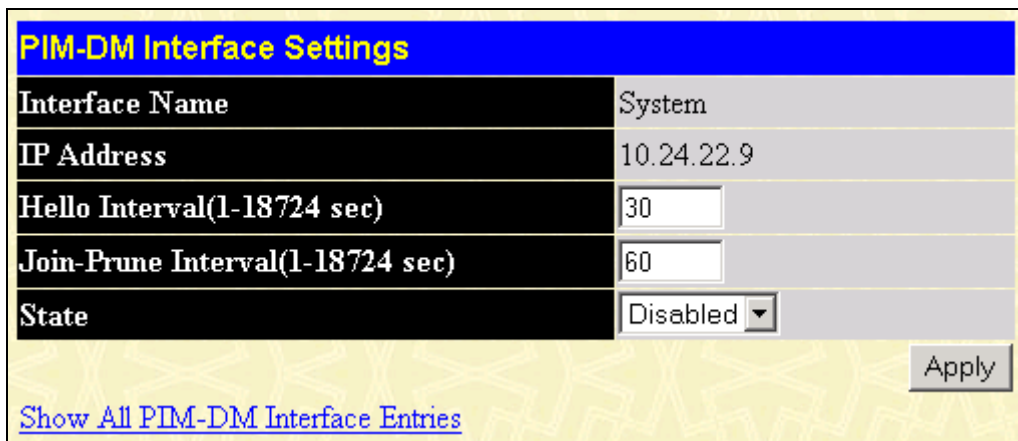
Figure 7- 54. first PIM-DM Interface Settings window

To configure PIM-DM for a particular interface, click the corresponding hyperlink for that IP interface. This will open the second **PIM-DM Interface Settings** window:

Figure 7- 55. second PIM-DM Interface Settings window

The following fields can be set:

Parameter	Description
Interface Name	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.

IP Address	Displays the IP address for the IP interface named above.
Hello Interval (1-18724 sec) *<30>*	This field allows an entry of between *1* and *18724* seconds and determines the interval between sending Hello packets to other routers on the network. The default is *30* seconds.
Join/Prune Interval (1-18724 sec) *<60 >*	This field allows an entry of between *1* 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.
State *<Disabled>*	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu, and is used to enable or disable PIM-DM for the IP interface. The default is *Disabled*.

Click **Apply** to implement changes made. Click Show All PIM-DM Interface Entries to return to the first **PIM-DM Interface Settings** window.

Section 8

Security Management

Security IP

User Accounts

Access Authentication Control (TACACS)

Policy and Parameters

Application Authentication Settings

Authentication Server Group

Authentication Server Host

Login Method Lists

Enable Method Lists

Local Enable Password

Enable Admin

Secure Sockets Layer (SSL)

Download Certificate

Configuration

Secure Shell (SSH)

SSH Configuration

SSH Algorithm

SSH User Authentication

The following section will aid the user in configuring security functions for the Switch. The Switch includes various functions for security, including TACACS, Security IPs, SSL, and SSH, all discussed in detail in the following section.

Security IP

Go to the **Security Management** folder and click on the **Security IP** link; the following window will appear.

Figure 8- 1. Security IP Management window

Use the **Security IP Management** window to permit remote stations 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 and click the **Apply** button.

User Accounts

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

Figure 8- 2. User Account Management window

To add a new user, click on the **Add** button.

Figure 8- 3. User Account Modify Table (New) 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.

To modify an existing user, click on the **Modify** button for that user on the **User Account Management** window.

Figure 8- 4. User Account Modify Table (Modify) window

To delete the user account, click on the **Delete** button for that user on the **User Account Management** window. To change the password, type in the New Password and retype it in the Confirm New Password entry field. The level of privilege (*Admin* or *User*) can be viewed in the Access Right field.

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

Table 8- 1. Admin and User Privileges

After establishing a User Account with Admin-level privileges, be sure to save the changes by opening the **Maintenance** folder, opening the **Save Settings** window, and clicking the **Save** button.

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 and 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 Management > Access Authentication Control > Policy & Parameters**:

Figure 8- 5. Policy & Parameters Settings window

The following parameters can be set:

Parameters	Description
Authentication Policy	Use the pull-down menu to enable or disable the Authentication Policy on the Switch.
Response Timeout (0-	This field will set the time the Switch will wait for a response of authentication from

255)	the user. The user may set a time between *0* and *255* seconds. The default setting is *30* seconds.
User Attempts (1-255)	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, web) for login at the user level and at the administration level (Enable Admin**)** utilizing a previously configured method list. To view the following window, click **Security Management > Access Authentication Control > Application Authentication Settings:**

Figure 8- 6. Application's Authentication Settings window

The following parameters can be set:

Parameter	Description
Application	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, SSH, and the Web (HTTP) application.
Login Method List	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 **Login Method Lists** window, in this section, for more information.
Enable Method List	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 **Enable Method Lists** 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 TACACS/XTACACS/TACACS+/RADIUS 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 Management > Access Authentication Control > Authentication Server Group**:
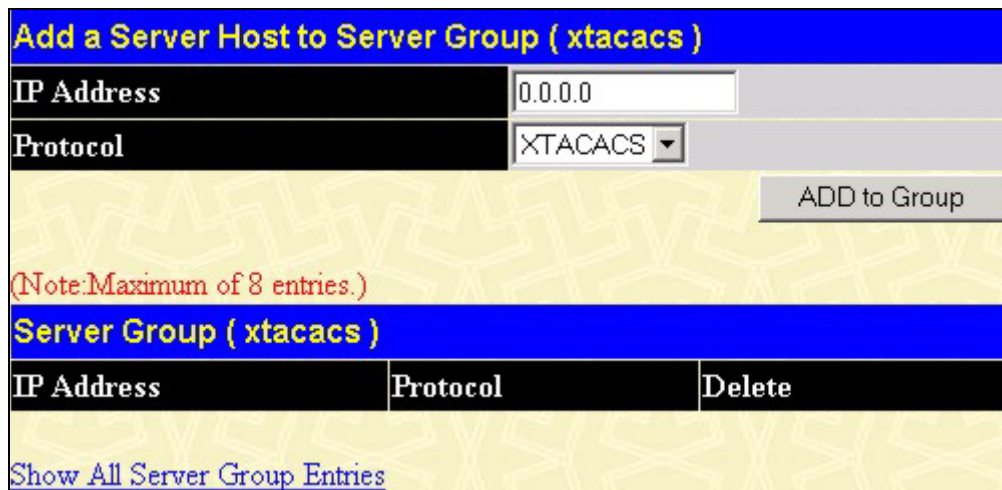

Figure 8- 7. Authentication Server Group Settings window

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.

Figure 8- 8. Add a Server Host to Server Group (xtacacs) 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 and click **Add to Group** to add this Authentication Server Host to the group.

To add a server group other than the ones listed, click the **Add** button on the **Authentication Server Group Settings** window, revealing the following window to configure.

Figure 8- 9. Authentication Server Group Table Add Settings window

Enter a group name of up to 15 characters into the Group Name field and click **Apply**. The entry should appear in the **Authentication Server Group Settings** window.

NOTE: The user must configure Authentication Server Hosts using the Authentication Server Hosts 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: These three built-in server groups can only have server hosts running the same TACACS daemon. TACACS/XTACACS/TACACS+ 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 TACACS/XTACACS/TACACS+/RADIUS 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 TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS 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 TACACS/XTACACS/TACACS+/RADIUS 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 Management > Access Authentication Control > Authentication Server Host**:

Figure 8- 10. Authentication Server Host Settings window

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

Figure 8- 11. Authentication Server Host Setting – Add window

Configure the following parameters to add an Authentication Server Host:

Parameter	Description
IP Address	The IP address of the remote server host the user wishes to add.
Protocol	The protocol used by the server host. The user may choose one of the following: • *TACACS* - Enter this parameter if the server host utilizes the TACACS protocol. • *XTACACS* - Enter this parameter if the server host utilizes the XTACACS protocol. • *TACACS+* - Enter this parameter if the server host utilizes the TACACS+ protocol. • *RADIUS* - Enter this parameter if the server host utilizes the RADIUS protocol.
Port (1-65535)	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+ servers and *1813* for RADIUS servers but the user may set a unique port number for higher security.
Timeout (1-255)	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.
Retransmit (1-255)	Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS server does not respond.
Key	Authentication key to be shared with a configured TACACS+ or RADIUS servers 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 TACACS/XTACACS/TACACS+ 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 Management > Access Authentication Control > Login Method Lists**:

Figure 8- 12. 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 ![X] 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 new Method List, click the **Add** button.

Both actions will result in the same window to configure:

Figure 8- 13. Login Method List - Edit window

Figure 8- 14. Login Method List – Add window

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

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.

Method 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list:
	• *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.
	• *xtacacs* - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server.
	• *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.
	• *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.
	• *server_group* - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch.
	• *local* - Adding this parameter will require the user to be authenticated using the local user account database on the Switch.
	• *none* - Adding this parameter will require no authentication to access the Switch.

Enable Method Lists

The **Enable Method List Settings** window is used to set up Method Lists to promote users with user level privileges to Administrator (Admin) 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 Management > Access Authentication Control > Enable Method Lists**:

Figure 8- 15. Enable Method List Settings window

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

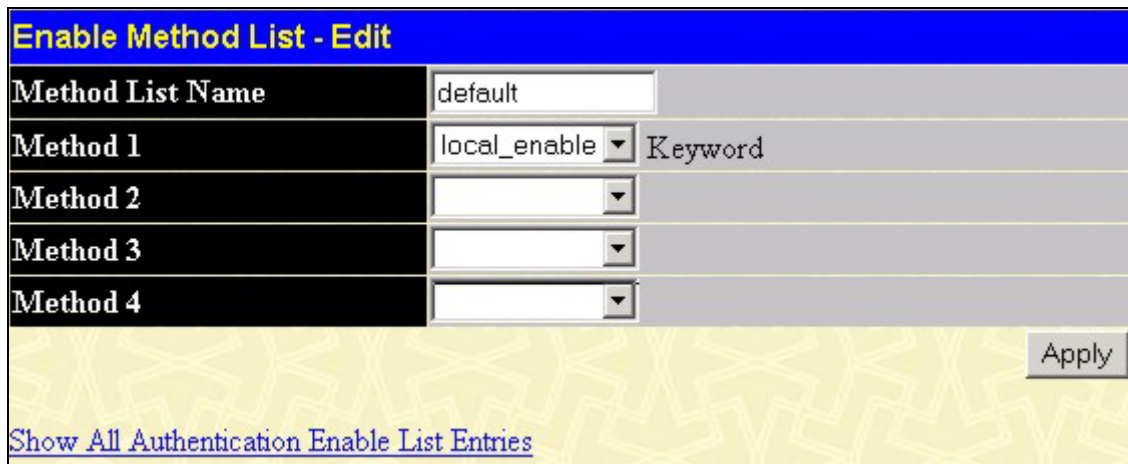Both actions will result in the same window to configure:
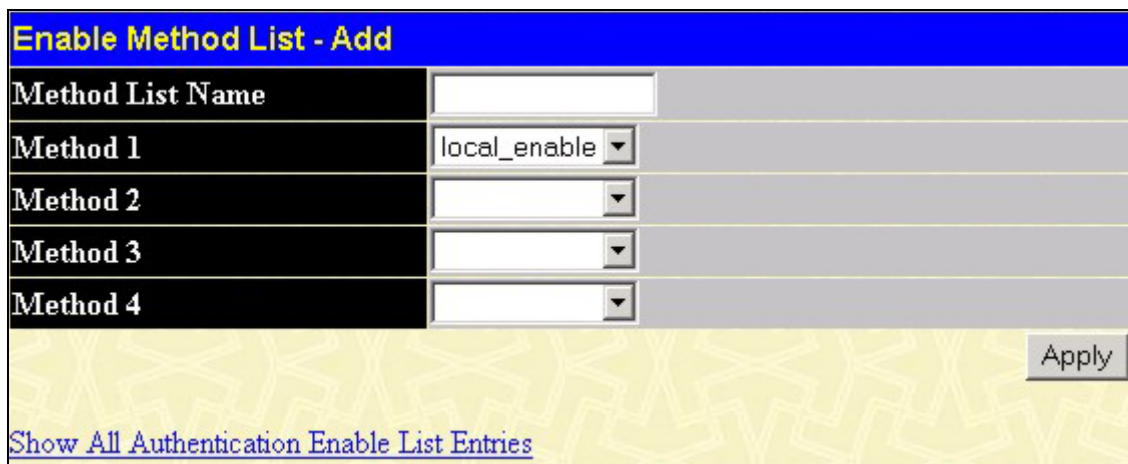
Figure 8- 16. Enable Method List - Edit window

Figure 8- 17. Enable Method List - Add window

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

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Method 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list: • *local_enable* - 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. • *none* - Adding this parameter will require no authentication to access the Switch. • *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. • *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.

	• *xtacacs* - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. • *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. • server_group - Adding a previously configured server group will require the user to be authenticated using a user-defined server group previously configured on the Switch.

Local Enable Password

This window will configure the locally enabled password for the Enable Admin command. 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 Management > Access Authentication Control > Local Enable Password**:

Figure 8- 18. Configure Local Enable Password window

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

Parameter	Description
Old Local Enabled Password	If a password was previously configured for this entry, enter it here in order to change it to a new password
New Local Enabled Password	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.
Confirm Local Enabled Password	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

The **Enable Admin** 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 TACACS/XTACACS/TACACS+/RADIUS, user defined server groups, 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 Management > Access Authentication Control > Enable Admin**:

Figure 8- 19. 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.
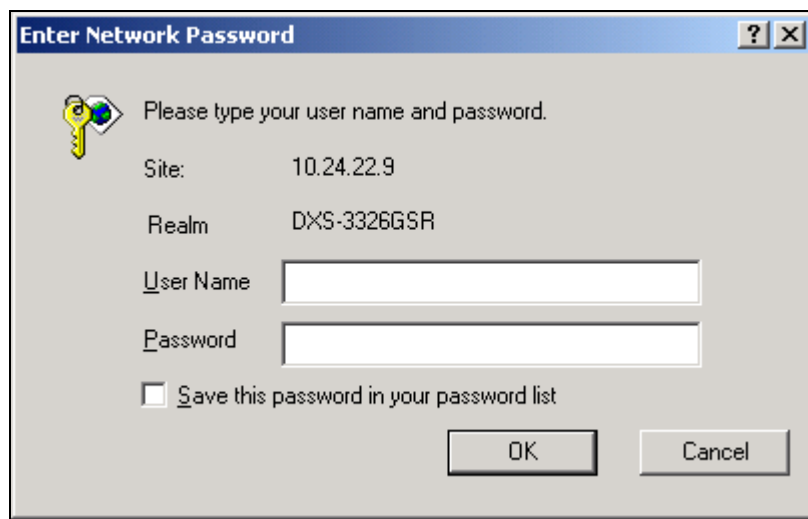

Figure 8- 20. Enter Network Password dialog box

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:

1. **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.

2. **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.

183

3. **Hash Algorithm**: This part of the ciphersuite allows the user to choose a message digest function which 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 Management > Secure Socket Layer (SSL) > Download Certificate**:

Figure 8- 21. Download Certificate window

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

Parameter	Description
Certificate Type	Enter the type of certificate to be downloaded. This type refers to the server responsible for issuing certificates. This field has been limited to *Local* for this firmware release.
Server IP	Enter the IP address of the TFTP server where the certificate files are located.
Certificate File Name	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)
Key File Name	Enter the path and the filename of the key file 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 Management > Secure Socket Layer (SSL) > Configuration**:

Figure 8- 22. Configuration window

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

Parameter	Description
Configuration	
SSL Status	Use the pull-down menu to enable or disable the SSL status on the switch. The default is *Disabled*.
Cache Timeout (60-86,400 sec)	This field will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process. The default setting is *600* seconds.
Ciphersuite	
RSA with RC4 128 MD5	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 *Enabled* by default.
RSA with 3DES EDE CBC SHA	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 *Enabled* by default.
DHS DSS with 3DES EDE CBC SHA	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 *Enabled* by default.
RSA EXPORT with RC4 40 MD5	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 *Enabled* by default.

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 ***DXS-3326GSR 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:// (ex. https://10.90.90.90). 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 an abbreviation of Secure Shell, which is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now 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 **Security 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 logon to the Switch, once a secure communication path 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 **Current Accounts** window (**Security Management** > **Secure Shell (SSH)** > **SSH User Authentication**). Click the hyperlinked User Name on the **Current Accounts** window to access an unnamed window that offers three Auth. Mode choices as to the method SSH will use to authorize the user: *Host Based*, *Password* and *Public Key*.

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 **Current SSH Configuration Settings** window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Configuration

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

Figure 8- 23. Current SSH Configuration Settings window

To configure the SSH server on the Switch, modify the following parameters and click **Apply**:

Parameter	Description
SSH Server Status	Use the pull-down menu to enable or disable SSH on the Switch. The default is *Disabled*.
Max Session (1-3)	Enter a value between *1* and *3* to set the number of users that may simultaneously access the Switch. The default setting is *3*.
Connection Time Out (120-600)	Allows the user to set the connection timeout. The use may set a time between *120* and *600* seconds. The default setting is *300* seconds.
Auth. Fail (2-20)	Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been 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 setting is *2*.
Session Rekeying	This field is used to set the time period that the Switch will change the security shell encryptions by using the pull-down menu. The available options are *Never*, *10 min*, *30 min*, and *60 min*. The default setting is *Never*.

SSH Algorithm

This window allows the configuration of the desired types of SSH algorithms used for authentication encryption. There are three categories of algorithms listed and specific algorithms of each may be enabled or disabled by using their corresponding pull-down menus. All algorithms are enabled by default. To open the following window, click **Security Management > Secure Shell (SSH) > SSH Algorithm:**

187

Figure 8- 24. Authentication Mode Configuration window

The following algorithms may be set:

Parameter	Description
Authentication Mode Configuration	
Password	This field may be enabled or disabled to choose if the administrator wishes to use a locally configured password for authentication on the Switch. This field is *Enabled* by default.
Public Key	This field may be enabled or disabled to choose if the administrator wishes to use a publickey configuration set on a SSH server, for authentication. This field is *Enabled* by default.
Host-based	This field may be enabled or disabled to choose 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. This field is *Enabled* by default.

Encryption Algorithm	
3DES-CBC	Use the pull-down to enable or disable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is *Enabled*.
Blow-fish CBC	Use the pull-down to enable or disable the Blowfish encryption algorithm with Cipher Block Chaining. The default is *Enabled*.
AES128-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. The default is *Enabled*.
AES192-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is *Enabled*.
AES256-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES-256 encryption algorithm with Cipher Block Chaining. The default is *Enabled*.
ARC4	Use the pull-down to enable or disable the Arcfour encryption algorithm with Cipher Block Chaining. The default is *Enabled*.
Cast128-CBC	Use the pull-down to enable or disable the Cast128 encryption algorithm with Cipher Block Chaining. The default is *Enabled*.
Twofish128	Use the pull-down to enable or disable the twofish128 encryption algorithm. The default is *Enabled*.
Twofish192	Use the pull-down to enable or disable the twofish192 encryption algorithm. The default is *Enabled*.
Twofish256	Use the pull-down to enable or disable the twofish256 encryption algorithm. The default is *Enabled*.
Data Integrity Algorithm	
HMAC-SHA1	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Secure Hash algorithm. The default is *Enabled*.
HMAC-MD5	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the MD5 Message Digest encryption algorithm. The default is *Enabled*.
Public Key Algorithm	
HMAC-RSA	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. The default is *Enabled*.
HMAC-DSA	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Digital Signature Algorithm encryption. The default is *Enabled*.

Click **Apply** to implement changes made.

SSH User Authentication

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

Figure 8- 25. Current Accounts window

In the example window above, the User Account "Hedo" has been previously set using the **User Accounts** window in the **Security Management** folder. A User Account MUST be set in order to set the parameters for the SSH user. To configure the parameters for a SSH user, click on the hyperlinked User Name in the **Current Accounts** window, which will reveal the following window to configure.

Figure 8- 26. unnamed current accounts configuration window

The user may set the following parameters:

Parameter	Description
User Name	Enter a User Name of no more than 15 characters to identify the SSH user. This User Name must be a previously configured user account on the Switch.
Auth. Mode	The administrator may choose one of the following to set the authorization for users attempting to access the Switch.
	Host Based – 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.
	• *Host Name* – Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user.
	• *Host IP* – Enter the corresponding IP address of the SSH user.
	Password – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation.
	Public Key – This parameter should be chosen if the administrator wishes to use the publickey on a SSH server for authentication.
Host Name	Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. This parameter is only used in conjunction with the Host Based choice in the Auth. Mode field.
Host IP	Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the Host Based choice in the Auth. Mode field.

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 **User Accounts** section of this manual located in this section.

<div style="border: 1px solid black; display: inline-block; float: right;">

Section 9

</div>

SNMP Manager

SNMP User Table

SNMP View Table

SNMP Group Table

SNMP Community Table

SNMP Host Table

SNMP Engine ID

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 DXS-3326GSR 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.

SNMPv3 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 SNMPv1 while assigning a higher level of security to another group, granting read/write privileges using SNMPv3.

Using SNMPv3 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 SNMPv3 in that SNMP messages may be encrypted. To read more about how to configure SNMPv3 settings for the Switch read the next section.

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.

The Switch 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 menus to select the SNMP version used for specific tasks.

The DXS-3326GSR supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used 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.

SNMP settings are configured using the menus 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 Management Station IP Address menu.

SNMP User Table

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

In the **SNMP Manager** folder, click on the **SNMP User Table** link. This will open the **SNMP User Table** window, as shown below.

Figure 9- 1. SNMP User Table window

To delete an existing SNMP User Table entry, click the ☒ below the **Delete** heading corresponding to the entry you wish to delete.

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

Figure 9- 2. SNMP User Table Display window

The following parameters are displayed:

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

To return to the **SNMP User Table** window, click the Show All SNMP User Table Entries link.

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

Figure 9- 3. SNMP User Table Configuration window

The following parameters can set:

Parameter	Description
User Name	Enter an alphanumeric string of up to 32 characters. This is used to identify the SNMP user.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Version	*V1* - Specifies that SNMP version 1 will be used. *V2* - Specifies that SNMP version 2 will be used. *V3* - Specifies that SNMP version 3 will be used.
Auth-Protocol	*MD5* - Specifies that the HMAC-MD5-96 authentication level will be used. This field is only operable when *V3* is selected in the SNMP Version field and the Encryption field

	has been checked. This field will require the user to enter a password.
	SHA - Specifies that the HMAC-SHA authentication protocol will be used. This field is only operable when *V3* is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password.
Priv-Protocol	*None* - Specifies that no authorization protocol is in use.
	DES - Specifies that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field is only operable when *V3* is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password between 8 and 16 alphanumeric characters.
Encrypted	Checking the corresponding box will enable encryption for SNMP V3 and is only operable in SNMP V3 mode.

To implement changes made, click **Apply**. To return to the **SNMP User Table** window, click the Show All SNMP User Table Entries link.

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. To view the **SNMP View Table** window, open the **SNMP Manager** folder under **Security Management** and click the **SNMP View Table** entry. The following screen should appear:
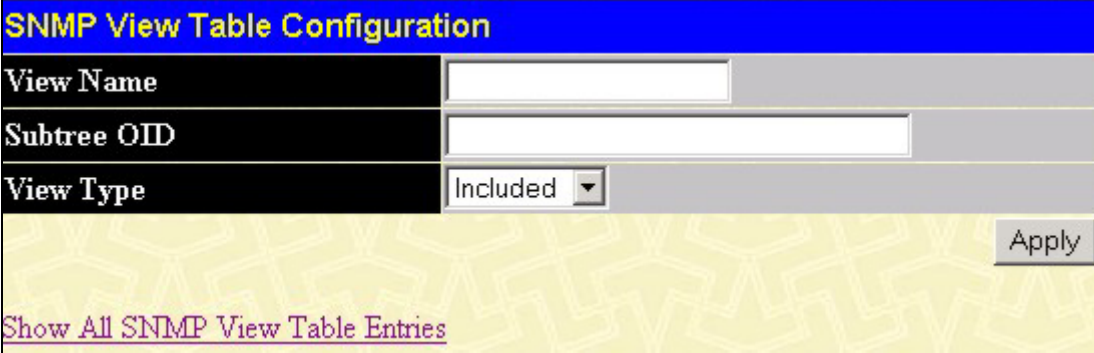
Figure 9- 4. SNMP View Table window

To delete an existing SNMP View Table entry, click the [X] in the Delete column corresponding to the entry you wish to delete. To create a new entry, click the **Add** button and a separate window will appear.

Figure 9- 5. SNMP View Table Configuration window

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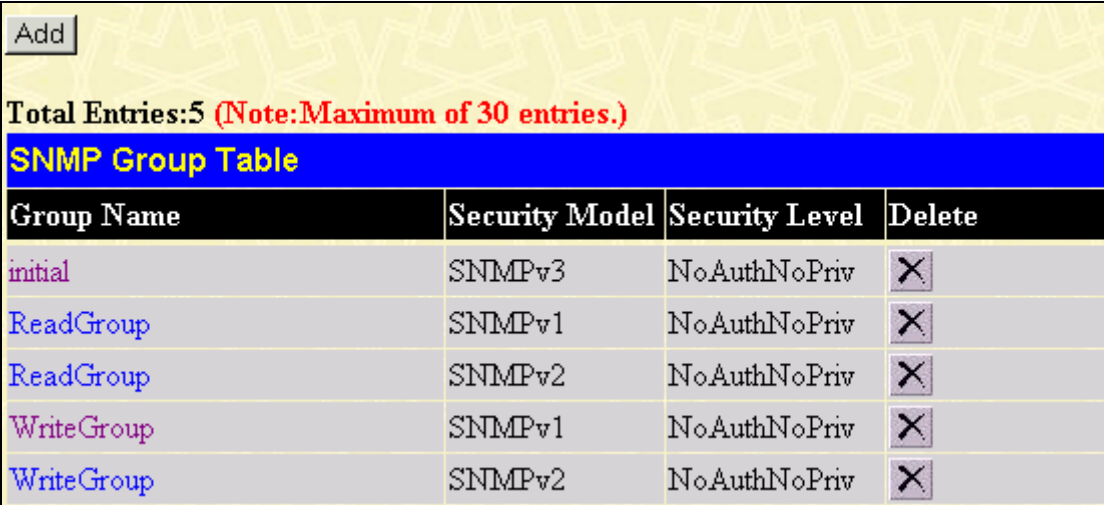
The following parameters can set:

Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID	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.

To implement your new settings, click **Apply**. To return to the **SNMP View Table** window, click the Show All SNMP View Table Entries link.

SNMP Group Table

An SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous window. To view the **SNMP Group Table** window, open the **SNMP Manager** folder and click the **SNMP Group Table** entry. The following window should appear:

Figure 9- 6. SNMP Group Table window

To delete an existing SNMP Group Table entry, click the corresponding ![X] under the Delete heading.

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

Figure 9- 7. SNMP Group Table Display window

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

Figure 9- 8. SNMP Group Table Configuration window

The following parameters can set:

Parameter	Description
Group Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Read View Name	This name is used to specify the SNMP group created can request SNMP messages.
Write View Name	Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.
Notify View Name	Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.
Security Model	*SNMPv1* - Specifies that SNMP version 1 will be used.
	SNMPv2 - Specifies that SNMP version 2c will be used. The SNMPv2 supports both

	centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.
	SNMPv3 - Specifies that the SNMP version 3 will be used. SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network.
Security Level	The Security Level settings only apply to SNMPv3.
	NoAuthNoPriv - Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.
	AuthNoPriv - Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.
	AuthPriv - Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.

To implement your new settings, click **Apply**. To return to the **SNMP Group Table** window, click the Show All SNMP Group Table Entries link.

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.

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

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

To configure **SNMP Community** entries, open the **SNMP Manager** folder, and click the **SNMP Community Table** link, which will open the following window:

Figure 9- 9. SNMP Community Table Configuration window

The following parameters can set:

Parameter	Description
Community Name	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.
View Name	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.
Access Right	*Read_Only* - Specifies that SNMP community members using the community string created can only read the contents of the MIBs on the Switch.
	Read_Write - Specifies that SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.

To implement the new settings, click **Apply**. To delete an entry from the SNMP Community Table, click the ![X] under the Delete heading, corresponding to the entry you wish to delete.

SNMP Host Table

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

Open the **SNMP Manager** folder and 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] under the Delete heading.
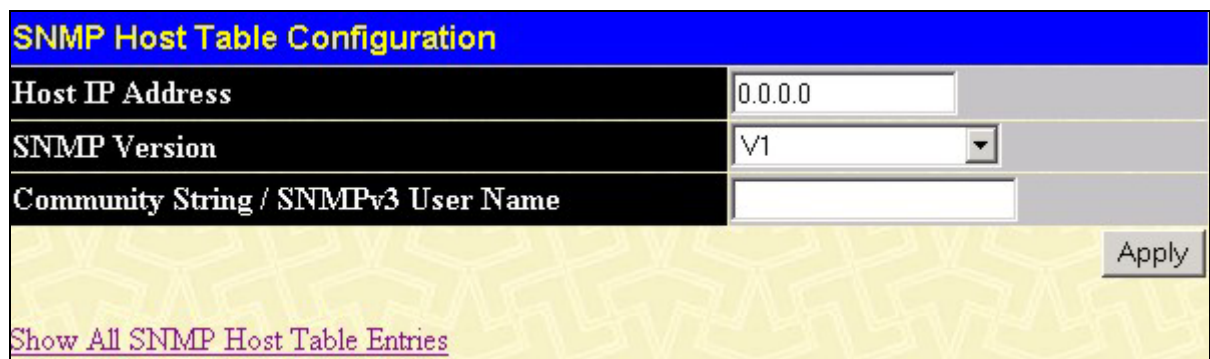
To display the current settings for an existing SNMP Group Table entry, click the blue link for the entry under the Host IP Address heading.

Figure 9- 10. SNMP Host Table window

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

Figure 9- 11. SNMP Host Table Configuration window

The following parameters can set:

Parameter	Description
Host IP Address	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.

SNMP Version	*V1* - To specifies that SNMP version 1 will be used.
	V2 - To specify that SNMP version 2 will be used.
	V3-NoAuth-NoPriv - To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level.
	V3-Auth-NoPriv - To specify that the SNMP version 3 will be used, with a Auth-NoPriv security level.
	V3-Auth-Priv - To specify that the SNMP version 3 will be used, with a Auth-Priv security level.
Community String or SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

To implement your new settings, click **Apply**. To return to the **SNMP Host Table**, click the Show All SNMP Host Table Entries link.

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 **SNMP Manger** folder and click on the **SNMP Engine ID** link. This will open the **SNMP Engine ID Configuration** window, as shown below.

Figure 9- 12. SNMP Engine ID Configuration window

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

Monitoring

Port Utilization

CPU Utilization

Packets

Received (RX)

UMB_cast (RX)

Transmitted (TX)

Errors

Received (RX)

Transmitted (TX)

Size

Packet Size

Stacking Information

Device Status

MAC Address

Switch History Log

IGMP Snooping Group

IGMP Snooping Forward

Browse Router Port

Port Access Control

Authenticator State

Authenticator Statistics

Authenticator Session-Statistics

Authenticator Diagnostics

RADIUS Authentication

RADIUS Accounting

Layer 3 Feature

Browse IP Address

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 Address Table

Browse DVMRP Routing Next Hop Table

PIM Monitor

PIM Neighbor Address Table

Port Utilization

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

To view the port utilization, open the **Monitoring** folder and then the **Port Utilization** link:
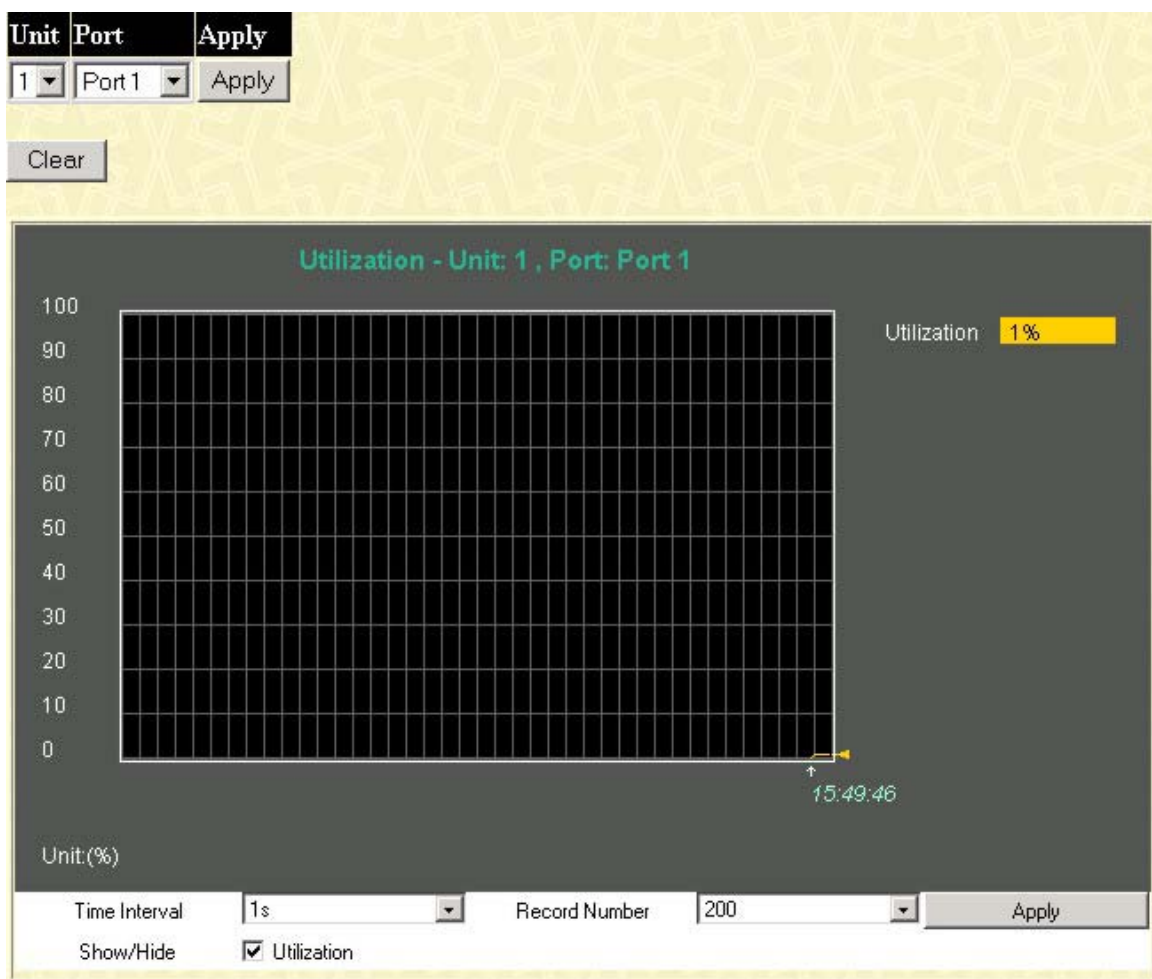
Figure 10- 1. Utilization window

The following field can be set:

Parameter	Description
Unit	Select the unit to display utilization for.
Port	Select the port to display the utilization for.
Clear	Clicking this button clears all statistics counters on this window.

Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether to display Utilization.

Click **Apply** to set changes implemented.

CPU Utilization

The **CPU Utilization** window displays the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval. To view this window, open the **Monitoring** folder and click the **CPU Utilization** link.
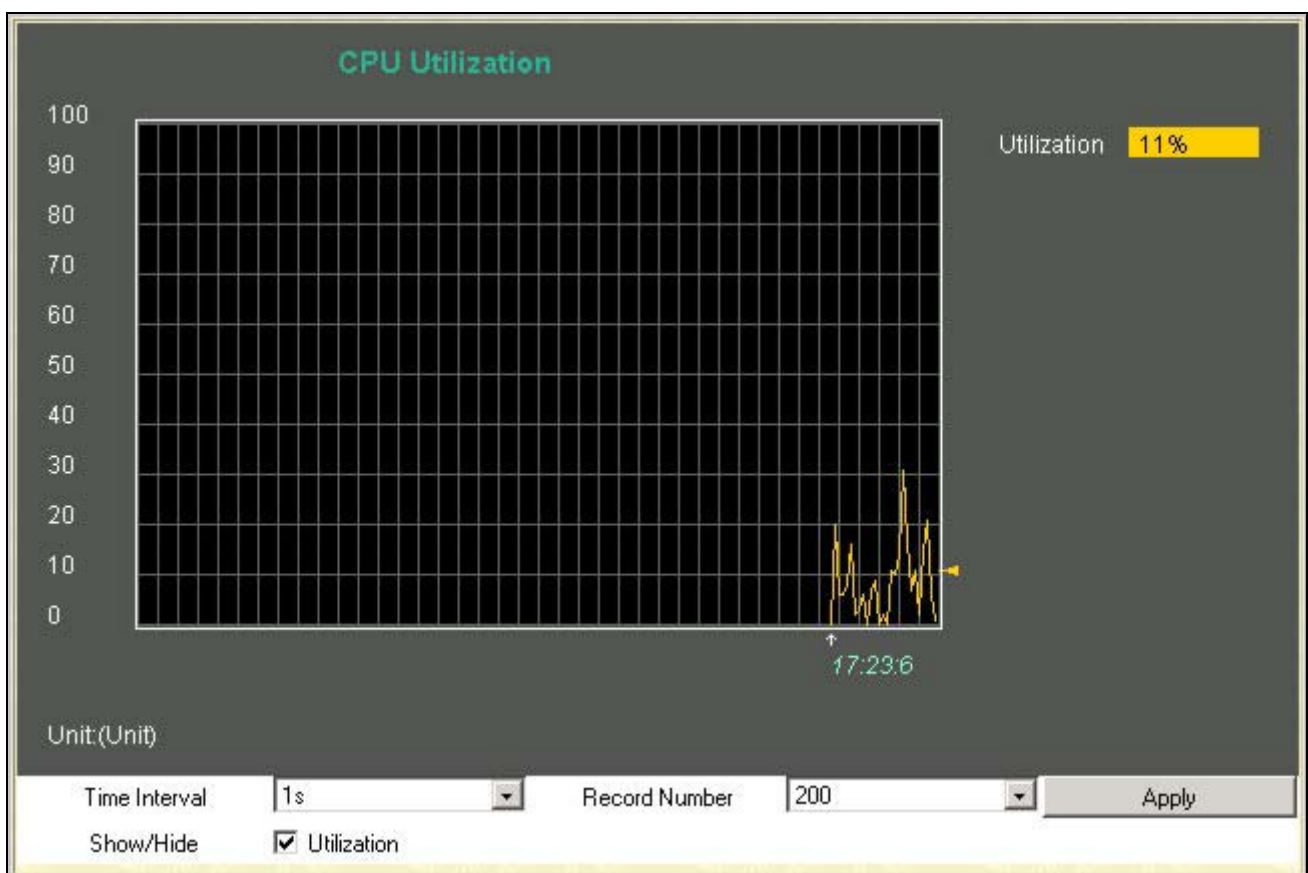
Figure 10- 2. CPU Utilization window

Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics

The information is described as follows:

Parameter	Description
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether to display Utilization.

Packets

The Web Manager allows various packet statistics to be viewed as either a line graph or a table. Six windows are offered.

Received (RX)

Click the **Received (RX)** link in the **Packets** folder of the **Monitoring** menu to view the following graph of packets received on the Switch.
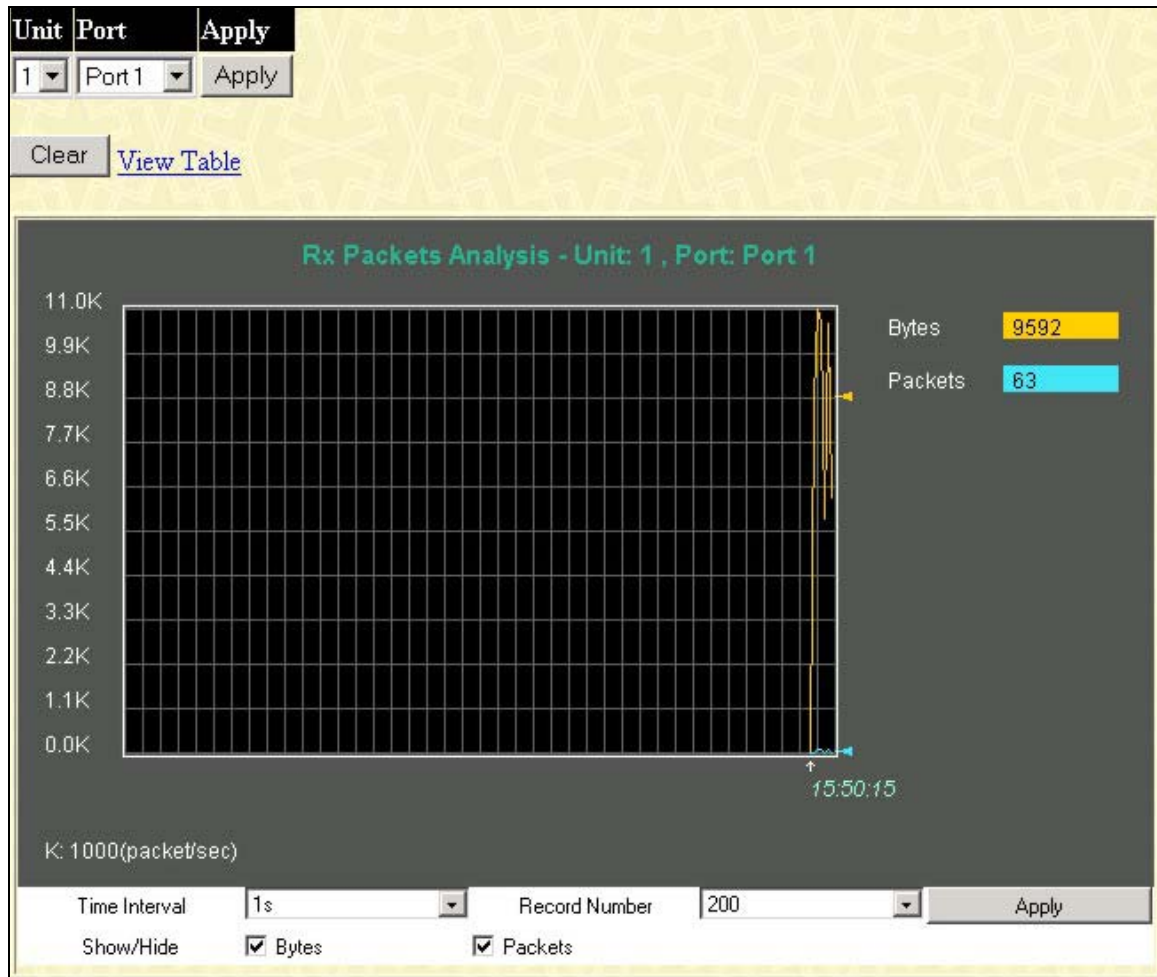
Figure 10- 3. Rx Packets Analysis window (line graph for Bytes and Packets)

To view in tabular format, click the link View Table, which will display the following table:
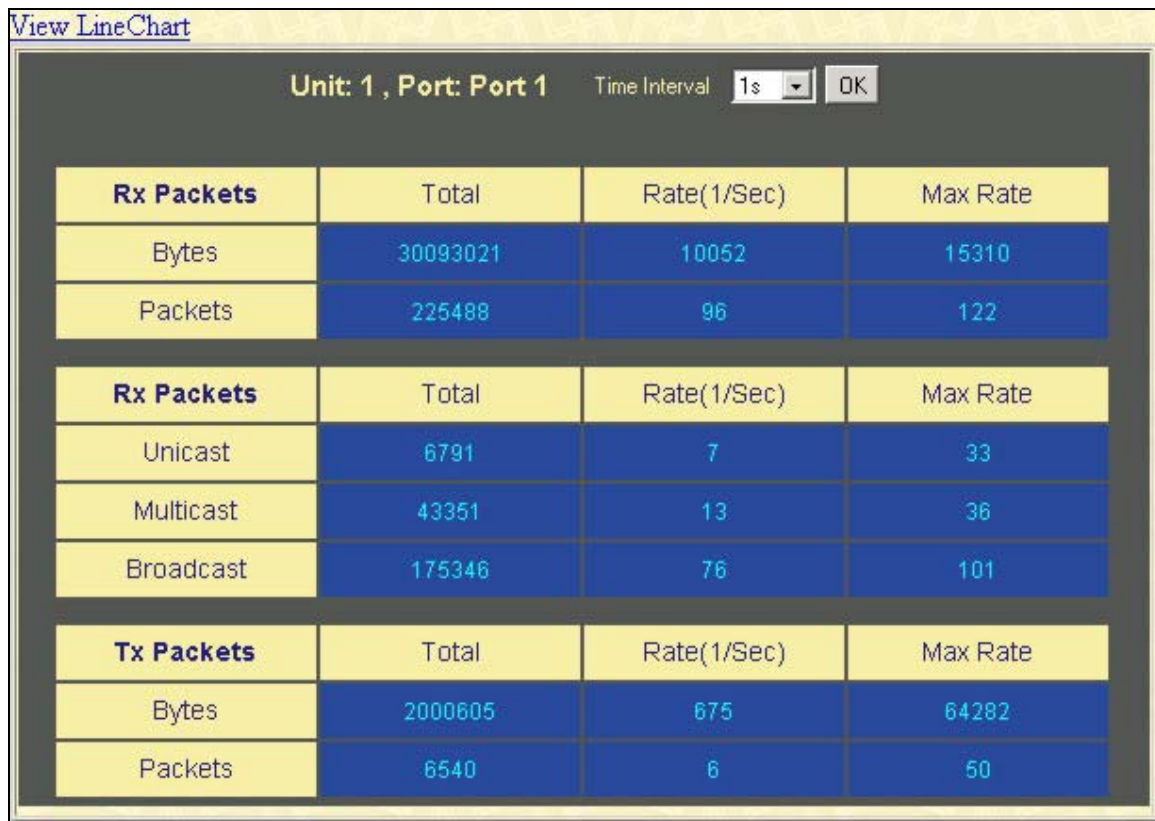
Figure 10- 4. Rx Packets Analysis window (table for Bytes and Packets)

The following fields may be set or viewed:

Parameter	Description
Unit	Select the unit to display statistics for.
Port	Select the port to display statistics for.
Clear	Clicking this button clears all statistics counters on this window.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes received on the port.
Packets	Counts the number of packets received on the port.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether to display Bytes and Packets.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

UMB Cast (RX)

Click the **UMB Cast (RX)** link in the **Packets** folder of the **Monitoring** menu to view the following graph of UMB cast packets received on the Switch. To select a port to view these statistics for, first select the Switch in the switch stack by using the Unit pull-down menu and then select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.

Figure 10- 5. Rx Packets Analysis window (line graph for Unicast, Multicast, and Broadcast Packets)

To view in tabular format, click the View Table link, which will show the following table:
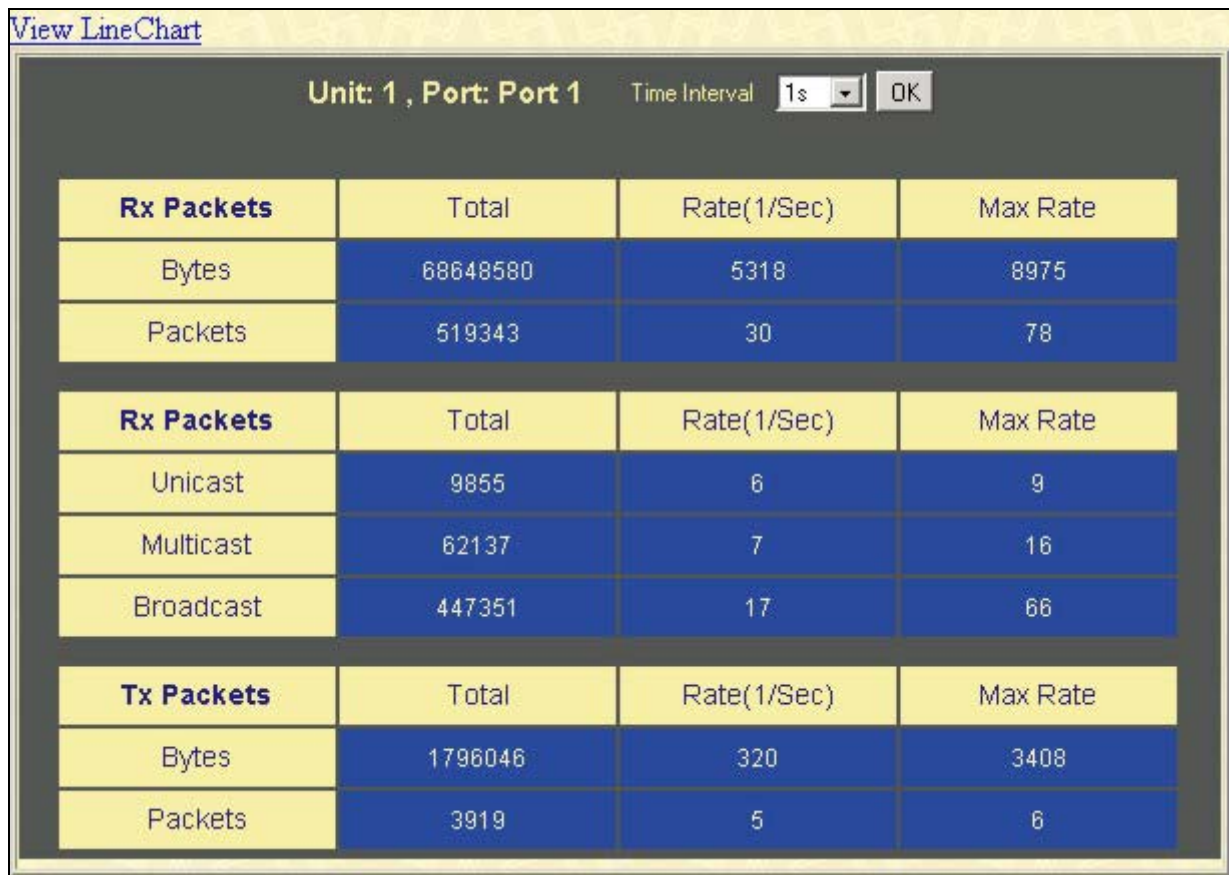
Figure 10- 6. Rx Packets Analysis window (table for Unicast, Multicast, and Broadcast Packets)

The following fields may be set or viewed:

Parameter	Description
Unit	Select the unit to display statistics for.
Port	Select the port to display statistics for.
Clear	Clicking this button clears all statistics counters on this window.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether or not to display Multicast, Broadcast, and Unicast Packets.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

Click the **Transmitted (TX)** link in the **Packets** folder of the **Monitoring** menu to view the following graph of packets transmitted from the Switch. To select a port to view these statistics for, first select the Switch in the switch stack by using the Unit pull-down menu and then select the port by using the Port pull down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.
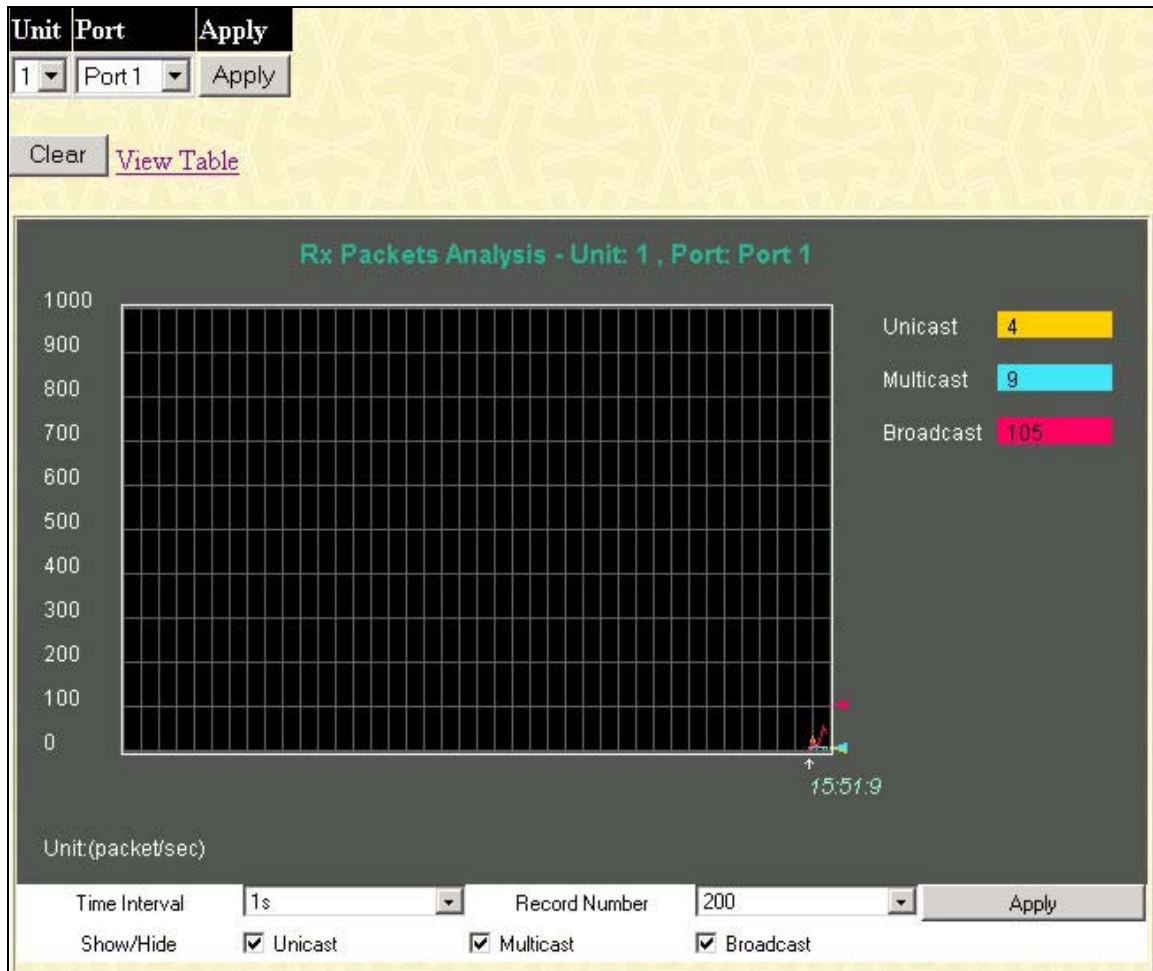

Figure 10- 7. Tx Packets Analysis window (line graph for Bytes and Packets)

To view in tabular format, click the link View Table, which will show the following table:
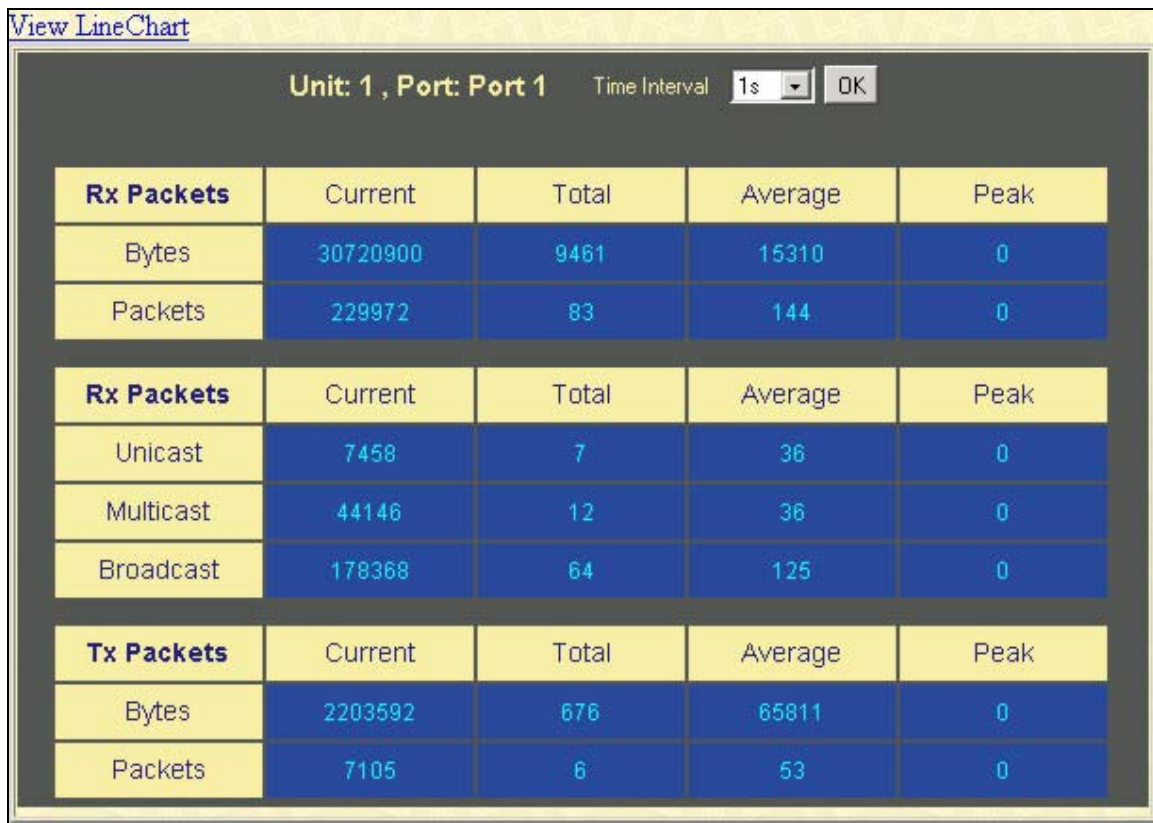
Figure 10- 8. Tx Packets Analysis window (table for Bytes and Packets)

The following fields may be set or viewed:

Parameter	Description
Unit	Select the unit to display statistics for.
Port	Select the port to display statistics for.
Clear	Clicking this button clears all statistics counters on this window.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes successfully sent from the port.
Packets	Counts the number of packets successfully sent on the port.
Unicast	Counts the total number of good packets that were transmitted by a unicast address.
Multicast	Counts the total number of good packets that were transmitted by a multicast address.
Broadcast	Counts the total number of good packets that were transmitted by a broadcast address.
Show/Hide	Check whether or not to display Bytes and Packets.

View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Errors

The Web Manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. Four windows are offered.

Received (RX)

Click the **Received (RX)** link in the **Errors** folder of the **Monitoring** menu to view the following graph of error packets received on the Switch. To select a port to view these statistics for, first select the Switch in the switch stack by using the Unit pull-down menu and then select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.
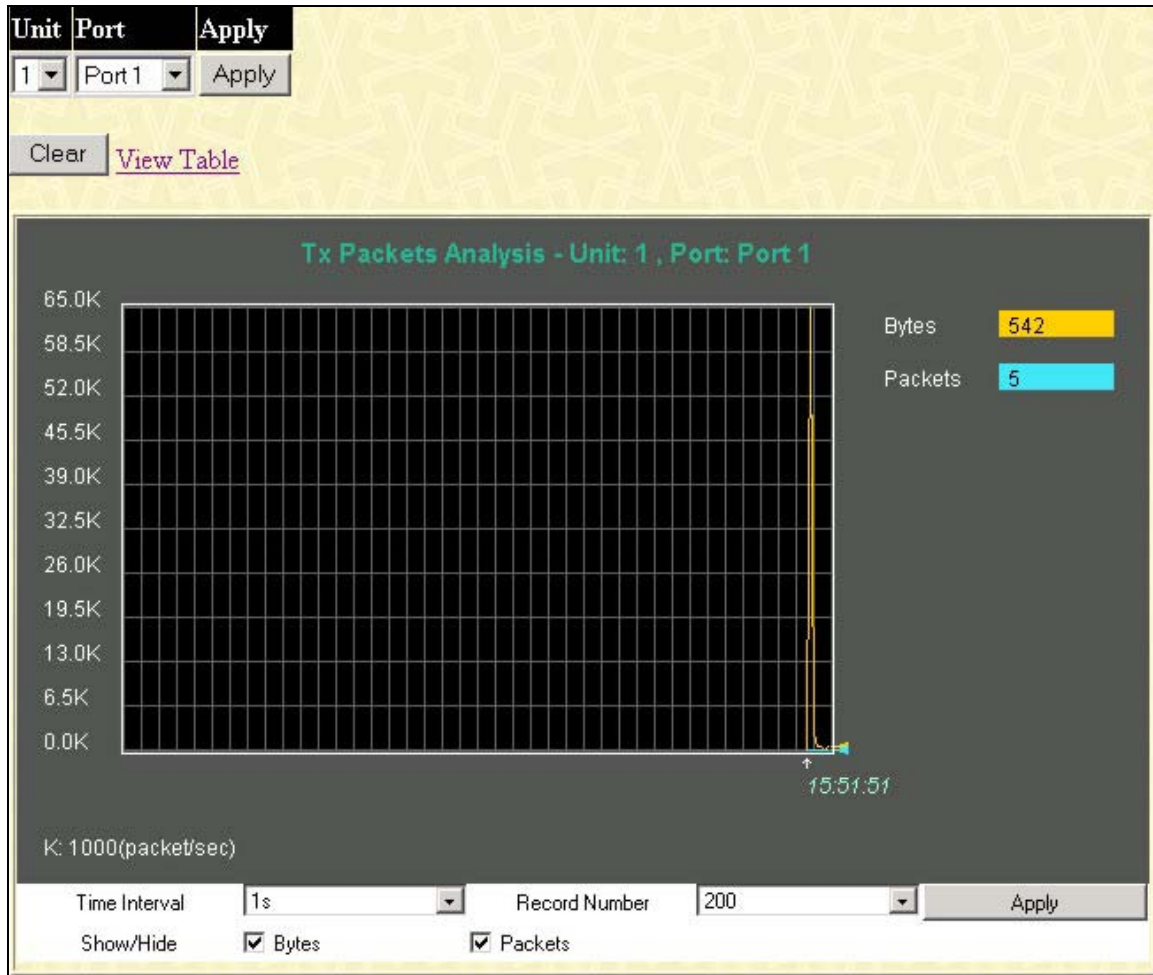

Figure 10- 9. Rx Error Analysis window (line graph)

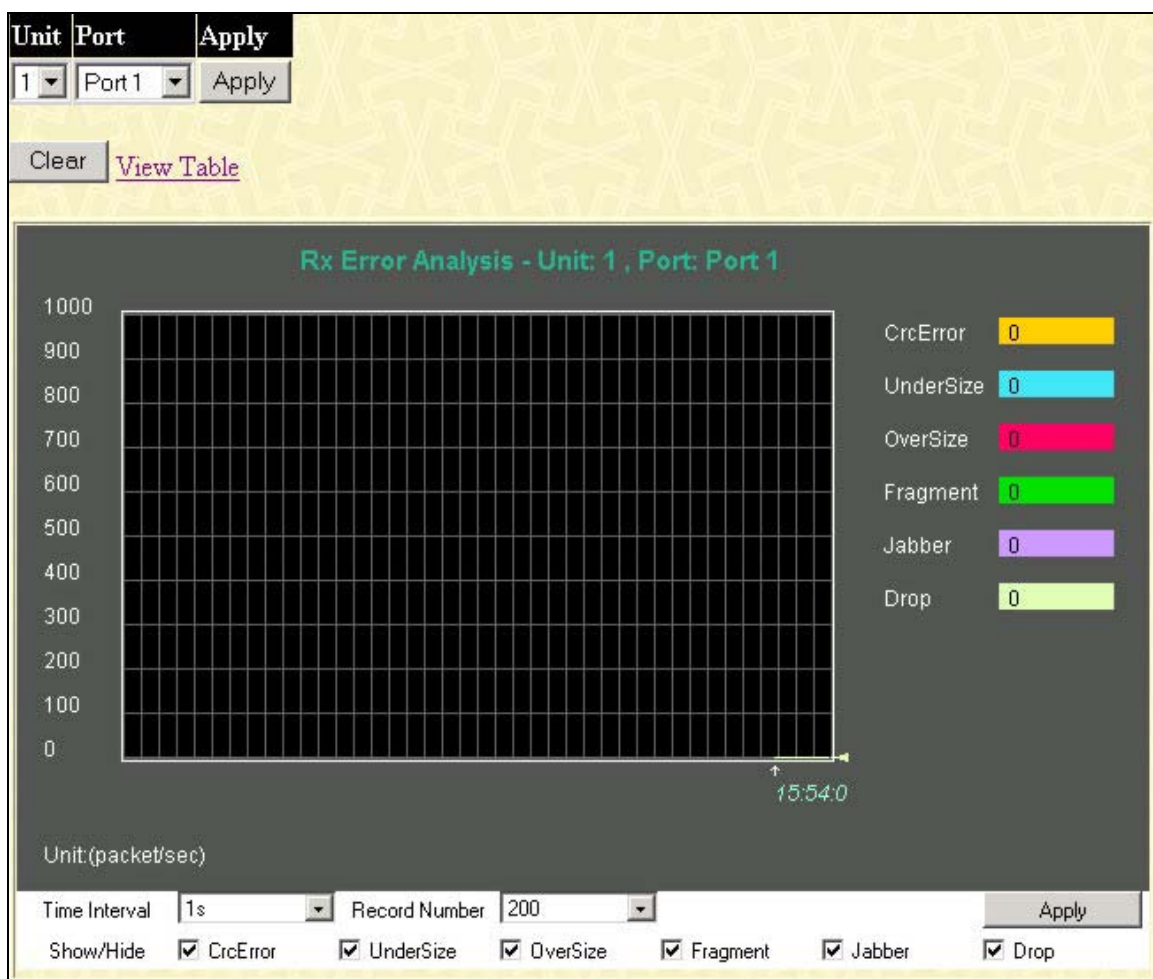To view in tabular format, click the link View Table, which will show the following table:
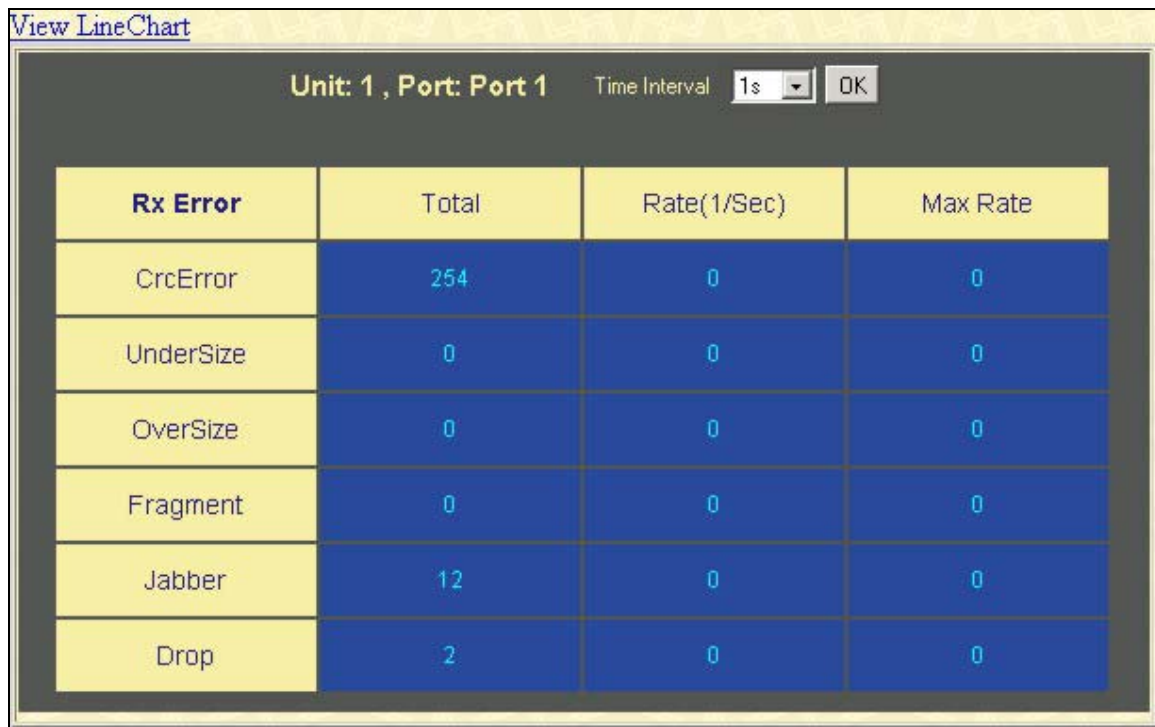
Figure 10- 10. Rx Error Analysis window (table)

The following fields can be set:

Parameter	Description
Unit	Select the unit to display statistics for.
Port	Select the port to display statistics for.
Clear	Clicking this button clears all statistics counters on this window.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Crc Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
Under Size	The number of packets detected that are less than the minimum permitted packets size of 64 bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence.
OverSize	Counts packets received that were longer than 1518 octets, or if a VLAN frame is 1522 octets, and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	The number of packets with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522.
Drop	The number of packets that are dropped by this port since the last Switch reboot.

Show/Hide	Check whether or not to display Crc Error, Under Size, Over Size, Fragment, Jabber, and Drop errors.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

Click the **Transmitted (TX)** link in the **Errors** folder of the **Monitoring** menu to view the following graph of error packets received on the Switch.

Figure 10- 11. Tx Error Analysis window (line graph)

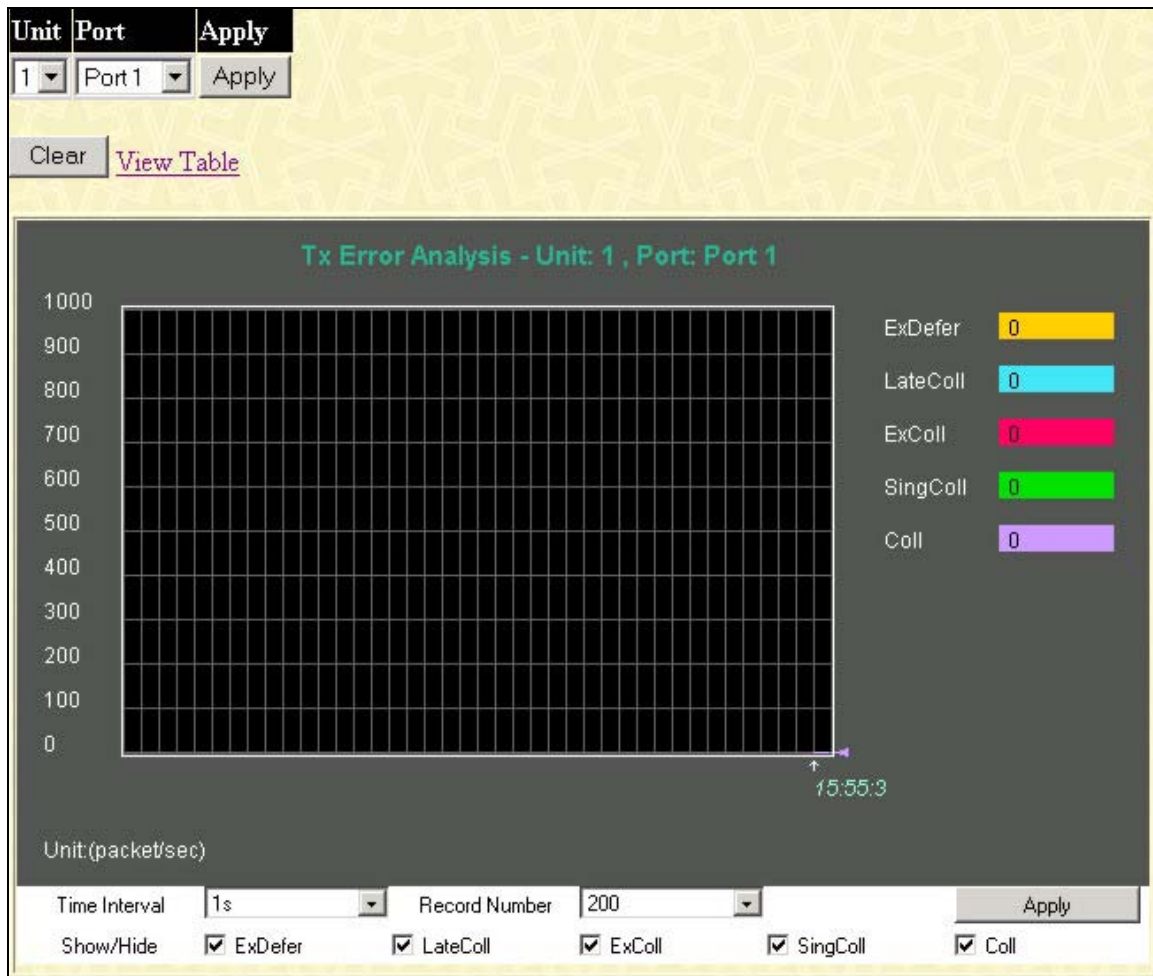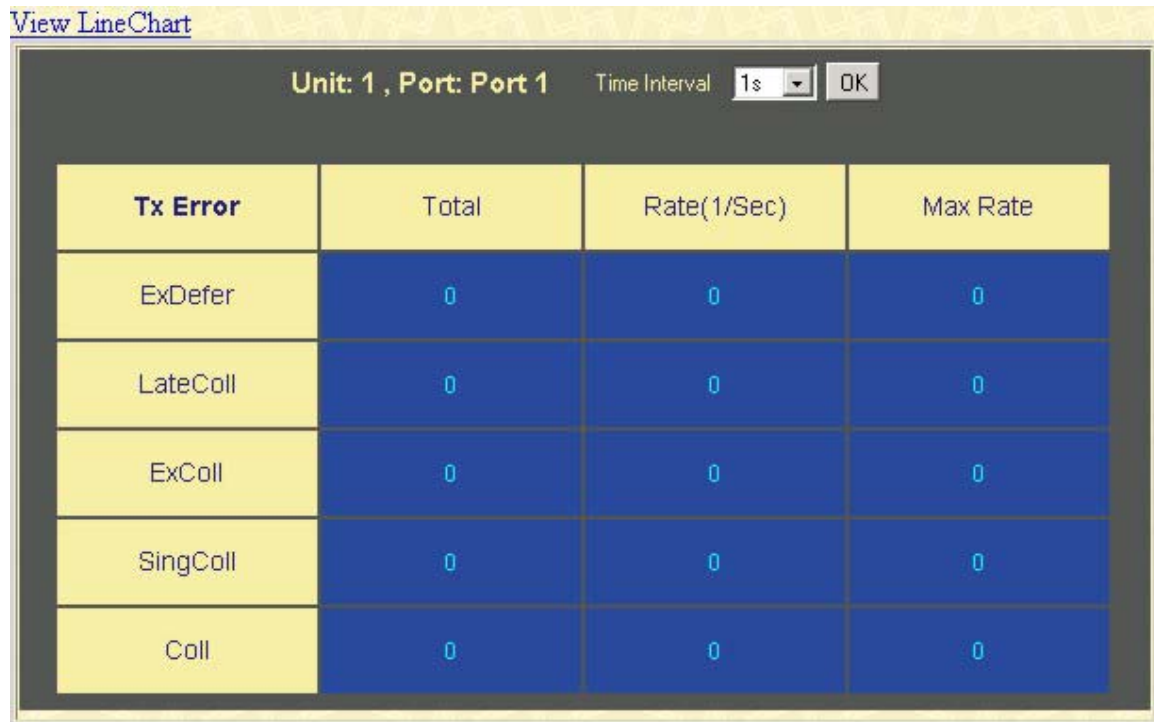To view in tabular format, click the link View Table, which will show the following table:

Figure 10- 12. Tx Error Analysis window (table)

The following fields may be set or viewed:

Parameter	Description
Unit	Select the unit to display statistics for.
Port	Select the port to display statistics for.
Clear	Clicking this button clears all statistics counters on this window.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
ExDefer	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.
LateColl	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
ExColl	Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.
SingColl	Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.
Coll	An estimate of the total number of collisions on this network segment.
Show/Hide	Check whether or not to display ExDefer, LateColl, ExColl, SingColl, and Coll errors.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.

| View Line Chart | Clicking this button instructs the Switch to display a line graph rather than a table. |

Size

The Web Manager allows packets received by the Switch, arranged in six groups and classed by size, to be viewed as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, first select the Switch in the switch stack by using the Unit pull-down menu and then select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.

Figure 10- 13. Rx Size Analysis window (line graph)

To view in tabular format, click the link View Table, which will show the following table:
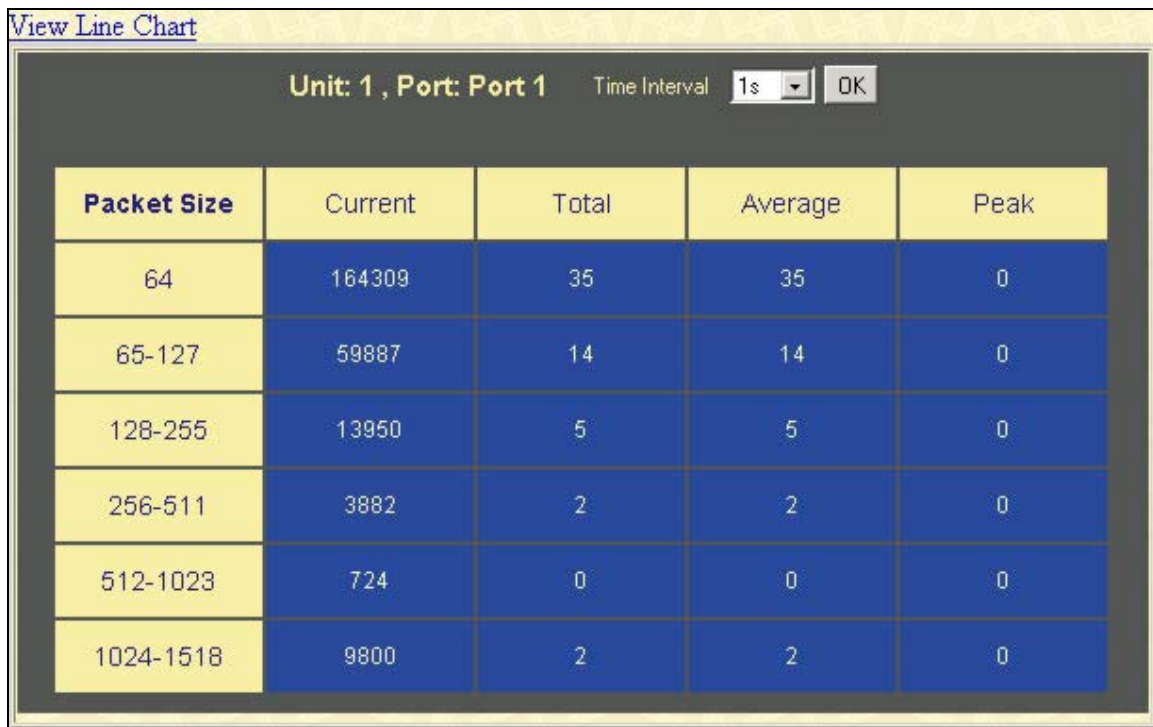
Figure 10- 14. Rx Size Analysis window (table)

The following fields can be set or viewed:

Parameter	Description
Unit	Select the unit to display statistics for.
Port	Select the port to display statistics for.
Clear	Clicking this button clears all statistics counters on this window.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
64	The total number of packets (including bad packets) received that were *64* octets in length (excluding framing bits but including FCS octets).
65-127	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).
128-255	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).
256-511	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).
512-1023	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).

1024-1518	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).
Show/Hide	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Stacking Information

To change a switch's default stacking configuration (for example, the order in the stack), see **Box Information** in the **Configuration** folder.

The number of switches in the switch stack (up to 12 total) are displayed in the upper right-hand corner of your web-browser. The icons are in the same order as their respective Unit numbers, with the Unit 1 switch corresponding to the icon in the upper left-most corner of the icon group.

When the switches are properly interconnected through their optional Stacking Modules, information about the resulting switch stack is displayed under the **Stack Information** link.

To view the stacking information, click on the **Stacking Information** link from the **Monitoring** folder:

Stacking Information

Box ID	User Set	Type	Exist	Priority	Prom version	Runtime version	H/W version
1	1	DXS-3326GSR	exist	16	2.00-B04	3.00-B16	2A1
2	___	USR-NOT-CFG	no				
3	___	USR-NOT-CFG	no				
4	___	USR-NOT-CFG	no				
5	___	USR-NOT-CFG	no				
6	___	USR-NOT-CFG	no				
7	___	USR-NOT-CFG	no				
8	___	USR-NOT-CFG	no				
9	___	USR-NOT-CFG	no				
10	___	USR-NOT-CFG	no				
11	___	USR-NOT-CFG	no				
12	___	USR-NOT-CFG	no				

Topology :   DUPLEX_CHAIN
My Box ID :   1
Current state :   MASTER
Box count :   1

Figure 10- 15. Stacking Information window

The **Stacking Information** window holds the following information:

Parameters	Description
Box ID	Displays the Switch's order in the stack.

User Set	Box ID can be assigned automatically (Auto), or can be assigned statically. The default is Auto.
Type	Displays the model name of the corresponding switch in a stack.
Exist	Denotes whether a switch does or does not exist in a stack.
Priority	Displays the priority ID of the Switch. The lower the number, the higher the priority. The box (switch) with the lowest priority number in the stack denotes the Master switch. The DXS-3326GSR will always be the master switch in a Star topology.
Prom Version	Shows the PROM in use for the Switch. This may be different from the values shown in the illustration.
Runtime Version	Shows the firmware version in use for the Switch. This may be different from the values shown in the illustrations.
H/W Version	Shows the hardware version in use for the Switch. This may be different from the values shown in the illustration.
Topology	Show the current topology employed using this Switch.
My Box ID	Displays the Box ID of the Switch currently in use.
Current State	Displays the current stacking state of the Switch, which may be MASTER or SLAVE
Box Count	Displays the number of switches in the switch stack.

Device Status

The **Device Status** window can be found in the **Monitoring** menu by clicking the **Device Status** link. This window shows the status of the physical attributes of the Switch, including power sources and fans.

Device Status

ID	Internal Power	External Power	Side Fan	Back Fan
1	Active	Fail	OK	OK

Figure 10- 16. Device Status window

The following fields may be viewed in this window:

Parameter	Description
ID	The Box ID of the Switch in the switch stack.
Internal Power	A read-only field denoting the current status of the internal power supply. Active will suggest the mechanism is functioning correctly while Fail will show the mechanism is not functioning correctly.
External Power	A read-only field denoting the current status of the external power supply. Active will suggest the mechanism is functioning correctly while Fail will show the mechanism is not functioning correctly.
Side Fan	A read-only field denoting if the side fan of the Switch is functioning properly.
Back Fan	A read-only field denoting if the back fan of the Switch is functioning properly.

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.

To view the MAC Address forwarding table, from the **Monitoring** menu, click the **MAC Address** link:

Figure 10- 17. MAC Address Table window

The following fields can be viewed or set:

Parameter	Description
VLAN Name	Enter a VLAN Name for the forwarding table to be browsed by.
MAC Address	Enter a MAC address for the forwarding table to be browsed by.
Unit – Port	Select the switch Unit ID of the switch in thye Switch stack and then the port by using the corresponding pull-down menus.
Find	Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.
VID	The VLAN ID of the VLAN the port is a member of.
MAC Address	The MAC address entered into the address table.
Unit	Refers to the Unit of the switch stack that the MAC address was learned from.
Port	The port that the MAC address above corresponds to.
Type	How the Switch discovered the MAC address. The possible entries are Dynamic, Self, and Static.
Next	Click this button to view the next page of the address table.
Clear Dynamic Entry	Clicking this button will clear Dynamic entries learned by the Switch. This may be accomplished by VLAN Name or by Port.
View All Entry	Clicking this button will allow the user to view all entries of the address table.
Clear All Entry	Clicking this button will allow the user to delete all entries of the address table.

Switch History Log

The Web manager allows the Switch's history log, as compiled by the Switch's management agent, to be viewed. To view the Switch history log, open the **Maintenance** folder and click the **Switch History Log** link.

Figure 10- 18. 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. Click **Next** to go to the next page of the **Switch History Log**. Clicking **Clear** will allow the user to clear the Switch History Log.

The information is described as follows:

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

IGMP Snooping Group

This window allows the Switch's IGMP Snooping Group 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 displayed in the Reports field.

To view the **IGMP Snooping Group Table** window, click **IGMP Snooping Group** on the **Monitoring** menu:

Figure 10- 19. IGMP Snooping Group Table window

The user may search the IGMP Snooping Group Table by VLAN Name by entering it in the top lefthand corner and clicking **Search**.

The following field can be viewed:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
Multicast Group	The IP address of the multicast group.
MAC Address	The MAC address of the multicast group.
Reports	The total number of reports received for this group.
Port Member	These are the ports where the IGMP packets were snooped are displayed.

NOTE: To configure IGMP snooping for the DXS-3326GSR, go to the **Configuration** folder and select **IGMP**. Configuration and other information concerning IGMP snooping may be found in Section 6 of this manual under **IGMP**.

IGMP Snooping Forward

This window will display the current IGMP snooping forwarding table entries currently configured on the Switch. To view the following window, open the **Monitoring** folder and click the **IGMP Snooping Forward** link.

Figure 10- 20. IGMP Snooping Forwarding Table

The user may search the **IGMP Snooping Forwarding Table** by VLAN Name using the top left hand corner **Search**.

The following field can be viewed:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
Source IP	The Source IP address of the multicast group.
Multicast Group	The IP address of the multicast group.
Port Map	These are the ports where the IP multicast packets are forwarding to.

Browse Router Port

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

Figure 10- 21. Browse Router Port window

Port Access Control

The following windows are used to monitor 802.1x statistics of the Switch, on a per port basis. To view the **Port Access Control** windows, open the **Monitoring** folder and click the **Port Access Control** folder.

Authenticator State

The following section describes the 802.1X Status on the Switch. To view the Authenticator State, click **Monitoring > Port Access Control > Authenticator State**.

Port	Auth_PAE_State	Backend_State	PortStatus
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized
13	ForceAuth	Success	Authorized
14	ForceAuth	Success	Authorized
15	ForceAuth	Success	Authorized
16	ForceAuth	Success	Authorized
17	ForceAuth	Success	Authorized
18	ForceAuth	Success	Authorized
19	ForceAuth	Success	Authorized
20	ForceAuth	Success	Authorized
21	ForceAuth	Success	Authorized
22	ForceAuth	Success	Authorized
23	ForceAuth	Success	Authorized
24	ForceAuth	Success	Authorized

Authenticator State of Unit 1   Time Interval 1s   OK

Unit 1   Apply

Figure 10- 22. Authenticator State (Port-Based 802.1x) window

Figure 10- 23. Show Authenticator State (MAC-Based 802.1x) window

This window displays the Authenticator Status for individual ports on a selected device. To select unit within the switch stack, use the pull-down menu at the top of the window and click **Apply**. A polling interval between *1* and *60* seconds can be set using the drop-down menu at the top of the window and clicking **OK**.

The information on this window is described as follows:

Parameter	Description
Auth PAE State	The Authenticator PAE State value can be: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force_Auth, Force_Unauth,* or *N/A*. *N/A* (Not Available) indicates that the port's authenticator capability is disabled.

Backend State	The Backend Authentication State can be *Request, Response, Success, Fail, Time-out, Idle, Initialize,* or *N/A*. *N/A* (Not Available) indicates that the port's authenticator capability is disabled.
Port Status	Controlled Port Status can be *Authorized, Unauthorized,* or *N/A*.

Authenticator Statistics

This table contains the statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function. To view the Authenticator Statistics, click **Monitoring > Port Access Control > Authenticator Statistics**.

Figure 10- 24. Show Authenticator Statistics window

The user can specify a switch in a switch stack using that switch's Unit ID by using the pull down menu in the top left hand corner. The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Frames Rx	The number of valid EAPOL frames that have been received by this Authenticator.
Frames Tx	The number of EAPOL frames that have been transmitted by this Authenticator.
Rx Start	The number of EAPOL Start frames that have been received by this Authenticator.
Tx ReqId	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Rx LogOff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Tx Req	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.

Rx RespId	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx Resp	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx Error	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Last Version	The protocol version number carried in the most recently received EAPOL frame.
Last Source	The source MAC address carried in the most recently received EAPOL frame.

Authenticator Session-Statistics

This table contains the session statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function. To view the **Authenticator Session Statistics**, click **Monitoring > Port Access Control > Authenticator Session-Statistics**.

Figure 10- 25. Authenticator Session Statistics window

The user can specify a switch in a switch stack using that switch's Unit ID by using the pull down menu in the top left hand corner. The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Octets Rx	The number of octets received in user data frames on this port during the session.

Octets Tx	The number of octets transmitted in user data frames on this port during the session.
Frames Rx	The number of user data frames received on this port during the session.
Frames Tx	The number of user data frames transmitted on this port during the session.
ID	A unique identifier for the session, in the form of a printable ASCII string of at least three characters.
Authentic Method	The authentication method used to establish the session. Valid Authentic Methods include: (1) Remote Authentic Server - The Authentication Server is external to the Authenticator's System. (2) Local Authentic Server - The Authentication Server is located within the Authenticator's System.
Time	The duration of the session in seconds.
Terminate Cause	The reason for the session termination. There are eight possible reasons for termination. 1) Supplicant Logoff 2) Port Failure 3) Supplicant Restart 4) Reauthentication Failure 5) AuthControlledPortControl set to ForceUnauthorized 6) Port re-initialization 7) Port Administratively Disabled 8) Not Terminated Yet
UserName	The User-Name representing the identity of the Supplicant PAE.

Authenticator Diagnostics

This table contains the diagnostic information regarding the operation of the Authenticator associated with each port. An entry appears in this table for each port that supports the Authenticator function. To view Authenticator Diagnostics, click **Monitoring > Port Access Control > Authenticator Diagnostics**.

Figure 10- 26. Authenticator Diagnostics window

The user can specify a switch in a switch stack using that switch's Unit ID by using the pull down menu in the top left hand corner. The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
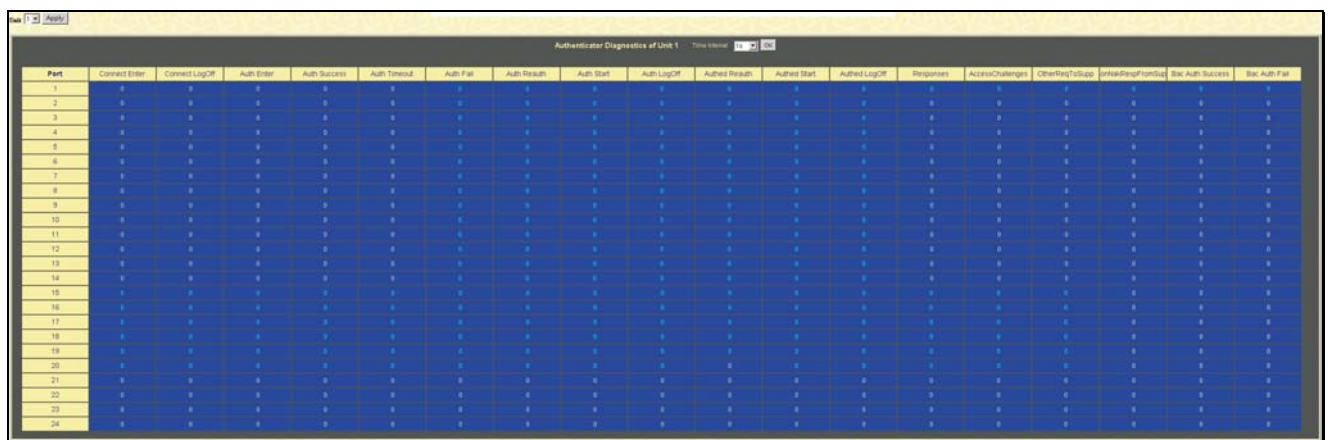
The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Connect Enter	Counts the number of times that the state machine transitions to the CONNECTING state from any other state.
Connect LogOff	Counts the number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
Auth Enter	Counts the number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.
Auth Success	Counts the number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant (authSuccess = TRUE).
Auth Timeout	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout (authTimeout = TRUE).
Auth Fail	Counts the number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure (authFail = TRUE).
Auth Reauth	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Auth Start	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
Auth LogOff	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
Authed Reauth	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Authed Start	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
Authed LogOff	Counts the number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
Responses	Counts the number of times that the state machine sends an initial Access-Request packet to the Authentication server (i.e., executes sendRespToServer on entry to the RESPONSE state). Indicates that the Authenticator attempted communication with the Authentication Server.

AccessChallenges	Counts the number of times that the state machine receives an initial Access-Challenge packet from the Authentication server (i.e., aReq becomes TRUE, causing exit from the RESPONSE state). Indicates that the Authentication Server has communication with the Authenticator.
OtherReqToSupp	Counts the number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant (i.e., executes txReq on entry to the REQUEST state). Indicates that the Authenticator chose an EAP-method.
NonNakRespFromSup	Counts the number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK (i.e., rxResp becomes TRUE, causing the state machine to transition from REQUEST to RESPONSE, and the response is not an EAP-NAK). Indicates that the Supplicant can respond to the Authenticator.s chosen EAP-method.
Bac Auth Success	Counts the number of times that the state machine receives an Accept message from the Authentication Server (i.e., aSuccess becomes TRUE, causing a transition from RESPONSE to SUCCESS). Indicates that the Supplicant has successfully authenticated to the Authentication Server.
Bac Auth Fail	Counts the number of times that the state machine receives a Reject message from the Authentication Server (i.e., aFail becomes TRUE, causing a transition from RESPONSE to FAIL). Indicates that the Supplicant has not authenticated to the Authentication Server.

RADIUS Authentication

This table contains information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol. It has one row for each RADIUS authentication server that the client shares a secret with. To view the **RADIUS Authentication**, click **Monitoring > Port Access Control > RADIUS Authentication**.

Figure 10- 27. RADIUS Authentication window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second. To clear the current statistics shown, click the **Clear** button in the top left hand corner.

The following fields can be viewed:

Parameter	Description
ServerIndex	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.
InvalidServerAddr	The number of RADIUS Access-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS authentication client. (This is not necessarily the same as sysName in MIB II.)

AuthServerAddr	The (conceptual) table listing the RADIUS authentication servers with which the client shares a secret.
ServerPortNumber	The UDP port the client is using to send requests to this server.
RoundTripTime	The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
AccessRequests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
AccessRetrans	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
AccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
AccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
AccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
AccessResponses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or known types are not included as malformed access responses.
BadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
PendingRequests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.
Timeouts	The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the authentication port
PacketsDropped	The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

RADIUS Accounting

This window shows managed objects used for managing RADIUS accounting clients, and the current statistics associated with them. It has one row for each RADIUS authentication server that the client shares a secret with. To view the **RADIUS Accounting**, click **Monitoring > Port Access Control > RADIUS Accounting**.

Figure 10- 28. RADIUS Accounting window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second. To clear the current statistics shown, click the *Clear* button in the top left hand corner.

The following fields can be viewed:

Parameter	Description
ServerIndex	The identification number assigned to each RADIUS Accounting server that the client shares a secret with.
InvalidServerAddr	The number of RADIUS Accounting-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS accounting client. (This is not necessarily the same as sysName in MIB II.)
ServerAddress	The (conceptual) table listing the RADIUS accounting servers with which the client shares a secret.
ServerPortNumber	The UDP port the client is using to send requests to this server.
RoundTrip Time	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Responses	The number of RADIUS packets received on the accounting port from this server.
MalformedResponses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
BadAuthenticators	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
PendingRequests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.

Timeouts	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type that were received from this server on the accounting port.
PacketsDropped	The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.

Note: To configure 802.1x features for the DXS-3326GSR, go to the **Configuration** folder and select **Port Access Entity**. Configuration and other information concerning 802.1x may be found in Section 6 of this manual under Port Access Entity.

Layer 3 Feature

This folder in the **Monitoring** section will display information concerning settings configured in **Layer 3 IP Networking** of the **Configuration** folder.

Browse IP Address

The **IP Address Table** window may be found in the **Monitoring** menu in the **Layer 3 Feature** folder. The **IP Address Table** window is where the user may 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 window and click **Find** to begin your search.

IP Address	0.0.0.0		Find

IP Address Table

Interface	IP Address	Port	Learned
System	10.0.0.1	1:19	Dynamic
System	10.0.0.121	1:19	Dynamic
System	10.0.1.100	1:19	Dynamic
System	10.0.25.1	1:19	Dynamic
System	10.0.34.1	1:19	Dynamic
System	10.0.46.1	1:19	Dynamic
System	10.0.51.1	1:19	Dynamic
System	10.0.58.4	1:19	Dynamic
System	10.0.85.168	1:19	Dynamic
System	10.1.1.1	1:19	Dynamic
System	10.1.1.4	1:19	Dynamic
System	10.1.1.80	1:19	Dynamic
System	10.1.1.101	1:19	Dynamic
System	10.1.1.102	1:19	Dynamic
System	10.1.1.103	1:19	Dynamic
System	10.1.1.163	1:19	Dynamic
System	10.1.1.164	1:19	Dynamic
System	10.1.1.166	1:19	Dynamic
System	10.1.1.167	1:19	Dynamic
System	10.1.1.168	1:19	Dynamic

Next

Figure 10- 29. IP Address Table window

Browse Routing Table

The **Browse Routing Table** window may be found in the **Monitoring** menu in the **Layer 3 Feature** 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 and click **Find**.

Destination Address	0.0.0.0	
Mask	0.0.0.0	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 10- 30. Routing Table window

Browse ARP Table

The **ARP Table** window may be found in the **Monitoring** menu in the **Layer 3 Feature** 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**. To clear the ARP Table, click **Clear All**.

Interface Name	IP Address	Mac Address	Type
System	10.0.0.0	ff-ff-ff-ff-ff-ff	Local/Broadcast
System	10.0.0.1	00-04-23-5a-34-df	Dynamic
System	10.0.0.121	00-a0-c5-15-3b-6e	Dynamic
System	10.0.1.100	00-50-ba-f4-96-9a	Dynamic
System	10.0.25.1	00-d0-59-a9-2a-c4	Dynamic
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	10.0.51.1	00-80-c8-4c-69-fb	Dynamic
System	10.0.58.4	00-0c-6e-43-13-ae	Dynamic
System	10.0.85.168	00-50-ba-11-08-e4	Dynamic
System	10.1.1.1	00-05-5d-00-00-00	Dynamic
System	10.1.1.4	00-ff-7f-47-d9-42	Dynamic
System	10.1.1.80	00-05-5d-95-bf-9b	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	10.1.1.163	00-50-ba-70-e4-55	Dynamic
System	10.1.1.164	00-50-ba-70-e4-65	Dynamic
System	10.1.1.166	00-50-ba-70-e4-58	Dynamic
System	10.1.1.167	00-50-ba-70-e4-45	Dynamic

Total Entries: 730

Figure 10- 31. ARP Table window

Browse IP Multicast Forwarding Table

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

Figure 10- 32. IP Multicast Forwarding Table window

Browse IGMP Group Table

The **IGMP Group Table** window may be found in the **Monitoring** menu in the **Layer 3 Feature** folder. This window will show current IGMP group entries on the Switch.

Figure 10- 33. IGMP Group Table window

To search a specific IGMP group entry, enter an interface name into the Interface Name field or a Multicast Group IP address and then click **Find**.

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 and click **OSPF Monitor**.

Browse OSPF LSDB Table

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

Figure 10- 34. Browse 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 in the Search Type field. The choices are *All*, *Area ID*, *Advertise Router ID*, *LSDB*, *Area ID & Advertise Router ID*, *Area ID & LSDB*, and *Advertise Router ID & LSDB*.

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 *Adv. Router ID* is selected, you must enter the IP address in the Advertisement 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**.

The following fields are displayed in the OSPF LSDB Table:

Parameter	Description
Area ID	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.
LSDB Type	Displays which one of eight types of link advertisements by which the current link was discovered by the Switch: *All*, Router link (*RTRLink*), Network link (*NETLink*), Summary link (*Summary*), Autonomous System link (*ASSummary*), Autonomous System external link (*ASExternal)*, MCGLink (*Multicast Group*), and NSSA (*Not So Stubby Area*)
Adv. Router ID	Displays the Advertising Router's ID.
Link State ID	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. **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.
Cost	Displays the cost of the table entry.
Sequence	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 10- 35. OSPF Neighbor Table window

To search for OSPF neighbors, enter an IP address and click **Find**. Valid OSPF neighbors will appear in the OSPF Neighbor Table below.

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 to specifically search a virtual neighbor by using one of the two search options at the top of the window. These are described below:

Parameter	Description
Transit Area ID	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.
Neighbor ID	The OSPF router ID for the remote router. This IP address uniquely identifies the remote area's Area Border Router.

Figure 10- 36. OSPF Virtual Neighbor Table window

DVMRP Monitor

This menu 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: **Browse DVMRP Routing Table**, **Browse DVMRP Neighbor Address Table** and **Browse DVMRP Routing Next Hop Table**. Information on DVMRP and its features in relation to the DXS-3326GSR can be found in Section 6, under IP Multicast Routing Protocol.

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 under **Browse DVMRP Monitoring**, 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.

Figure 10- 37. DVMRP Routing Table window

Browse DVMRP Neighbor Address Table

This table, found in the **Monitoring** menu under **DVMRP Monitor > Browse DVMRP Neighbor Address Table** contains information about DVMRP neighbors of the Switch. To search this table, enter either an Interface Name or Neighbor Address into the respective field and click the **Find** button. DVMRP neighbors of that entry will appear in the **DVMRP Neighbor Table** window below.

Figure 10- 38. DVMRP Neighbor Table window

Browse DVMRP Routing Next Hop Table

The **DVMRP Routing Next Hop Table** window contains information regarding the next-hop for forwarding multicast packets on outgoing interfaces. Each entry in the DVMRP Routing Next Hop Table refers to the next-hop of a specific source to a specific multicast group address. This table is found in the **Monitoring** menu under **DVMRP Monitoring,** with the heading **Browse DVMRP Routing Next Hop Table**. To search this table, enter either an Interface Name or Source IP Address into the respective field and click the **Find** button. The next hop of that DVMRP Routing entry will appear in the **DVMRP Routing Next Hop Table** window below.

Figure 10- 39. 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 earlier in this manual.

PIM Neighbor Address Table

The **PIM Neighbor Table** window contains information regarding each of a router's PIM neighbors. This window may be found in the **Monitoring** folder under the heading **PIM Monitor**.

Figure 10- 40. PIM Neighbor Table window

To search this table, enter either an Interface Name or Neighbor Address into the respective field and click the **Find** button. PIM neighbors of that entry will appear in the **PIM Neighbor Table** window.

<div align="right">

Section 11

</div>

Maintenance

> ### *TFTP Services*
> ### *Download Firmware*
> ### *Download Configuration File*
> ### *Upload Configuration*
> ### *Upload Log*
> ### *Multiple Image Services*
> ### *Firmware Information*
> ### *Config Firmware Image*
> ### *Ping Test*
> ### *Save Changes*
> ### *Reset*
> ### *Reboot Device*
> ### *Logout*

TFTP Services

Trivial File Transfer Protocol (TFTP) services allow the Switch's 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, open the **TFTP Services** folder in the **Maintenance** folder and then click the **Download Firmware** link:

Figure 11- 1. Download Firmware window

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. All indicates all switches in a switch stack will download the same firmware.

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

Select the Image ID of the firmware. The DXS-3326GSR can hold two firmware images in its memory. Image ID 1 will always be the boot up firmware for the Switch unless specified by the user. Information on configuring Image IDs can be found in this section, under the heading Multiple Image Services.

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. Note that in the above example, the firmware file is in the root directory of the D drive of 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 **TFTP Service** folder in the **Maintenance** folder and then the **Download Configuration File** link:
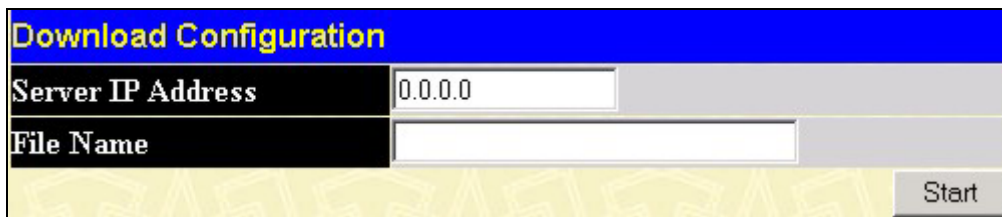
Figure 11- 2. Download Configuration window

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

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

Upload Configuration

To upload the Switch's settings to a TFTP server, click on the **TFTP Service** folder in the **Maintenance** folder and then click the **Save Settings** link:
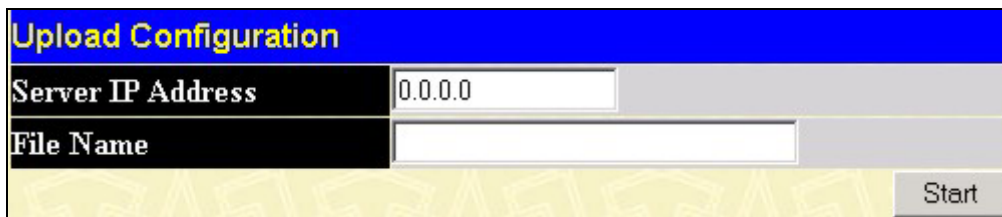
Figure 11- 3. Upload Configuration window

Enter the IP address of the TFTP server and the path and filename for the configuration file on the TFTP server.

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

Upload Log

To upload the Switch history log file to a TFTP server, open the **TFTP Service** folder in the **Maintenance** folder and then click the **Upload Log** link:
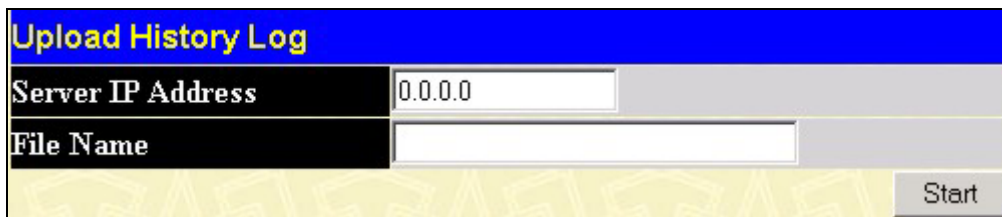
Figure 11- 4. Upload History Log window

Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server.

Click **Start** to record the IP address of the TFTP server and to initiate the file transfer.

Multiple Image Services

The **Multiple Image Services** folder allows users of the DXS-3326GSR to configure and view information regarding firmware located on the Switch. The Switch allows two firmware images to be stored in its memory and either can be configured to be the boot up firmware for the Switch. For information regarding firmware images located on the Switch, open the **Firmware Information** link. The default setting for the Switch's firmware will have the boot up firmware stored in Image 1, but the user may set either firmware stored to be the boot up firmware by using the **Config Firmware Image** window.

Firmware Information

The following window allows the user to view information about current firmware images stored on the Switch. To access the following window, click **Maintenance > Multiple Image Services > Firmware Information**.

Firmware Information						
BOX	**ID**	**Version**	**Size**	**Update Time**	**From**	**User**
1	1	*3.00-B16	3888181	0 days 00:00:00	Serial Port(Prom)	Unknown
1	2	(empty)				

'*' means boot up firmware

(R) means firmware update thru Serial Port(RS232)

(T) means firmware update thru TELNET

(S) means firmware update thru SNMP

(W) means firmware update thru WEB

Figure 11- 5. Firmware Information window

This window holds the following information:

Parameter	Description
BOX	States the stacking ID number of the switch in the switch stack.
ID	States the image ID number of the firmware in the Switch's memory. The Switch can store 2 firmware images for use. Image ID 1 will be the default boot up firmware for the Switch unless otherwise configured by the user.
Version	States the firmware version.
Size	States the size of the corresponding firmware, in bytes.
Update Time	States the specific time the firmware version was downloaded to the Switch.
From	States the IP address of the origin of the firmware. There are four ways firmware may be downloaded to the Switch. • R – If the IP address has this letter attached to it, it denotes a firmware upgrade through the Console Serial Port (RS-232). • T - If the IP address has this letter attached to it, it denotes a firmware

	upgrade through Telnet.
	• S - If the IP address has this letter attached to it, it denotes a firmware upgrade through the Simple Network Management Protocol (SNMP).
	• W - If the IP address has this letter attached to it, it denotes a firmware upgrade through the web-based amangement interface.
User	States the user who downloaded the firmware. This field may read "Anonymous" or "Unknown" for users that are not identified.

Config Firmware Image

The **Config Firmware Image** window allows users to configure firmware images saved in the memory of the Switch. To access the following window, click **Maintenance > Multiple Image Services > Config Firmware Image**.

Figure 11- 6. Config Firmware Image window
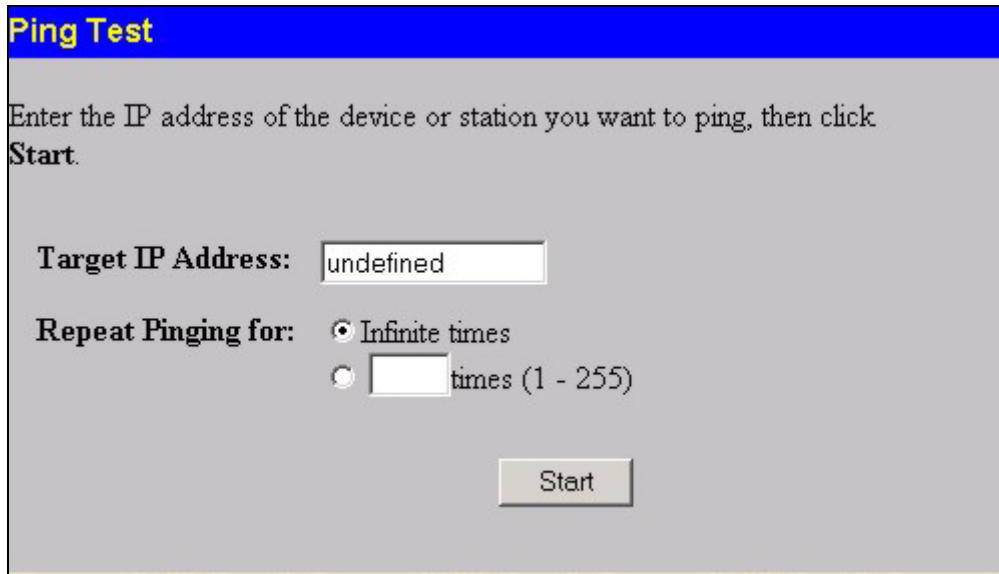
This window offers the following information:

Parameter	Description
Image	Select the firmware image to be configured using the pull-down menu. The Switch allows two firmware images to be stored in the Switch's memory.
Active	This field has two options for configuration.
	• *Delete* – Select this option to delete the firmware image specified in the Image field above.
	• *Boot* – Select this option to set the firmware image specified above as the boot up firmware for the Switch. This firmware will be set as the boot up firmware after a switch reboot has been performed. The default setting has firmware image ID 1 as the boot up firmware image for the Switch unless specified here.

Click **Apply** to implement changes made.

Ping Test

PING is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or "echoes" the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

Figure 11- 7. Ping Test window
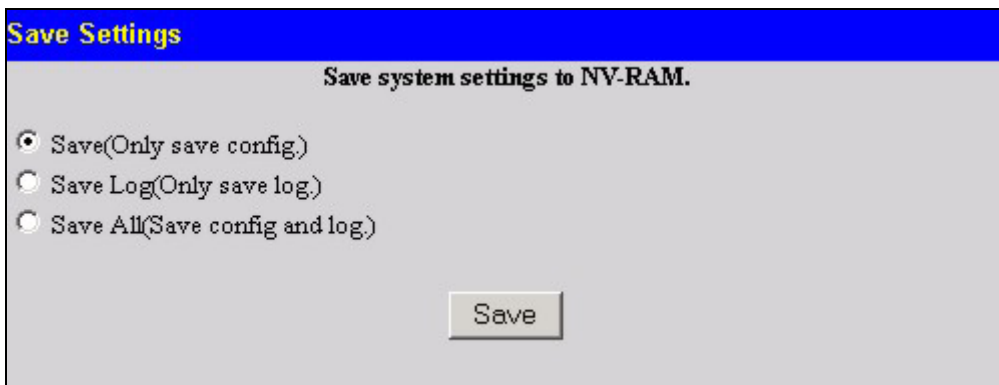
The user may use Infinite times radio button, in the Repeat Pinging for field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the Target IP Address by clicking its radio button and entering a number between *1* and *255*. Click **Start** to initiate the PING program.

Save Changes

The DXS-3326GSR 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 on the **Save** button in the **Save Settings** window, as shown below.

Figure 11- 8. Save Settings window

The Switch has three levels of save, which are as follows:

Parameter	Description
Save (Only save config)	Clicking the radio button for this entry will save only the current switch configuration to NV-RAM.
Save Log (Only save log)	Clicking the radio button for this entry will save only the current log file to NV- RAM.

log)	
Save All (Save config and log)	Clicking the radio button for this entry will save both the current switch configuration and the current log file to NV-RAM.

Once the Switch configuration settings have been saved to NV-RAM, they become the default settings for the Switch, and one of the following three windows will appear depending on which option you choose in the **Save Settings** window.
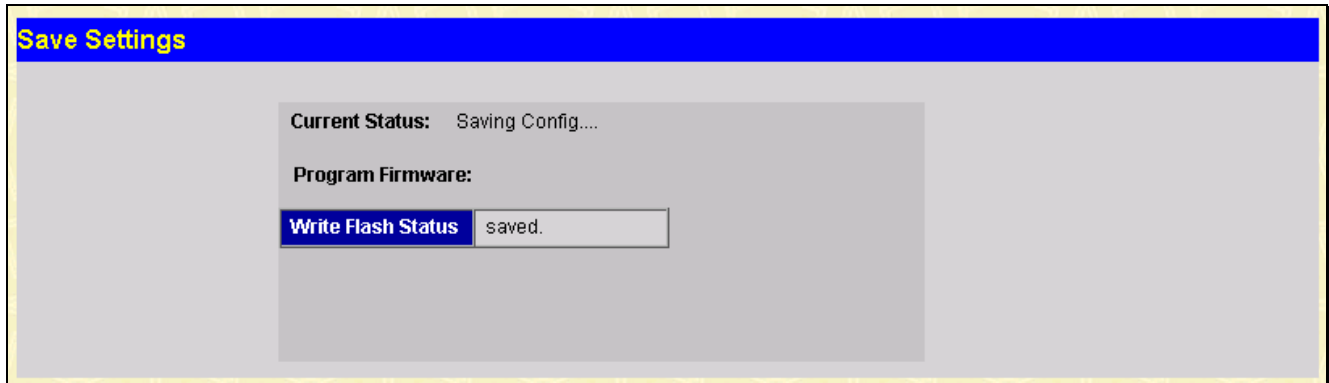
Figure 11- 9. Save Settings window (only save configuration)
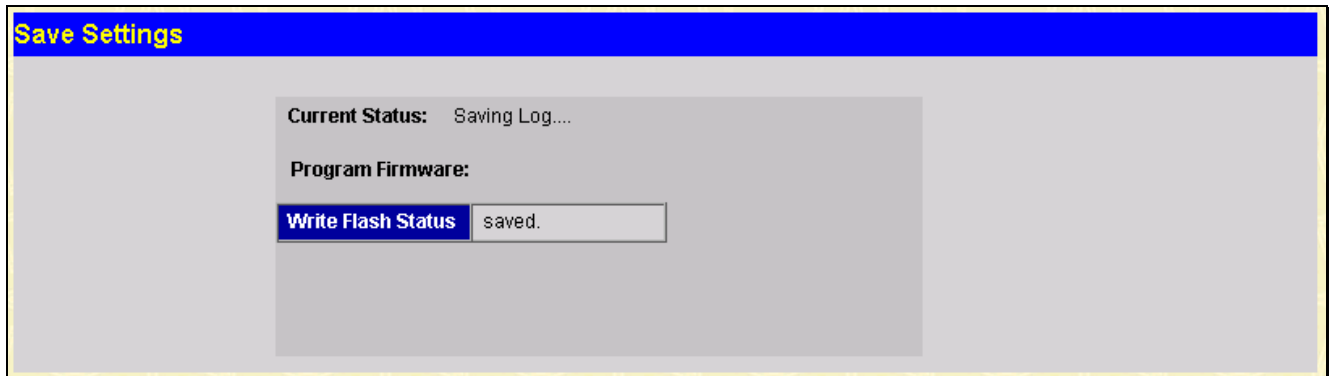
Figure 11- 10. Save Settings window (only save log)
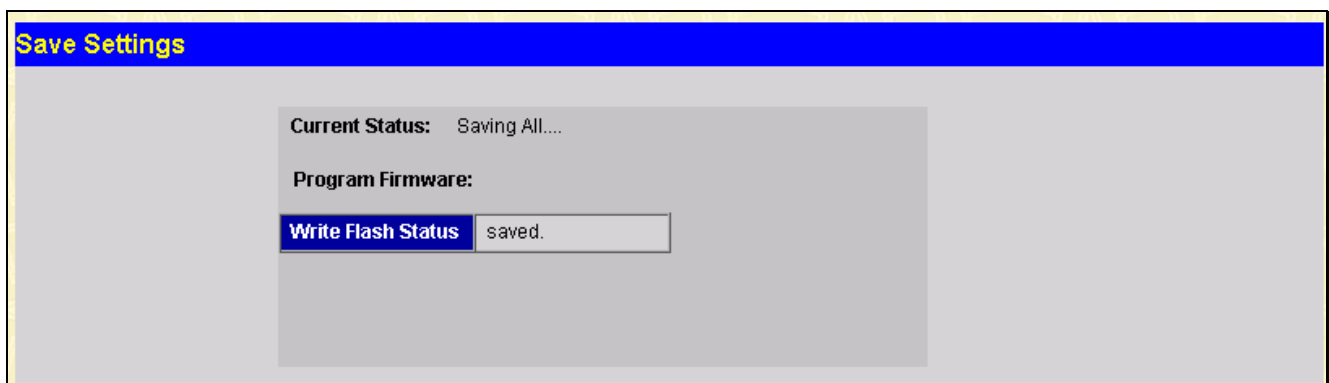
Figure 11- 11. Save Settings window (save configuration and log)
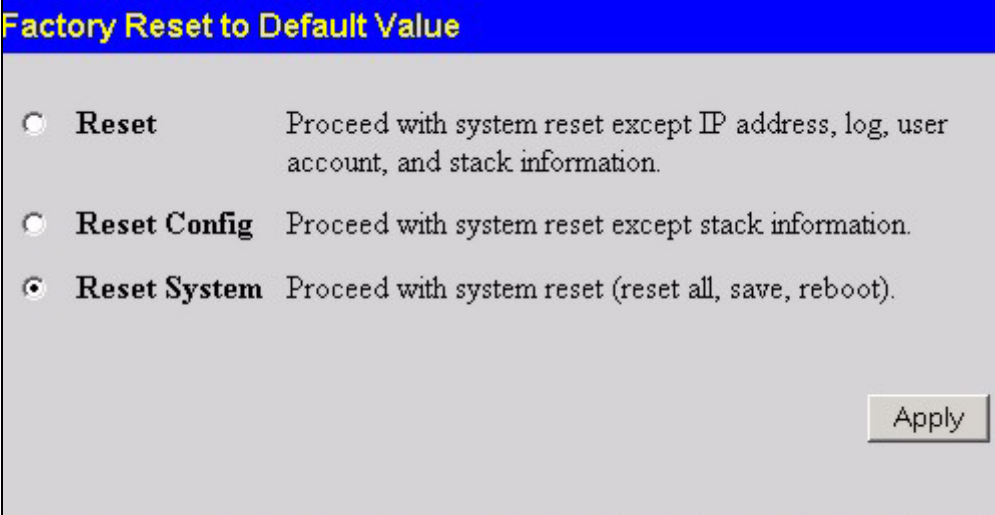
These settings will be used every time the Switch is rebooted. See the Reset section for more information on changing configurations saved to NV-Ram.

Reset

The **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.

NOTE: Only 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

Figure 11- 12. Factory Reset to Default Value window

Reboot Device

The following window is used to restart the Switch.

Figure 11- 13. Restart System window

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.

Logout

Use the **Logout** page to logout of the Switch's Web-based management agent by clicking on the **Log Out** button.
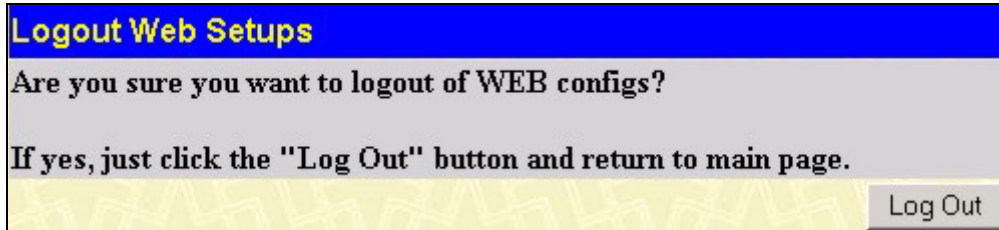
Figure 11- 14. Logout Web Setups window

Single IP Management

SIM Settings

Topology

Firmware Upgrade

Configuration Backup/Restore

Simply put, D-Link Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. There are some advantages in implementing the "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 D-Link 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 or Web 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 switches that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The DXS-3326GSR may take on three different roles:

1. **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.

2. **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.

3. **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 DXS-3326GSR, 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-3324SRi 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, 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 CaS 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.

SIM Settings

All DXS-3326GSR switches are set as Candidate (CaS) switches as their factory default configuration and Single IP Management is 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.

Figure 12- 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 new **SIM Settings** window will look like this:

Figure 12- 2. SIM Settings window (enabled)

The following parameters can be set:

Parameters	Description
SIM State	Use the pull-down menu to either enable or disable the SIM state on the Switch. *Disabled* will render all SIM functions on the Switch inoperable.
Role State	Use the pull-down menu to change the SIM role of the Switch. The two choices are:
	Candidate - 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 DXS-3326GSR.
	Commander - 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.
Discovery Interval	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.
Holdtime	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.

Figure 12- 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 12- 4. Single IP Management Tree View window

The Tree View window holds the following information under the **Data** tab:

Parameter	Description
Device Name	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.
Local Port	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.
Speed	Displays the connection speed between the CS and the MS or CaS.
Remote Port	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.
MAC Address	Displays the MAC Address of the corresponding Switch.
Model Name	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 window. The Topology View will refresh itself periodically (20 seconds by default).

Figure 12- 5. Topology view

This window 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:

Icon	Description
	Group
	Layer 2 commander switch
	Layer 3 commander switch
	Commander switch of other group
	Layer 2 member switch
	Layer 3 member switch
	Member switch of other group

	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.
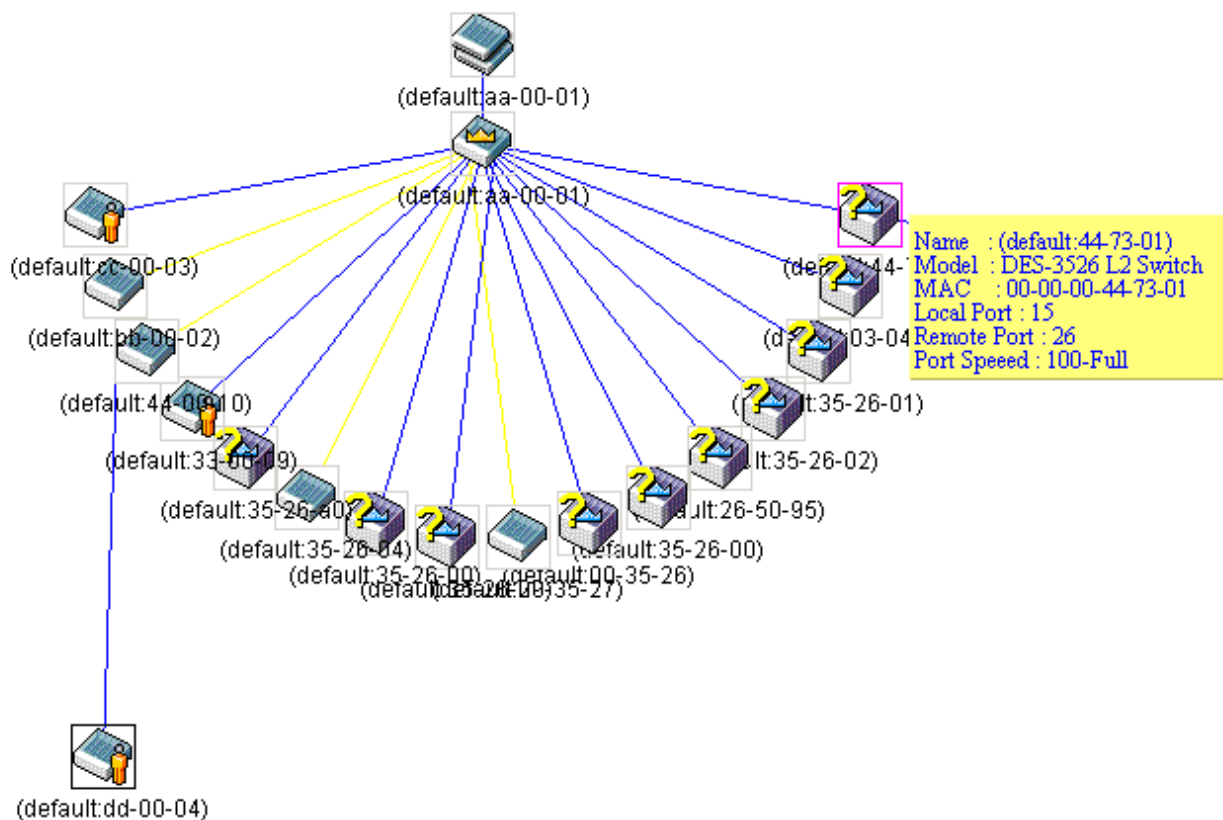
Figure 12- 6. Device Information Utilizing the Tool Tip

Setting the mouse cursor over a line between two devices will display the connection speed between the two devices, as shown below.

Figure 12- 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 12- 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 12- 9. Property window

Commander Switch Icon
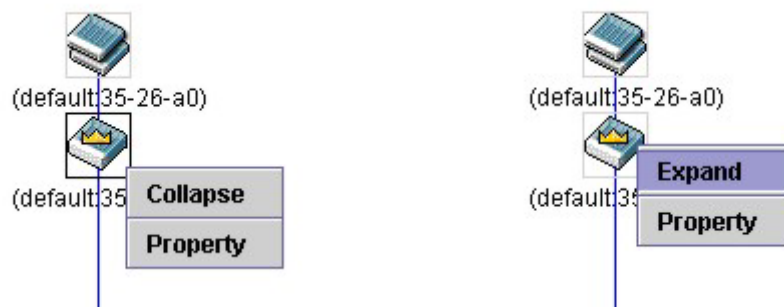
Figure 12- 10. Right-clicking a Commander Icon

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.
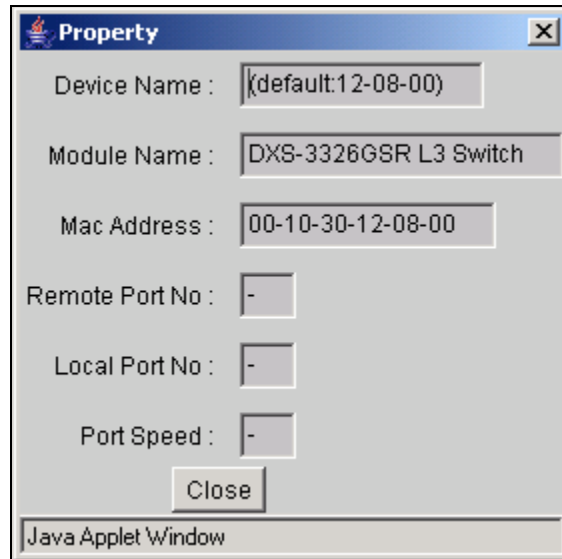
Figure 12- 11. Property window

Member Switch Icon
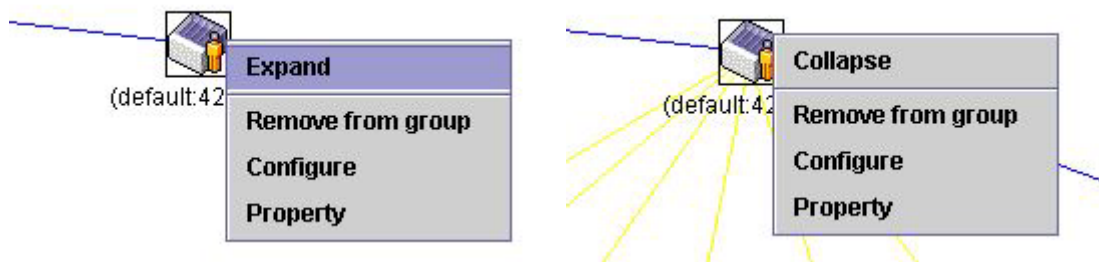
Figure 12- 12. Right-Clicking a Member icon

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.
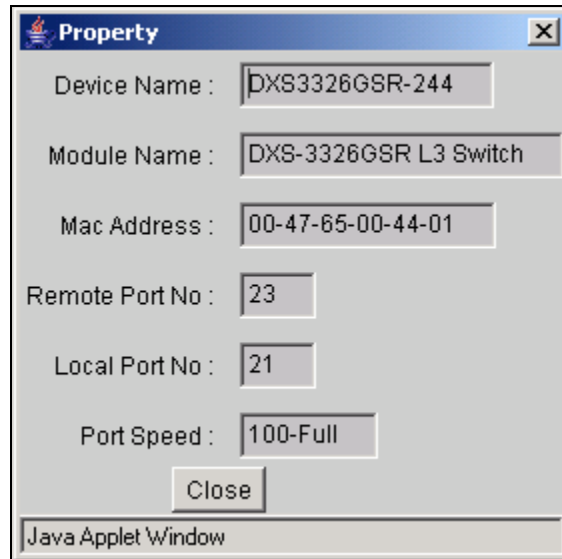
Figure 12- 13. Property window

Candidate Switch Icon
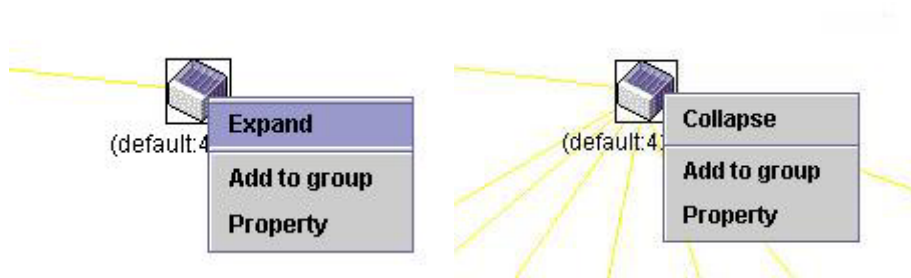
Figure 12- 14. Right-Clicking a Candidate icon

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.
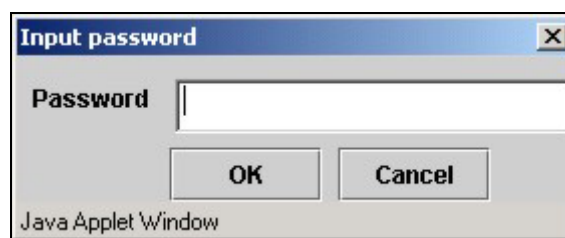
Figure 12- 15. Input password window.

- **Property** - To pop up a window to display the device information, as shown below.

257
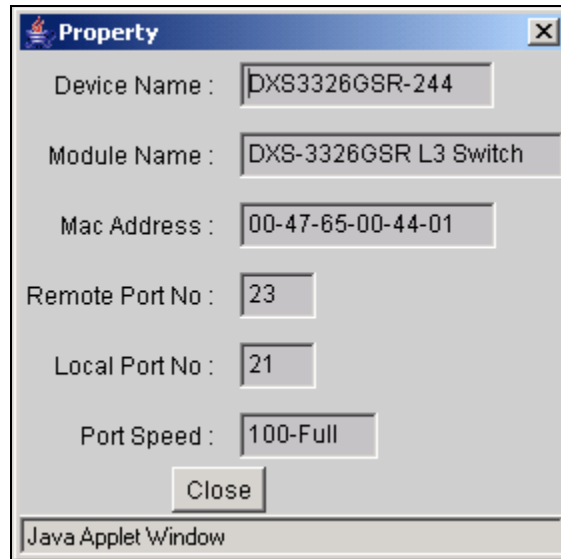
Figure 12- 16. Device Property window

This window holds the following information:

Parameter	Description
Device Name	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.
Module Name	Displays the full module name of the switch that was right-clicked.
MAC Address	Displays the MAC Address of the corresponding Switch.
Remote Port No.	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.
Local Port No.	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.
Port Speed	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 12- 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 12- 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.

NOTE: Upon this firmware release, some functions of the SIM can only be configured through the Command Line Interface. See the ***DXS-3326GSR Command Line Interface Reference Manual*** for more information on SIM and its configurations.

Firmware Upgrade

This window 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/Filename of the firmware. Click **Download** to initiate the file transfer.

Figure 12- 19. Firmware Upgrade window

Configuration File Backup/Restore

This window is used to both backup and restore configuration files from the Commander Switch to the Member Switch using a TFTP server. 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.

Figure 12- 20. Configuration File Backup/Restore window

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 file resides and enter the Path/Filename of the configuration file. Click **Download** to initiate the file transfer from a TFTP server to the Switch. Click **Upload** to backup the configuration file to a TFTP server.

Appendix A

Technical Specifications

Physical and Environmental	
AC Input & External Redundant Power Supply	100 – 120; 200 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption	66 watts maximum
DC Fans	2 built-in 40 x 40 x10 mm fans
Operating Temperature	0 to 40 degrees Celsius
Storage Temperature	-25 to 55 degrees Celsius
Humidity	Operating: 5% to 95% RH non-condensing Storage: 0% to 95% RH non-condensing
Dimensions	445 mm x 430 mm x 45 mm
Weight	5.5 kg
EMC	FCC Part 15 Class A / IECES-003 Class (Canada) EN55022 Class A / EN55024
Safety	CSA International

General	
Standards	IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1D Spanning Tree IEEE 802.1W Rapid Spanning Tree IEEE 802.1 P/Q VLAN IEEE 802.1p Priority Queues IEEE 802.3ad Link Aggregation Control IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation
Protocols	CSMA/CD
Data Transfer Rates	Half duplex Full duplex
Ethernet	10 Mbps 20 Mbps
Fast Ethernet	100 Mbps 200 Mbps
Gigabit Ethernet	2000 Mbps (Full duplex only)
Topology	Star
Network Cables	
10BASE-T	UTP Category 3, 4, 5 (100 meters max.)

100BASE-TX	EIA/ TIA- 568 150-ohm STP (100 meters max.)
	UTP Cat. 5 (100 meters max.)
	EIA/TIA-568 150 -ohm STP (100 meters max.)
1000BASE-T	UTP Cat. 5e (100 meters max.)
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)
Mini-GBIC	SFP Transceiver for 1000BASE-LX Single-mode fiber module (10km)
Number of Ports	24 Mini-GBIC Ports
	4 1000BASE-T Combo ports

Performance

Transmission Method	Store-and-forward
Packet Buffer	16 MB per device
Packet Filtering/Forwarding Rate	Full-wire speed for all connections. 1,488,095 pps per port (for 1000Mbps)
MAC Address Learning	Automatic update. Supports 8K MAC address.
Priority Queues	8 Priority Queues per port.
Forwarding Table Age Time	Max age: 10-1000000 seconds. Default = 300.

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.
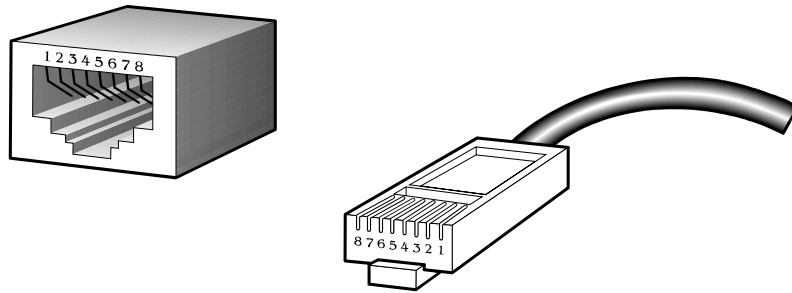
Appendix B- 1. The standard RJ-45 port and connector

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

Appendix 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.

aging: 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.

D-Link International Offices

U.S.A
17595 Mt. Herrmann Street
Fountain Valley, CA 92708
TEL: 714-885-6000
FAX: 866-743-4905
URL: www.dlink.com

Canada
2180 Winston Park Drive
Oakville, Ontario, L6H 5W1
Canada
TEL: 1-905-8295033
FAX: 1-905-8295223
URL: www.dlink.ca

Europe (U. K.)
4th Floor, Merit House
Edgware Road, Colindale
London NW9 5AB
U.K.
TEL: 44-20-8731-5555
FAX: 44-20-8731-5511
URL: www.dlink.co.uk

Germany
Schwalbacher Strasse 74
D-65760 Eschborn
Germany
TEL: 49-6196-77990
FAX: 49-6196-7799300
URL: www.dlink.de

France
Le Florilege #.2, Allee de la Fresnerie
78330 Fontenay le Fleury
France
TEL: 33-1-30238688
FAX: 33-1-30238689
URL: www.dlink-france.fr

Netherlands
Weena 290
3012 NJ Rotterdam
Netherlands
TEL: +31-10-282-1445
FAX: +31-10-282-1331
URL: www.dlink-benelux.com

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

Italy
Via Nino Bonnet n. 6/b
20154 – Milano,
Italy
TEL: 39-02-2900-0676
FAX: 39-02-2900-1723
URL: www.dlink.it

Sweden
P.O. Box 15036, S-167 15 Bromma
Sweden
TEL: 46-(0)8564-61900
FAX: 46-(0)8564-61901
URL: www.dlink.se

Denmark
Naverland 2, DK-2600
Glostrup, Copenhagen,
TEL: 45-43-969040
FAX: 45-43-424347
URL: www.dlink.dk

Norway
Karihaugveien 89
1086 Oslo
Norway
TEL: 47-22-309075
FAX: 47-22-309085
URL: www.dlink.no

Finland
Pakkalankuja 7A
01510 Vantaa,
Finland
TEL : +358-9-2707 5080
FAX: + 358-9-2707 5081
URL: www.dlink.fi

Iberia
C/Sabino De Arana,
56 Bajos
08028 Barcelona
TEL: 34 93 4090770
FAX: 34 93 4910795
URL: www.dlinkiberia.es

Singapore
1 International Business Park
#03-12 The Synergy
Singapore 609917
TEL: 65-6774-6233
FAX: 65-6774-6322
URL: www.dlink-intl.com

Australia
1 Giffnock Avenue,
North Ryde, NSW 2113
Australia
TEL: 61-2-8899-1800
FAX: 61-2-8899-1868
URL: www.dlink.com.au

India
D-Link House, Kurla Bandra Complex Road,
Off CST Road, Santacruz (East), Mumbai - 400098.
India
TEL: 91-022-26526696/56902210
FAX: 91-022-26528914
URL: www.dlink.co.in

Middle East (Dubai)
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: www.dlink-me.com

Turkey
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: www.dlink.com.tr

Egypt
19 El-Shahed Helmy, El Masri
Al-Maza, Heliopolis
Cairo, Egypt
TEL:+202 414 4295
FAX:+202 415 6704
URL: www.dlink-me.com

Israel
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: www.dlink.co.il

Latin America
Isidora Goyeechea 2934 of 702,
Las Condes
Santiago – Chile S.A.
TEL: 56-2-232-3185
FAX: 56-2-232-0923
URL: www.dlink.cl

Brasil
Av das Nacoes Unidas,
11857 - 14 - andar - cj 141/142
Brooklin Novo
Sao Paulo - SP - Brazil
CEP 04578-000
TEL: +55 11 55039320
FAX: +55 11 55039322
URL: www.dlinkbrasil.com.br

South Africa
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: www.d-link.co.za

Russia
Grafsky per., 14, floor 6
Moscow
129626 Russia
TEL: 7-095-744-0099
FAX: 7-095-744-0099 #350
URL: www.dlink.ru

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

Taiwan
2F, No. 119, Pao-Chung Rd.
Hsin-Tien, Taipei
Taiwan
TEL: 886-2-2910-2626
FAX: 886-2-2910-1515
URL: www.dlinktw.com.tw

Headquarters
2F, No. 233-2, Pao-Chiao Rd.
Hsin-Tien, Taipei
Taiwan
TEL: 886-2-2916-1600
FAX: 886-2-2914-6299
URL: www.dlink.com

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., 53 Discovery Drive, Irvine, CA 92618**. 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:

D-Link ®