D-Link
Building Networks for People

xStack User Manual

Product Model: xStack™ DGS-3400 Series

Layer 2 Gigabit EthernetManaged Switch

Release 2.3

October 2007 P/N 651GS3400055G

Table of Contents

Intended Readers

The ***xStack DGS-3400 series Manual*** contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry. For example: [copy filename] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
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 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 the actual filename should be typed 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 make better use of the device.

A **NOTICE** indicates either potential damage to hardware or loss of data and tells 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 need to be reviewed and followed.

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 the system documentation.
  - Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose the user 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:
  - Damage to the power cable, extension cable, or plug.
  - 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 the operating instructions are correctly followed.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in the troubleshooting guide or contact your trained service provider.
- Do not push any objects into the openings of the 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 unsure of the type of power source required, consult your service provider or local power company.
- To help avoid damaging the system, be sure the voltage selection switch (if provided) on the power supply is set to match the power available at the Switch's 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 using an extension cable is necessary, 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 the 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 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.

Lithium Battery Precaution

CAUTION: Incorrectly replacing the lithium battery of the Switch may cause the battery to explode. Replace this battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturers instructions.

Protecting Against Electrostatic Discharge

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

The following steps can also be taken 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 ready to install the component in the 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

The DGS-3400 Gigabit Ethernet switches are members of the D-Link xStack family. Ranging from 10/100Mbps edge switches to core gigabit switches, the xStack switch family has been future-proof designed to deliver a system with fault tolerance, flexibility, port density, robust security and maximum throughput with a user-friendly management interface for the networking professional.

This manual describes the installation, maintenance and configurations concerning members of the xStack DGS-3400 Switch Series. These switches include: the DGS-3426, DGS-3426P, DGS-3427 and the DGS-3450. The xStack DGS-3400 Series switches are similar in configurations and basic hardware and consequentially, most of the information in this manual will be universal to the whole xStack DGS-3400 Series. Corresponding screen pictures of the web manager may be taken from any one of these switches but the configuration will be identical, except for varying port counts.

Switch Description

D-Link's next-generation xStack DGS-3400 Series switches are high port-density stackable switches that combine the ultimate performance with fault tolerance, security, management functions with flexibility and ease-of-use. All these features, typically found in the more expensive chassis-based solutions, are available from the xStack DGS-3400 switch series at the price of a stackable switch!

All xStack DGS-3400 Series switches have some combination of 1000BASE-T ports, SFP ports and 10-Gigabit 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. The SFP (Small Form Factor Portable) combo ports are used with fiber-optical transceiver cabling in order to uplink various other networking devices for a gigabit link that may span great distances. These 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), DEM-312GT2 (100BASE-SX) and DEM-315GT (1000BASE-ZX) transceivers. Users may also use one of the WDM Single Mode Transceivers, such as the DEM-330T/R or the DEM-331T/R. The rear panel of the xStack DGS-3400 Series Switches include spaces for optional single-port module inserts for single port 10GE XFP or 10GBASE-CX4 modules used for backbone uplink or stacking connection to another xStack DGS-3400 Series Switch.

Features

The list of features below highlights the significant features of the xStack DGS-3400 Series.

- 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
- IEEE 802.3af Power-over-Ethernet support for the DGS-3426P
- Stacking support in either Duplex-Ring or Duplex-Chain 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
- Port Trunking with flexible load distribution and fail-over function
- IGMP Snooping support
- MLD Snooping support (MLD v1 and v2)
- SNMP support
- Secure Sockets Layer (SSL) and Secure Shell (SSH) support

- System Severity control
- 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.
- PoE Support for the DGS-3426P
- IPv6 Support

Ports

The xStack DGS-3400 Series switches port options, as listed by device.

DGS-3426	DGS-3426P	DGS-3427	DGS-3450
• Twenty-four 10/100/1000BASE-T Gigabit ports • Four Combo SFP Ports • Two slots open for single port 10GE XFP or 10GBASE-CX4 modules • One RS-232 DB-9 console port	• Twenty-four PoE Compliant 10/100/1000BASE-T Gigabit ports • Four Combo SFP Ports • Two slots open for single port 10GE XFP or 10GBASE-CX4 modules • One RS-232 DB-9 console port	• Twenty-four 10/100/1000BASE-T Gigabit ports • Four Combo SFP Ports • Three slots open for single port 10GE XFP or 10GBASE-CX4 modules • One RS-232 DB-9 console port	• Forty-eight 10/100/1000BASE-T Gigabit ports • Four Combo SFP Ports • Two slots open for single port 10GE XFP or 10GBASE-CX4 modules • One RS-232 DB-9 console port

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

Front-Panel Components

The front panel of the Switch consists of LED indicators for Power, Master, Console, RPS, and for Link/Act for each port on the Switch including 10GE Ports for optional modules and SFP port LEDs. The front panel includes a seven-segment LED indicating the Stack ID number. A separate table below describes LED indicators in more detail. DGS-3426P also includes a Mode Select button for changing the mode Link/Act/State to PoE.

DGS-3426

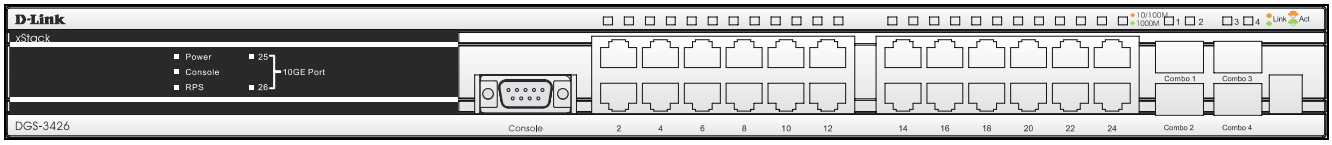


Figure 2- 1. Front Panel View of the DGS-3426 as shipped

DGS-3426P

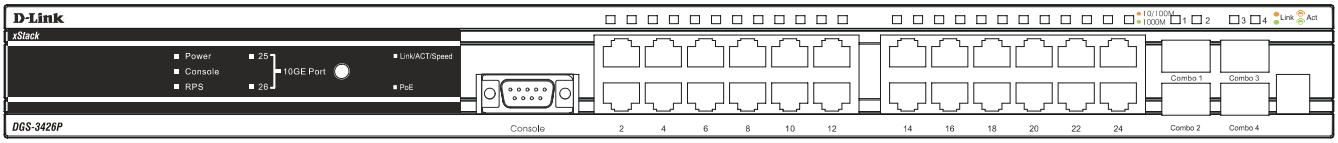


Figure 2- 2. Front Panel View of the DGS-3426P as shipped

DGS-3427

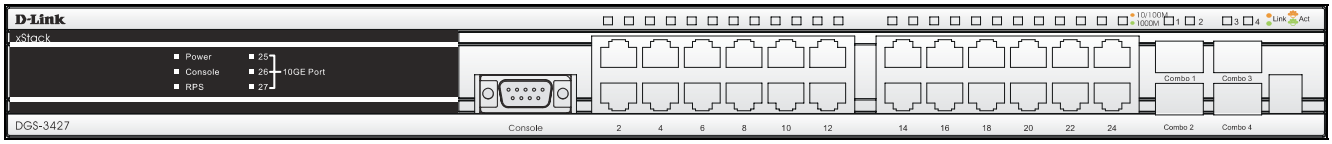


Figure 2- 3. Front Panel View of the DGS-3427 as shipped

DGS-3450

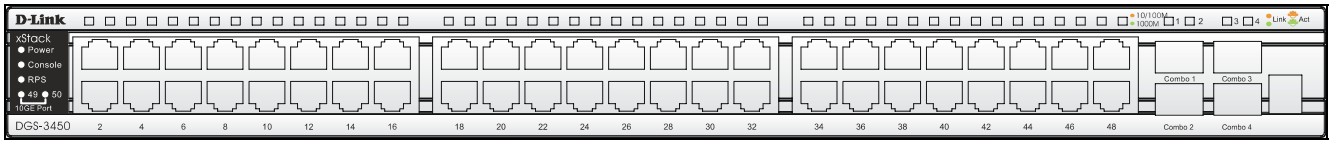


Figure 2- 4. Front Panel View of the DGS-3450 as shipped

LED Indicators

The Switch supports LED indicators for Power, Console, RPS and Port LEDs including 10GE port LEDs for optional module inserts.

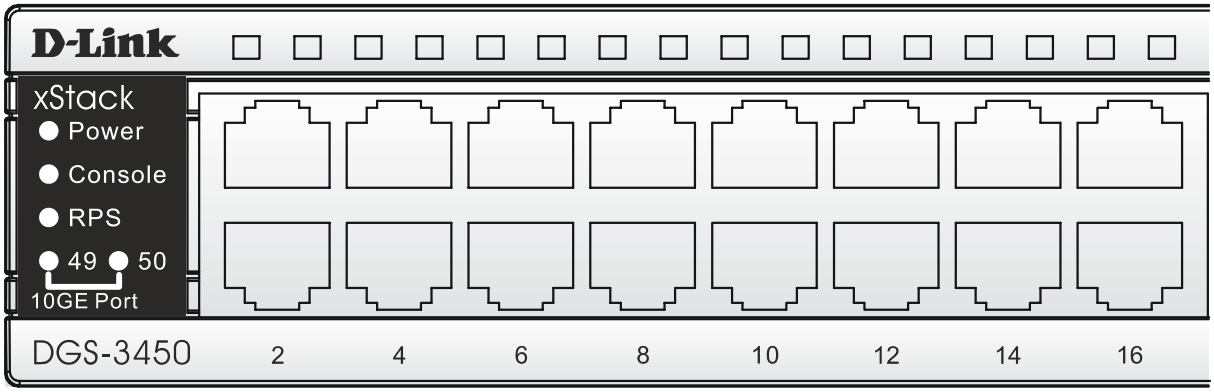


Figure 2- 5. LED Indicators on DGS-3450

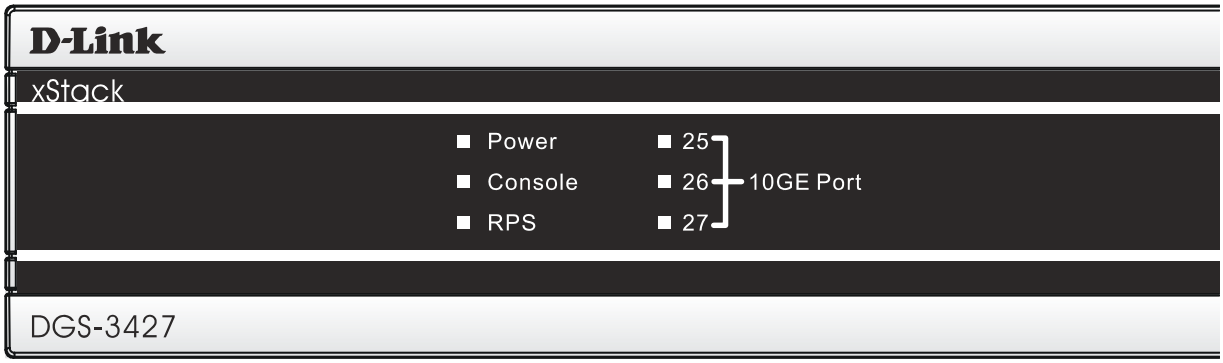


Figure 2- 6. LED Indicators on DGS-3427

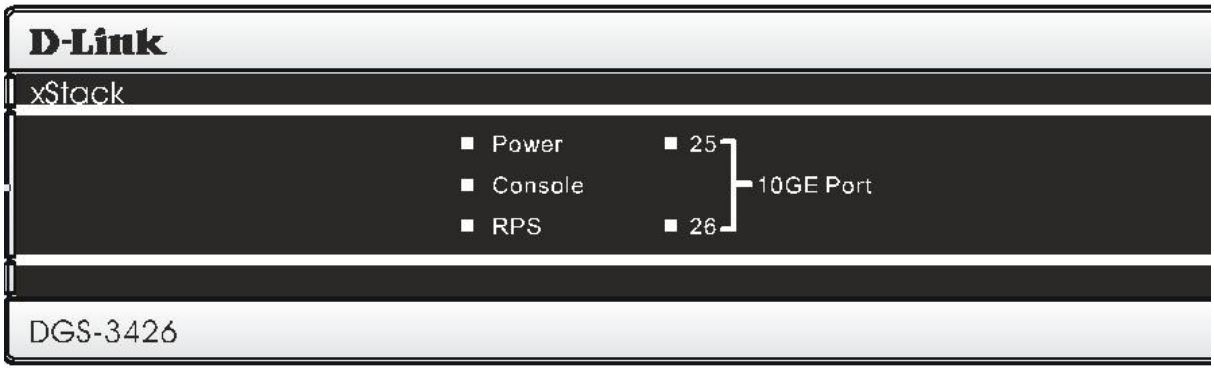


Figure 2- 7. LED Indicators on DGS-3426

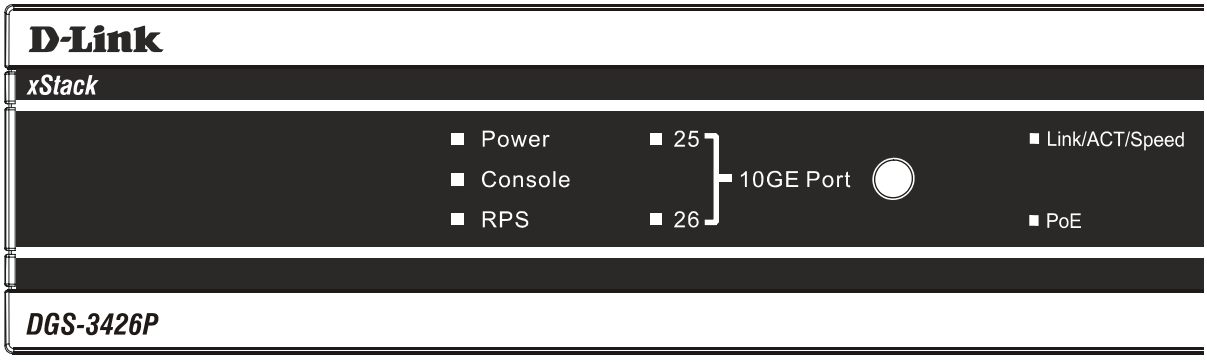


Figure 2- 8. LED Indicators on DGS-3426P

LED	Description
Power	This LED will light green after powering the Switch on to indicate the ready state of the device. The indicator is dark when the Switch is no longer receiving power (i.e powered off).
Console	This LED will blink green during the Power-On Self Test (POST). When the POST is finished, the LED goes dark. The indicator will light steady green when an active console link is in session via RS-232 console port.
RPS	This LED will light 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 indicator above the left side of a port corresponds to the port below the indicator in the upper row of ports. The indicator above the right side of a port corresponds to the port below the indicator in the lower row of ports. A steady green light denotes a valid 1000Mbps link on the port while a blinking green light indicates activity on the port (at 1000Mbps). A steady orange light denotes a valid 10 or 100Mbps link on the port while a blinking orange light indicates activity on the port (at 100Mbps). These LEDs will remain dark if there is no link/activity on the port.
10GE Ports	A steady green light denotes a valid link on the port while a blinking green light indicates activity on the port. These LEDs will remain dark if there is no link/activity on the port.
Combo SFP Ports	LED indicators for the Combo ports are located above the ports and numbered 1 – 4 for Combo 1, Combo 2, etc. ports. A steady green light denotes a valid link on the port while a blinking green light indicates activity on the port. These LEDs will remain dark if there is no link/activity on the port.
Stack ID	These two seven segment LEDs display the current switch stack order of the Switch while in use.
Link/Act/Speed and PoE (DGS-3426P only)	To change the LED mode from Link/Act/Speed to PoE and vice versa, press the LED Mode Select Button. The Link/Act/Speed LED will light solid green when selected and will shut off when PoE is selected. Likewise, when Link/Act/Speed is selected, the PoE LED shuts off and the Link/Act/Speed LED lights solid green.

Rear Panel Description

DGS-3426

The rear panel of the DGS-3426 contains an AC power connector, a redundant power supply connector and two empty slots for optional module inserts.

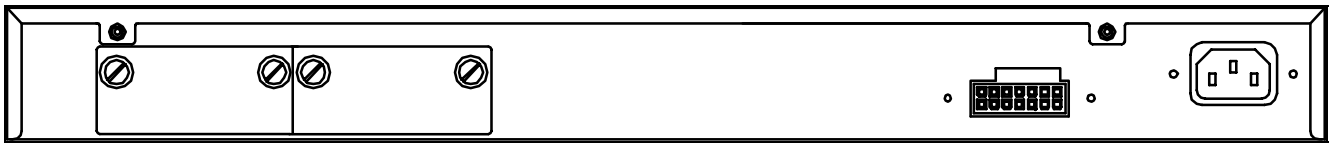


Figure 2- 9. Rear panel view of DGS-3426

DGS-3426P

The rear panel of the DGS-3426P contains an AC power connector, a redundant power supply connector, a heat vent for the rear fan and two empty slots for optional module inserts.

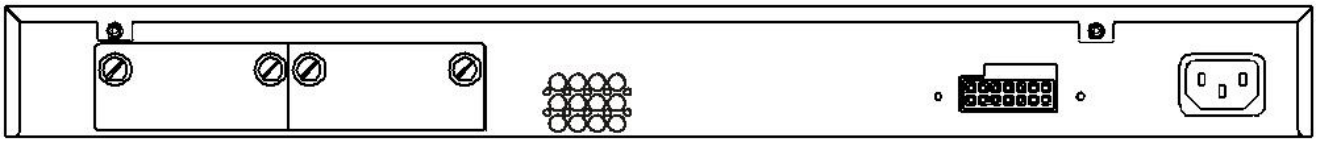


Figure 2- 10. Rear panel view of the DGS-3426P

DGS-3427

The rear panel of the DGS-3427 contains an AC power connector, a redundant power supply connector and three empty slots for optional module inserts.

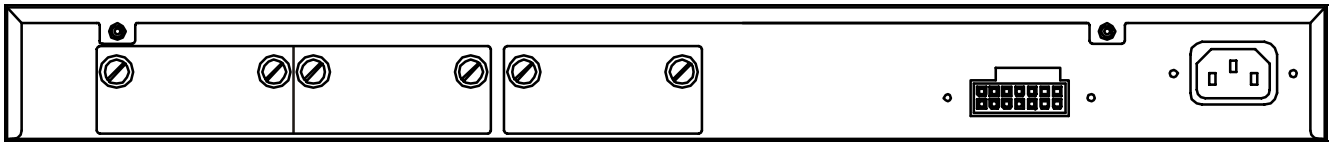


Figure 2- 11. Rear panel view of DGS-3427

DGS-3450

The rear panel of the DGS-3450 contains an AC power connector, two empty slots for optional module inserts, a redundant power supply connector, a RS-232 DCE console port for Switch management and a system fan vent.

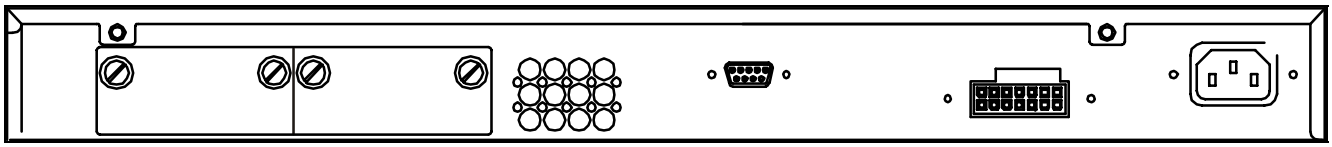


Figure 2- 12. Rear panel view of DGS-3450

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 a power failure occurs, the optional external RPS will automatically assume the power supply for the Switch immediately.

Side Panel Description

The system fans and heat vents located on each side dissipate heat. Do not block these openings. 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 and severely damage components.

Figure 2- 13. Side Panels (DGS-3450)

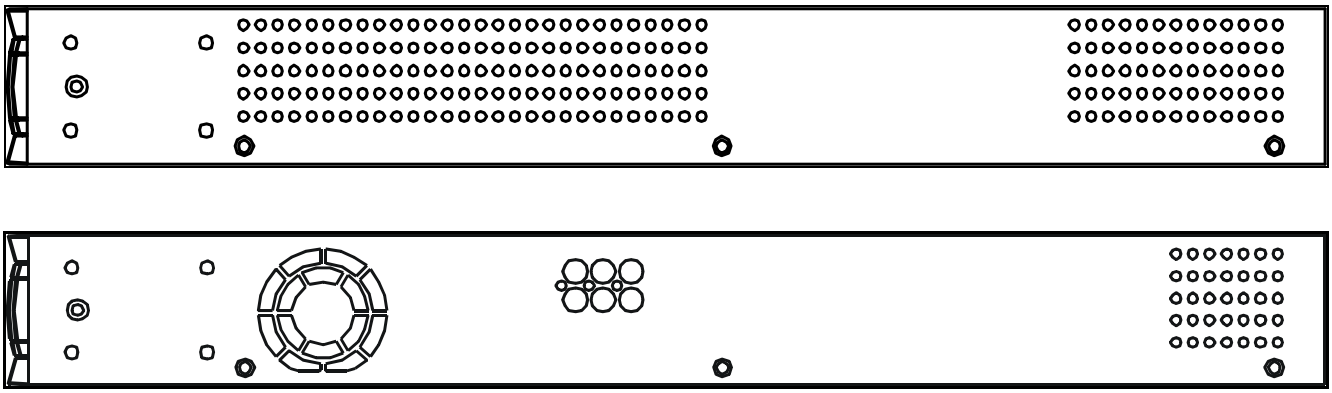


Figure 2- 14. Side Panels (DGS-3426 and DGS-3427)

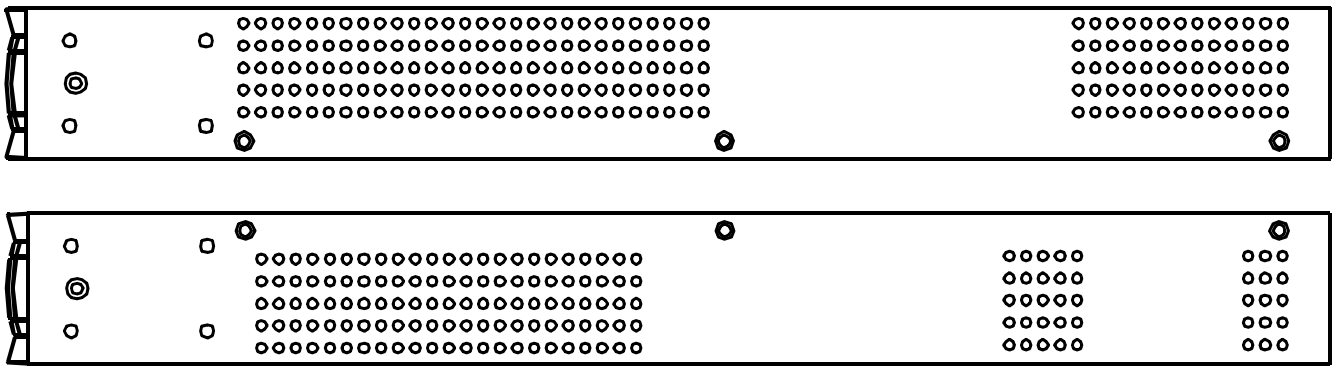


Figure 2- 15. Side Panels of the DGS-3426P

Section 2

Installation

Package Contents

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

1. One xStack Stackable Switch
2. One AC power cord
3. Mounting kit (two brackets and screws)
4. Four rubber feet with adhesive backing
5. RS-232 console cable
6. One CD Kit for User's Guide/CLI/D-View module
7. One CD Kit for D-View 5.1 Standard version (for Europe only)
8. Registration card & China Warranty Card (for China only)

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

Installation Guidelines

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

First, attach the rubber feet included with the Switch if installing on a desktop or shelf. 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.

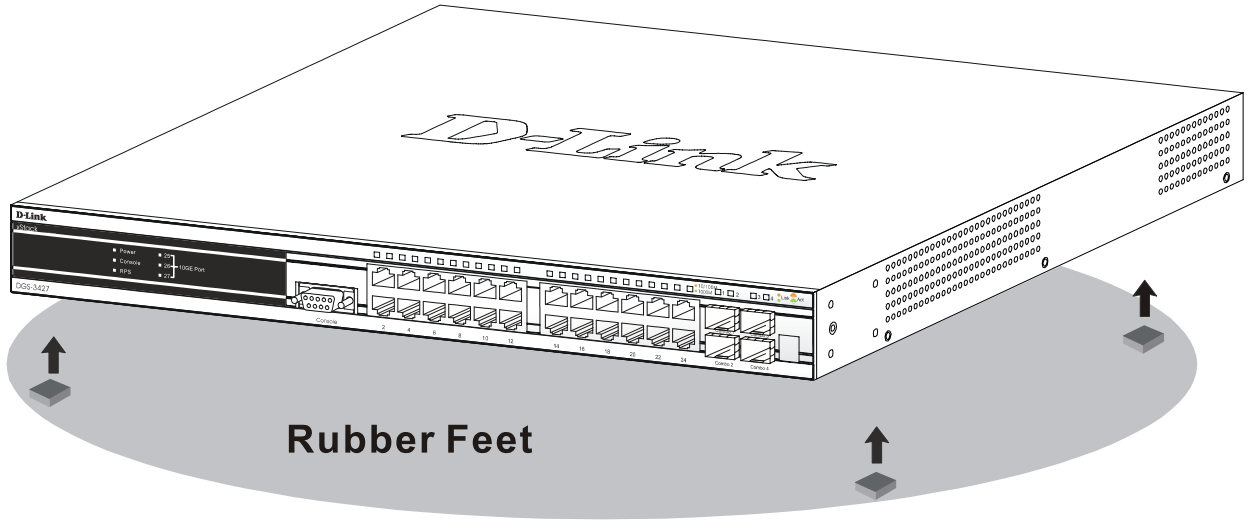


Figure 2- 16. Prepare Switch for installation on a desktop or shelf

Installing the Switch in a Rack

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

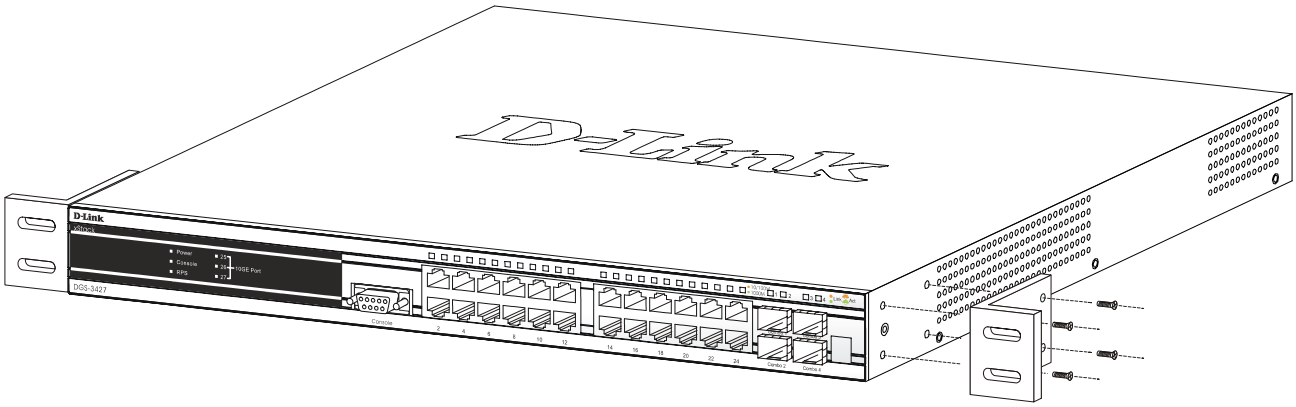


Figure 2- 17. Fasten mounting brackets to Switch

Fasten the mounting brackets to the Switch using the screws provided. With the brackets attached securely, the Switch can be mounted in a standard rack as shown below.

Mounting the Switch in a Standard 19" Rack

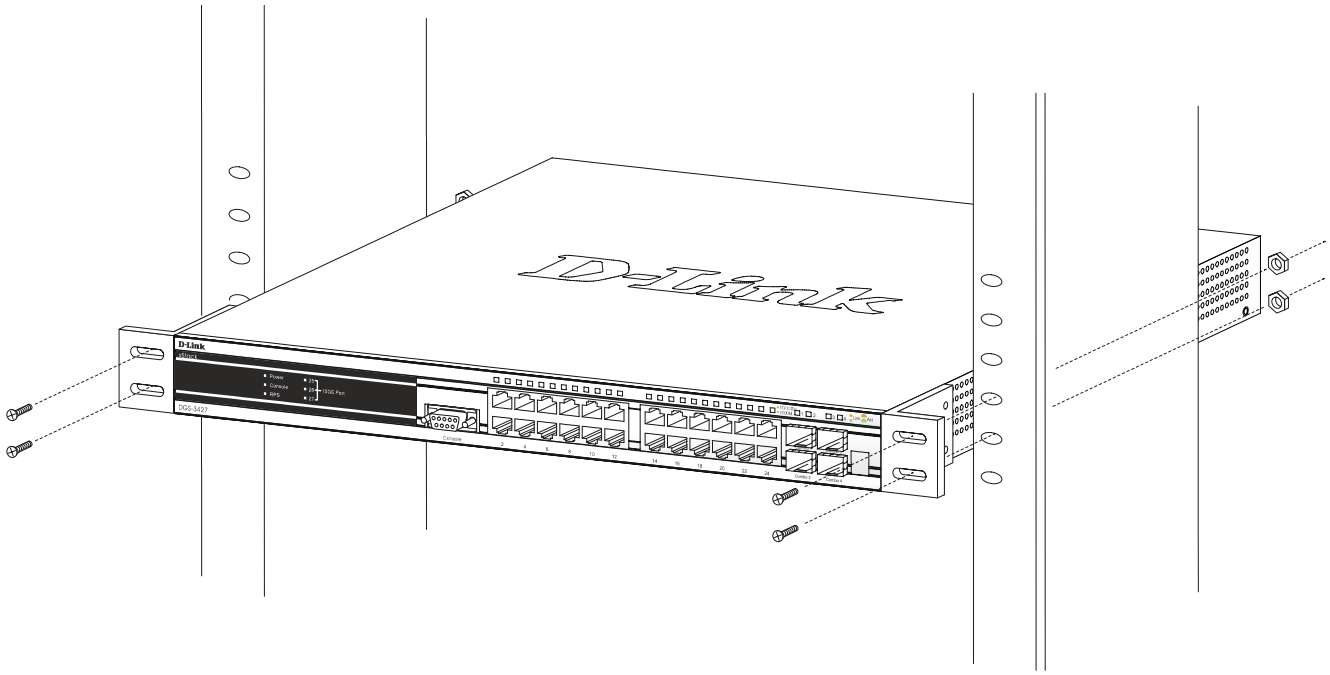


Figure 2- 18. Installing Switch in a rack

Power On

1. 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.
2. After powering on the Switch, 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.

Installing the SFP ports

The xStack DGS-3400 series switches are equipped with 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 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.

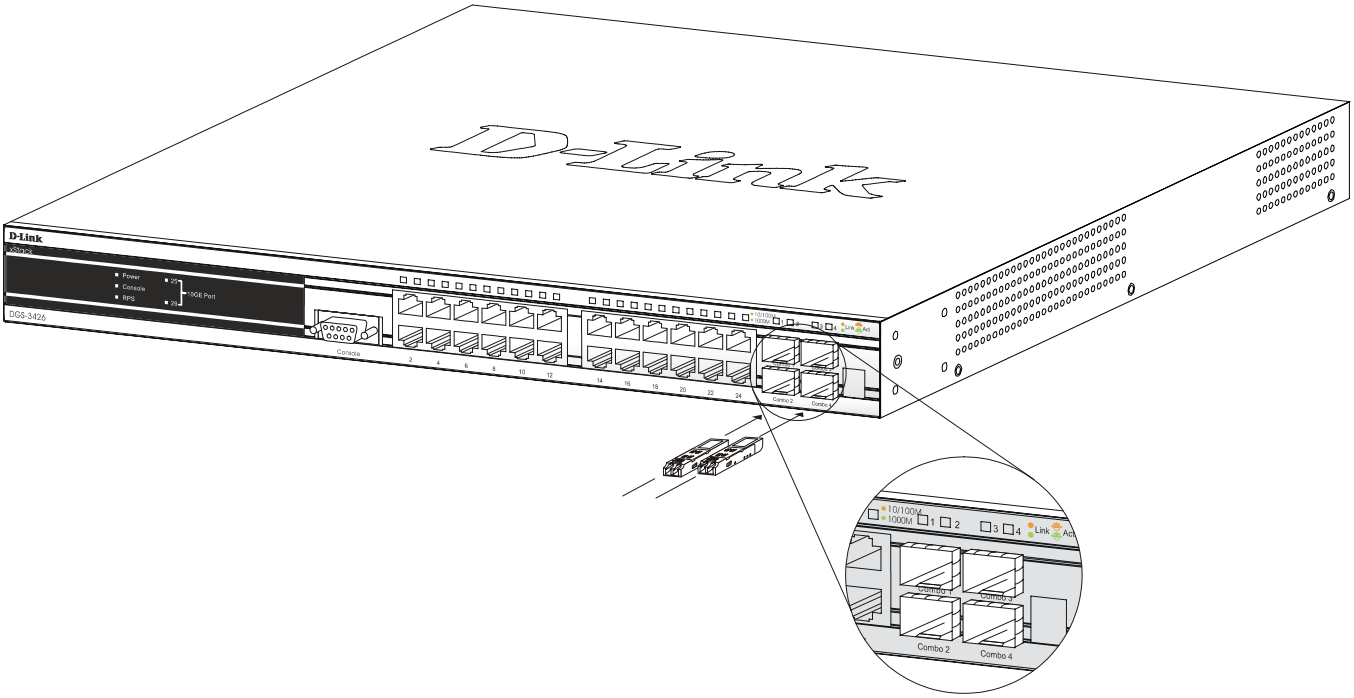


Figure 2- 19. Inserting the fiber-optic transceivers into the DGS-3426

The Optional Module

The rear panel of the DGS-3426, DGS-3426P, DGS-3427 and DGS-3450 include open slots that may be equipped with the DEM-410X 1-port 10GE XFP stacking uplink module, or a DEM-410CX 1-port 10GBASE-CX4 stacking uplink module, both sold separately. These modules may be used to stack switches in a switch stack using a Duplex Ring or Duplex Chain topology.

Adding the DEM-410X optional module will allow the administrator to transmit data at a rate of ten gigabits a second. The module port(s) are compliant with standard IEEE 802.3ae, support full-duplex transmissions only and must be used with XFP MSA compliant transceivers.

The DEM-410CX uses copper wire medium, not optic fiber and therefore has a transmit length limit up to 1 meter. Compliant with the IEEE802.3ak standard, this module uses a 4-laned copper connector for data transfer in full-duplex mode within a stacking configuration.

To install these modules in the DGS-3400 Series Switch, 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, which 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. This slot must be covered with the faceplate if the slot is not being used. If a module will be installed in an available slot, the faceplate is easily removed by loosening the screws and pulling off the plate.

The front panels of the available modules are shown here:

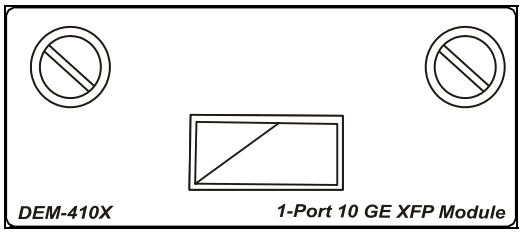


Figure 2- 20. Front Panel of the DEM-410X

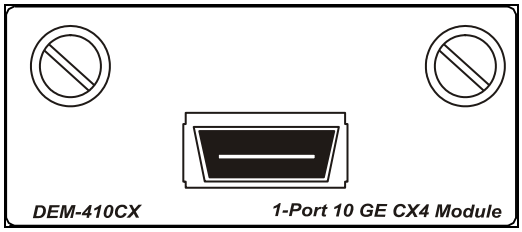


Figure 2- 21. Front Panel of the DEM-410CX

Installing the Module

Unplug the Switch before removing the faceplate covering the empty slot. To install the module, slide it in to the available slot at the rear of the Switch until it reaches the back, as shown in the following figure. Gently, but firmly push in on the module to secure it to the Switch. The module should fit snugly into the corresponding receptors.

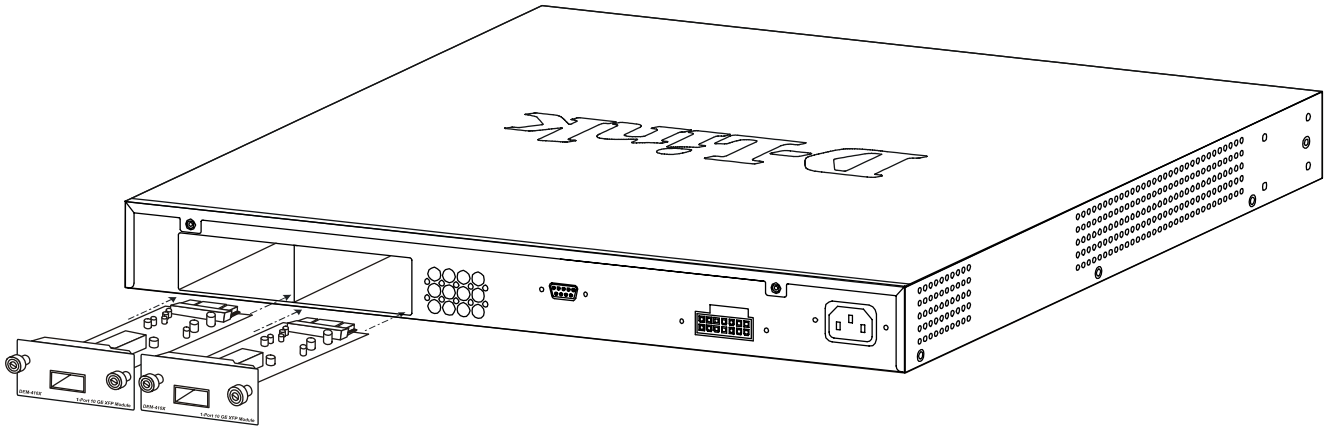


Figure 2- 22. Inserting the optional module into the Switch (DGS-3450)

Now tighten the two screws at adjacent ends of the module into the available screw holes on the Switch. The upgraded Switch is now ready for use.

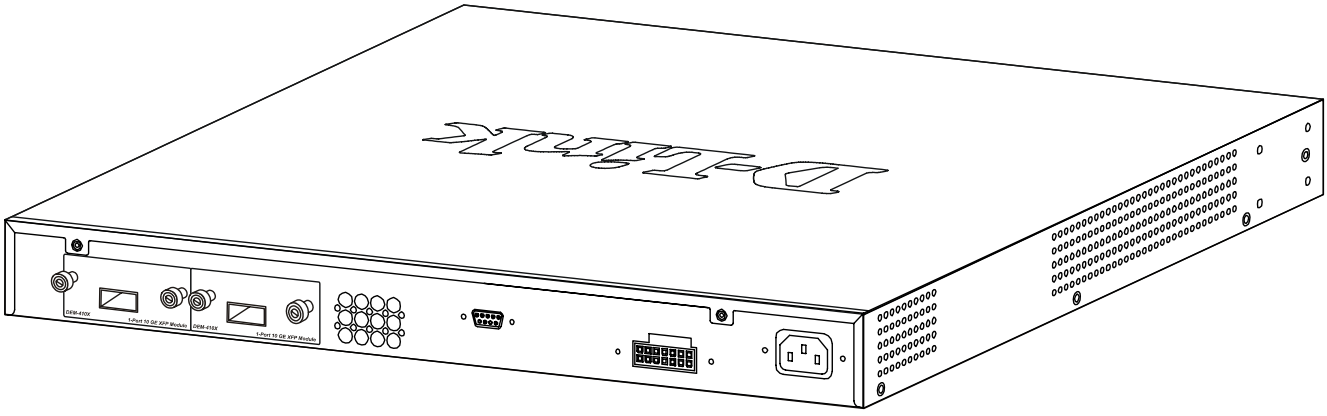


Figure 2- 23. DGS-3450 with optional DEM-410X module installed

External Redundant Power System

The Switch supports an external redundant power system. The diagrams below illustrate a proper RPS power connection to the Switch. Please consult the documentation for information on power cabling and connectors and setup procedure.

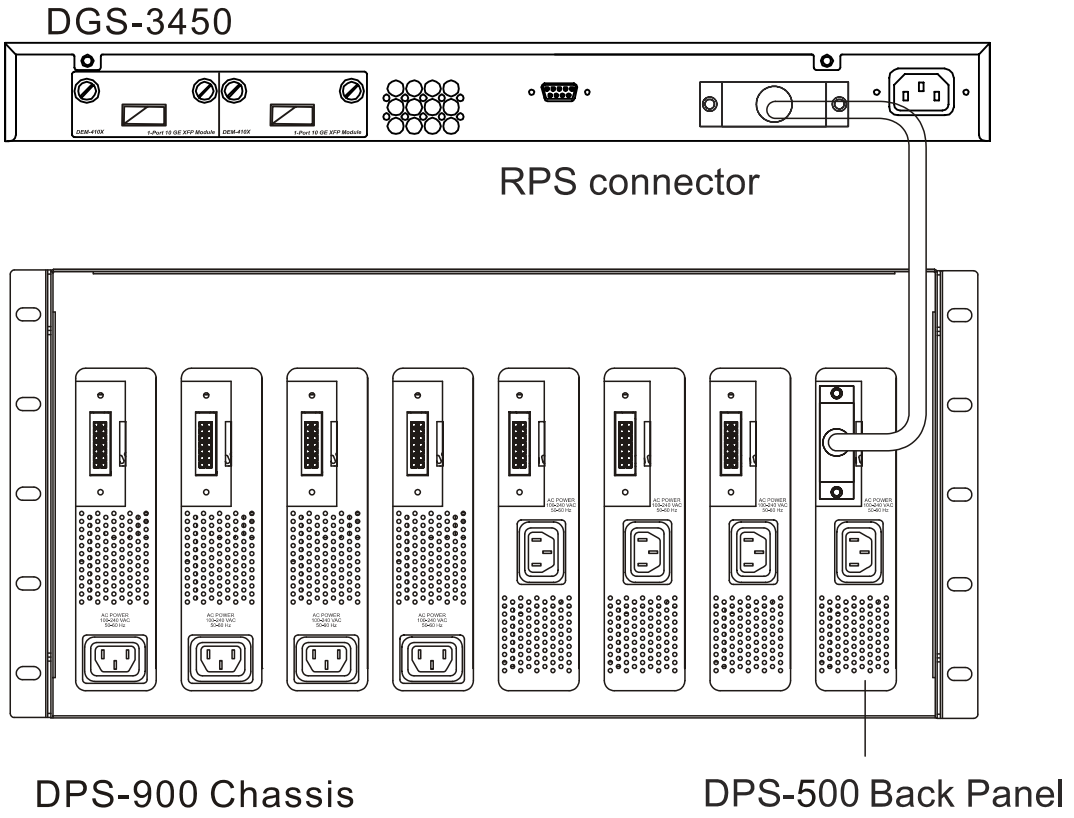


Figure 2- 24. The DGS-3450 with the DPS-500 chassis RPS

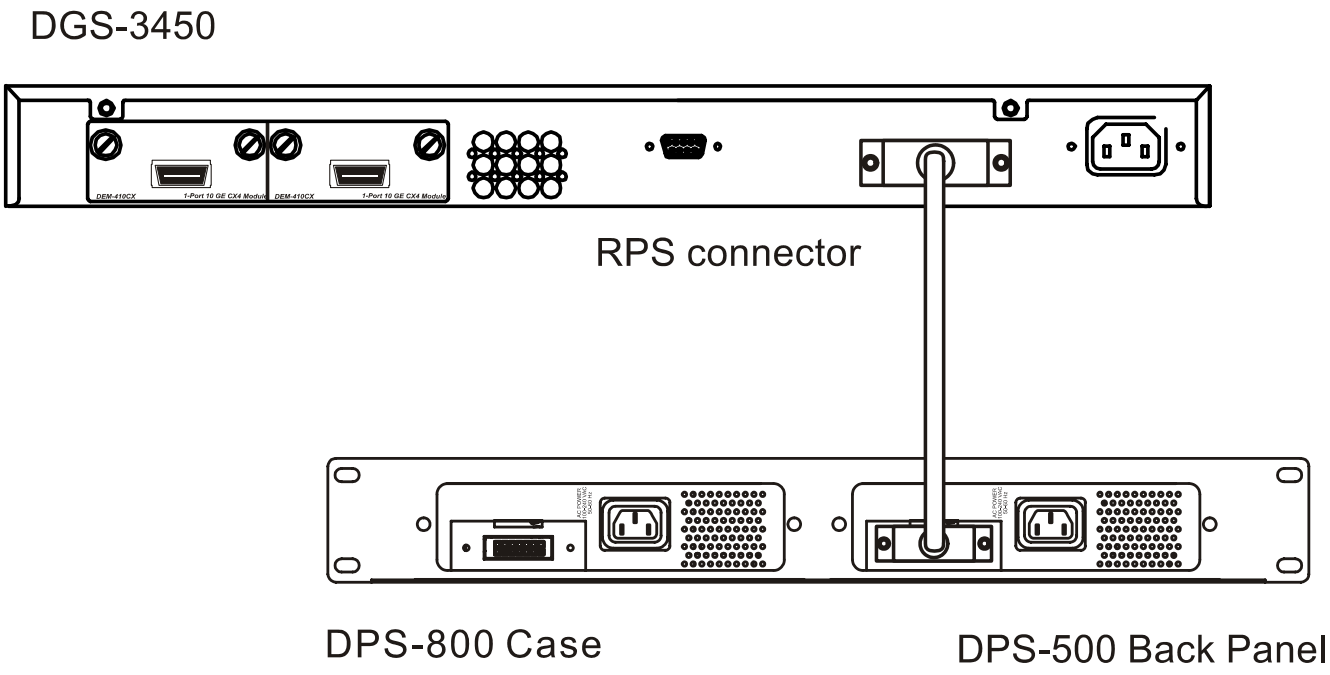
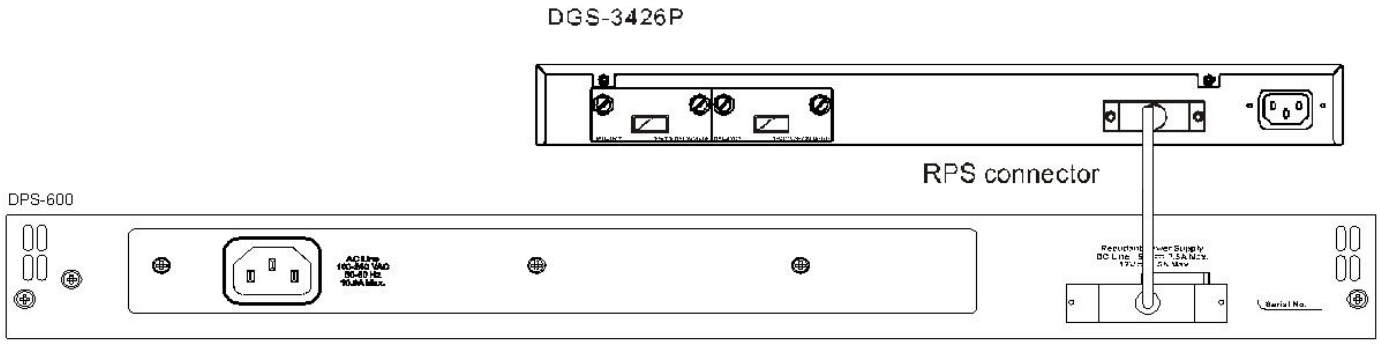


Figure 2- 25. The DGS-3450 with the DPS-500 Redundant External Power Supply

Alternate to the other Switches in the xStack DGS-3400 Switch Series, the DGS-3426P utilizes the DPS-600 as its External Redundant Power Supply. The DPS-600 is the ONLY RPS to be used with the DGS-3426P.



NOTE: See the DPS-500 or DPS-600 documentation for more information.

CAUTION: Do not use the Switch (except DGS-3426P) with any redundant power system other than the DPS-500.

Section 3

Connecting the Switch

Switch to End Node

Switch to Switch

Connecting To Network Backbone or Server

NOTE: All high-performance N-Way 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 routers.

An end node connects to the Switch via a twisted-pair UTP/STP cable. Connect the end node to any of the 1000BASE-T ports of the Switch.

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 Switch

There is a great deal of flexibility on how connections are made using the appropriate cabling.

- Connect a 10BASE-T hub or switch to the Switch via a twisted-pair Category 3, 4 or 5 UTP/STP cable.
- Connect a 100BASE-TX hub or switch to the Switch via a twisted-pair Category 5 UTP/STP cable.
- Connect 1000BASE-T switch to the Switch via a twisted pair Category 5e UTP/STP cable.
- Connect 10G optional module ports at the rear of the device using CX4 or fiber-optic cables
- Connect switch supporting a fiber-optic uplink to the Switch's SFP ports via fiber-optic cabling. See cabling guidelines in Appendix B for more information.

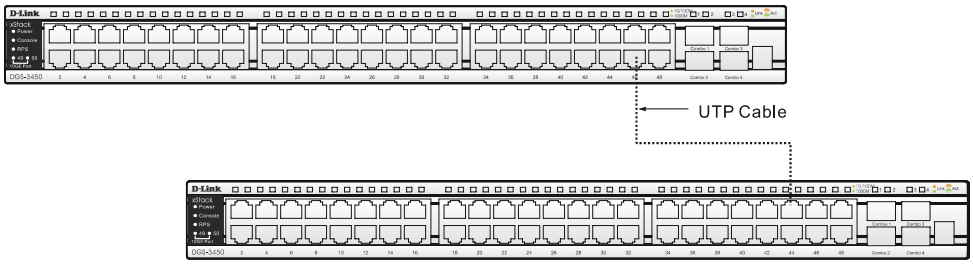


Figure 3- 1. Connect the Switch to a port on a switch with straight or crossover cable

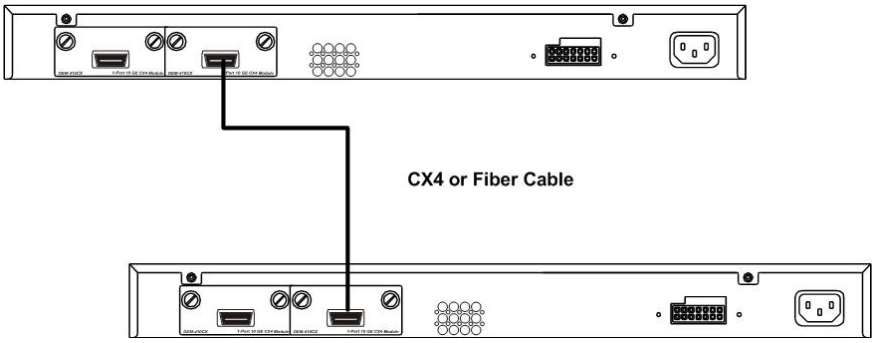


Figure 3- 2. Connect the Switch utilizing the 10G optional modules at the rear of the Switch.

Connecting To Network Backbone or Server

The combo SFP ports and the 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 a 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.

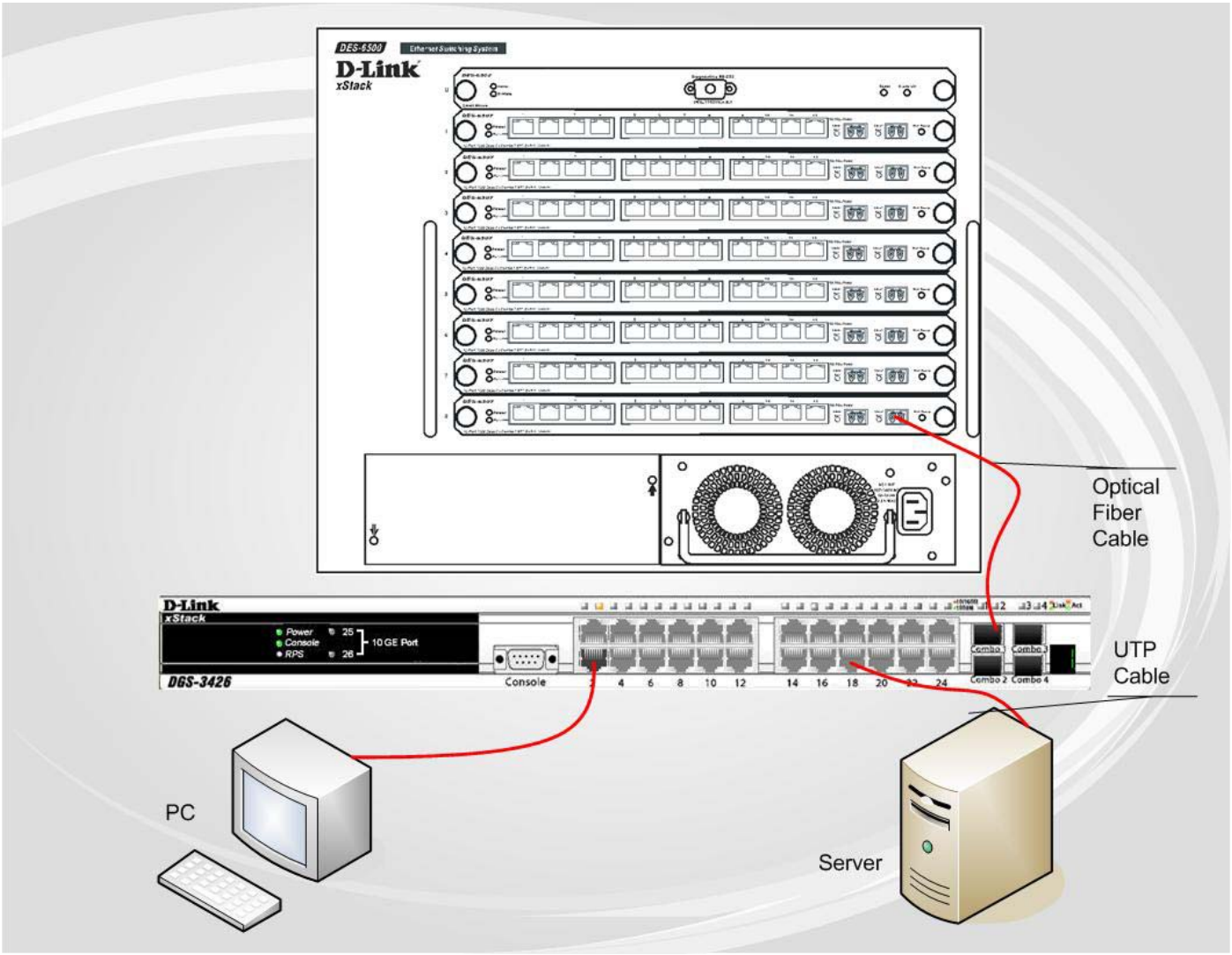


Figure 3- 3. DGS-3400 uplink connection to a server, PC or switch stack.

Section 4

Introduction to Switch Management

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.

1. Web-based Management Interface

After successfully installing the Switch, the user 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).

2. SNMP-Based Management

The Switch can be managed 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.

3. Command Line Console Interface through the Serial Port

The user 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, the following equipment is needed:

- A terminal or a computer with both a serial port and the ability to emulate a terminal.
- A null modem or crossover RS-232 cable with a female DB-9 connector for the console port on the Switch.

To connect a terminal to the console port:

Connect the female connector of the RS-232 cable directly to the console port on the Switch, and tighten the captive retaining screws.

Connect the other end of the cable to a terminal or to the serial connector of a computer running terminal emulation software. Set the terminal emulation software as follows:

- Select the appropriate serial port (**COM port 1** or **COM port 2**).
- Set the data rate to **115200 baud**.
- Set the data format to **8 data bits**, **1 stop bit**, and **no parity**.
- Set **flow control** to **none**.
- Under Properties, select **VT100** for Emulation mode.
- Select **Terminal** keys for **Function**, **Arrow** and **Ctrl** keys. Make sure to use Terminal keys (not Windows keys) are selected.

NOTE: When using HyperTerminal with the Microsoft® Windows® 2000 operating system, ensure that Windows 2000 Service Pack 2 or later is installed. Windows 2000 Service Pack 2 allows use of arrow keys in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

- After you have correctly set up the terminal, plug the power cable into the power receptacle on the back of the Switch. The boot sequence appears in the terminal.
- After the boot sequence completes, the console login screen displays.
- If the user has 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. The administrator must first create user names and passwords. If user accounts have been previously set up, log in and continue to configure the Switch.
- Enter the commands to complete desired tasks. Many commands require administrator-level access privileges. Read the next section for more information on setting up user accounts. See the ***xStack DGS-3400 series CLI Manual*** on the documentation CD for a list of all commands and additional information on using the CLI.
- To end a management session, use the logout command or close the emulator program.

If problems occur in making this connection on a PC, make sure the emulation is set to VT-100. The emulation settings can be configured by clicking on the **File** menu in the HyperTerminal window by 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 the 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.

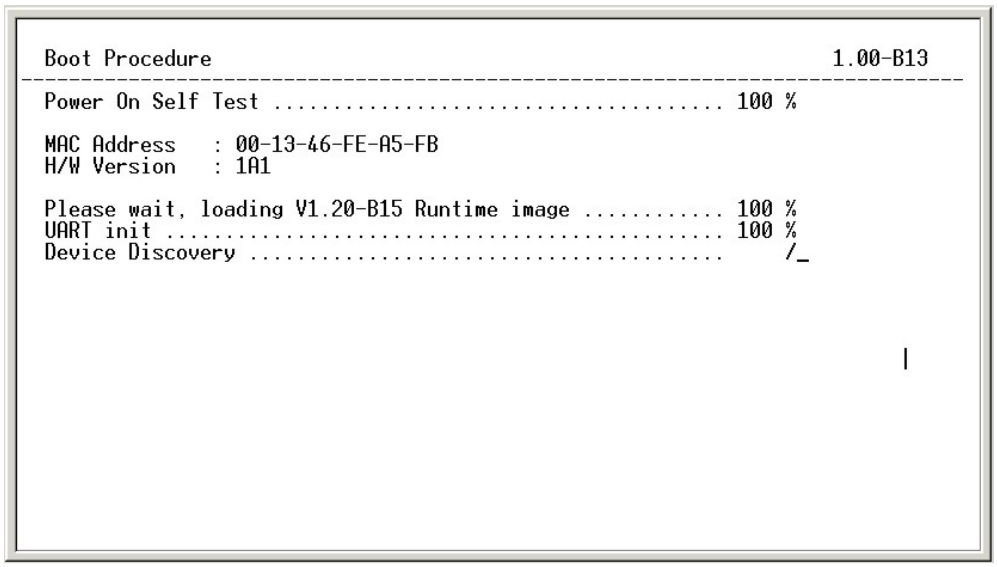


Figure 4- 1. Boot up display in console screen (DGS-3427)

Managing the Switch for the First Time

The Switch supports user-based security that can allow prevention of unauthorized users from accessing the Switch or changing its settings. This section tells how to log onto the Switch via out-if-band console connection.

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

Upon initial connection to the Switch, the login screen appears (see example below).

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.

Figure 4- 2. Initial screen, first time connecting to the Switch

Press Enter in both the Username and Password fields. Then access will be given to enter commands after the command prompt **DGS-3426:4#**, **DGS-3426P:4#, DGS-3427:4#** or **DGS-3450:4#** as shown below:

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

NOTE: The first user automatically gets Administrator level privileges. At least one Admin-level user account must be created for the Switch.

Password Protection

The xStack DGS-3400 Series switches do not have a default user name and password. One of the first tasks when settings up the Switch is to create user accounts. Logging in using a predefined administrator-level user name will give the user privileged access to the Switch's management software.

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

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

1. At the CLI login prompt, enter create account admin followed by the <*user name*> and press the Enter key.
2. The Switch will then prompt the user to provide a password. Type the <*password*> used for the administrator account being created and press the Enter key.
3. Once entered, the Switch will again ask the user to enter the same password again to verify it. Type the same password and press the Enter key.
4. A “Success” response by the Switch will verify the creation of the new administrator.

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".

```
DGS-34xx:4#create account admin newmanager
Command: create account admin newmanager

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

Success.

DGS-34xx:4#
```

NOTICE: CLI configuration commands only modify the running configuration file and are not saved when the Switch is rebooted. To save all configuration changes in non-volatile memory, 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 xStack DGS-3400 series switches support SNMP versions 1, 2c, and 3. The administrator may specify which version of SNMP 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, a group of SNMP managers can be created 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

The Switch in the Management Information Base (MIB) stores management and counter information. 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

An IP Address must be assigned to each switch, 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. The user may 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.

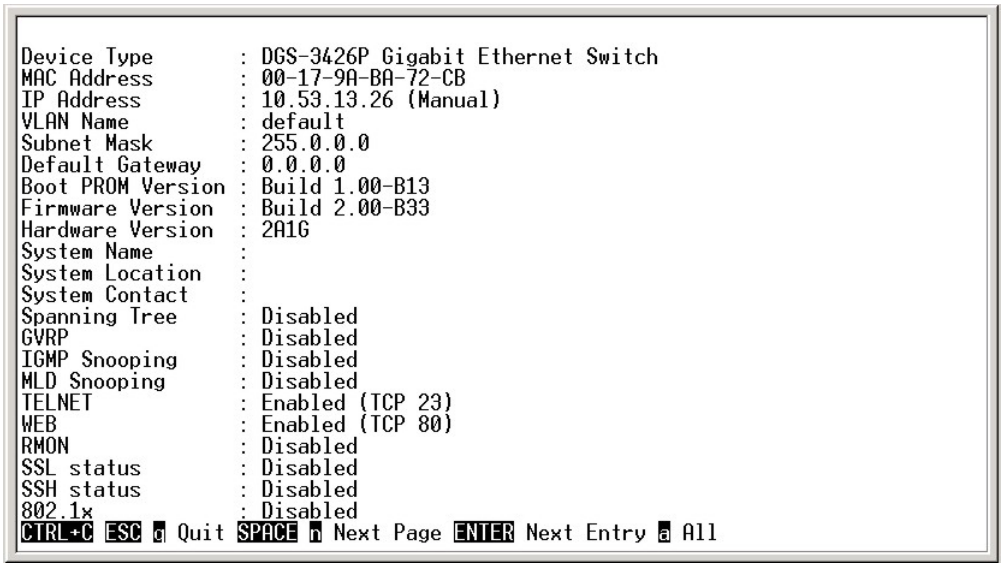


Figure 4- 3. "show switch" command

The Switch's MAC address also appears in **Switch Information** menu of the web-based management interface. The IP address for the Switch must be set before using 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 command:

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, the user 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.

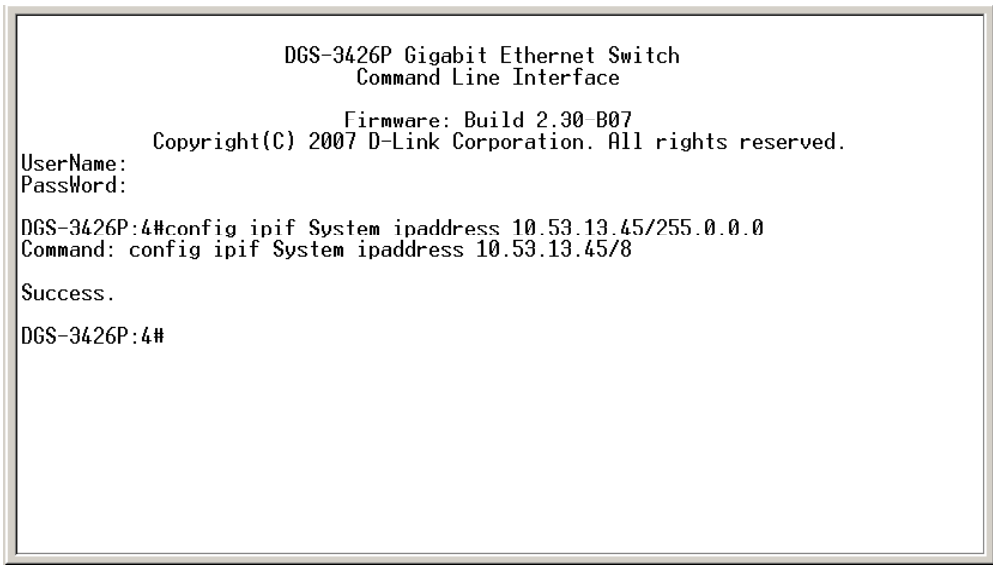


Figure 4- 4. Assigning the Switch an IP Address

In the above example, the Switch was assigned an IP address of 10.53.13.26 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.

NOTE: The DGS-3400 series of switches have the capability to be configured for an IP address of 0.0.0.0, or, in essence, have no IP address. This function maybe used to disable Layer 3 functions of the Switch. When the IP address is set to 0.0.0.0 (invalid IP address), the Switch can only be managed through the console port or SIM. Other management applications such as Telnet, Web-based and SNMP cannot be used to manage the Switch when its IP address is 0.0.0.0.

Section 5

Web-based Switch Configuration

Introduction

All software functions of the xStack DGS-3400 switch series can be managed, configured and monitored via the embedded web-based (HTML) interface. Manage the Switch from remote stations anywhere on the network through a standard browser. 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.

Logging in to the Web Manager

To begin managing the Switch, simply run the browser 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 is 10.90.90.90.

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

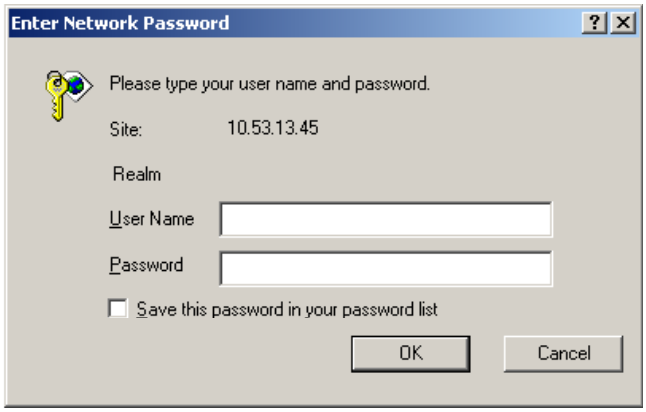


Figure 5- 1. Enter Network Password window

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 the user to view performance statistics, and permits graphical monitoring of the system status.

Areas of the User Interface

The figure below shows the user interface. Three distinct areas divide the user interface, as described in the table.

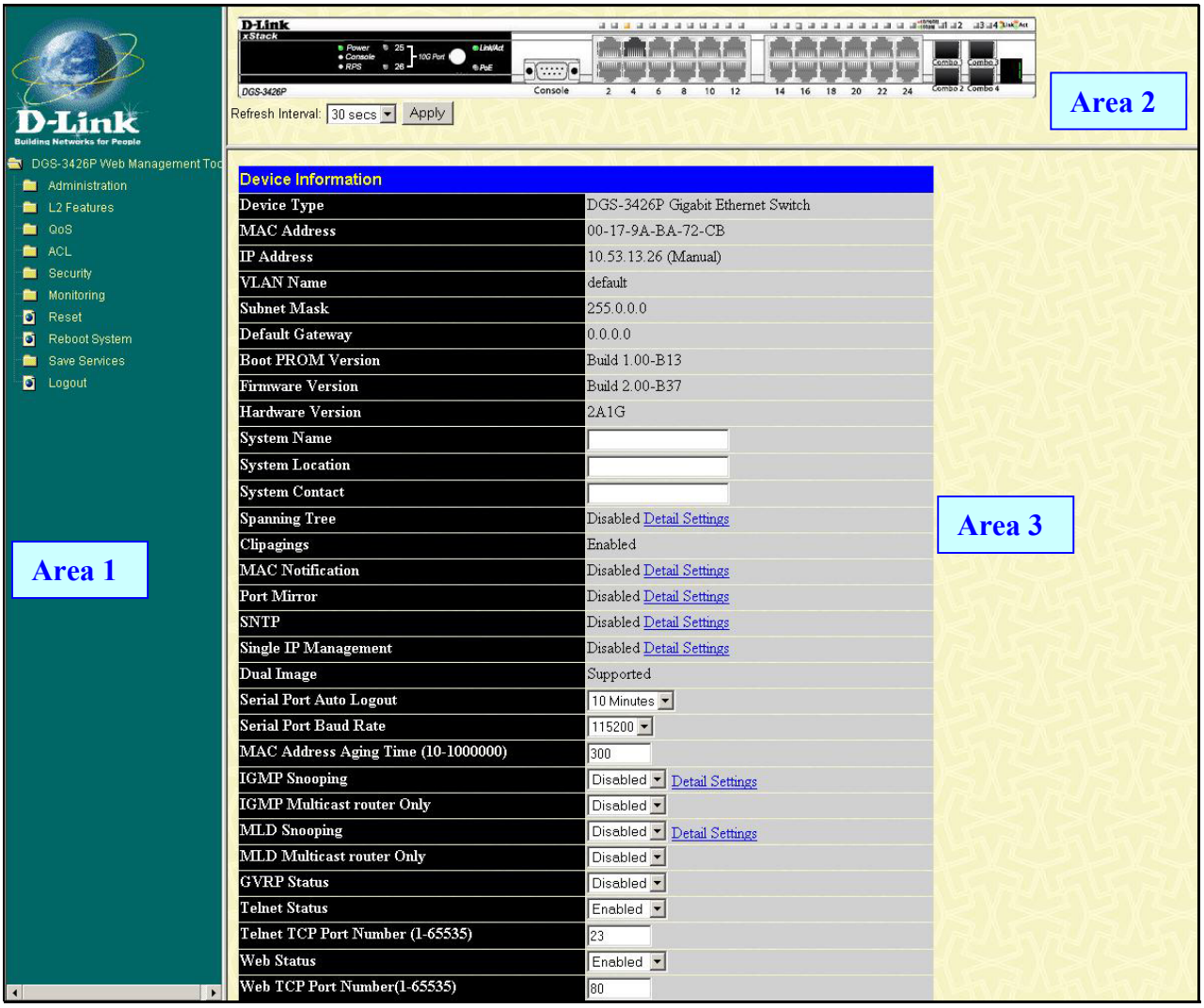


Figure 5- 2. Main Web-Manager Screen

Area	Function
Area 1	Select the menu or window to display. Open folders and click the hyperlinked menu buttons and subfolders contained within them to display menus. 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. Some management functions, including port configuration are accessible here.
Area 3	Presents switch information based on user selection and the entry of configuration data.

Web Pages

When connecting to the management mode of the Switch with a web browser, a login screen is displayed. Enter a user name and password to access the Switch's management mode.

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

Administration – Contains the following menu pages and sub-directories: IP Address, Interface Settings, Stacking, Port Configuration, User Accounts, Port Mirroring, System Log, System Severity Settings, SNTP Settings, MAC Notification Settings, TFTP Services, Multiple Image Services, Ping Test, Safeguard Engine, Static ARP Settings, IPv6 Neighbor, Routing Table, DHCP/BOOTP Relay, DHCP Auto Configuration, SNMP Manager, IP-MAC-Port Binding, PoE (DGS-3426P only), and Single IP Management Settings.

L2 Features – Contains the following menu pages and sub-directories: VLAN, Trunking, IGMP Snooping, MLD Snooping, Spanning Tree and Forwarding & Filtering.

QoS – Contains the following menu pages and sub-directories: Bandwidth Control, QoS Scheduling Mechanism, QoS Output Scheduling, 802.1p Default Priority and 802.1p User Priority.

ACL – Contains the following menu pages and sub-directories: Time Range, Access Profile Table and CPU Interface Filtering.

Security – Contains the following menu pages and sub-directories: Traffic Control, Port Security, 802.1X, Trust Host, Access Authentication Control, Traffic Segmentation, SSL and SSH.

Monitoring – Contains the following menu pages and sub-directories: Device Status, Stacking Information, Module Information, CPU Utilization, Port Utilization, Packets, Errors, Packet Size, Browse Router Port, Browse MLD Router Port, VLAN Status, Port Access Control, MAC Address Table, IGMP Snooping Group, MLD Snooping Group, Switch Logs, Browse ARP Table, Session Table, IP Forwarding Table and Browse Routing Table.

Save Services – Contains the following menu pages and sub-directories: Save Changes, Configure Information and Current Configuration Settings.

Reset, **Reboot System** and **Logout** menu links are displayed in the main directory.

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

Configuring the Switch

DGS-3400 Web Management Tool

IP Address

Interface Settings

Stacking

Port Configuration

User Accounts

Port Mirroring

System Log

System Severity Settings

SNTP Settings

MAC Notification Settings

TFTP Services

Multiple Image Services

Ping Test

Safeguard Engine

Static ARP Settings

IPv6 Neighbor

Routing Table

DHCP/BOOTP Relay

DHCP Auto Configuration

SNMP Manager

IP-MAC-Port Binding

PoE

Single IP Management Settings

Device Information

The **Device Information** window contains the main settings for all major functions for the Switch. It appears automatically when you log on to the Switch. To return to the **Device Information** window after viewing other windows, click the **DGS-3400 Web Management Tool** folder. The Device Information 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. In addition, this screen displays the status of functions on the Switch to quickly assess their current global status. Some Functions are hyper-linked for easy access from the Device Information window.

Many miscellaneous functions are enabled and disabled in the Device Information menu.

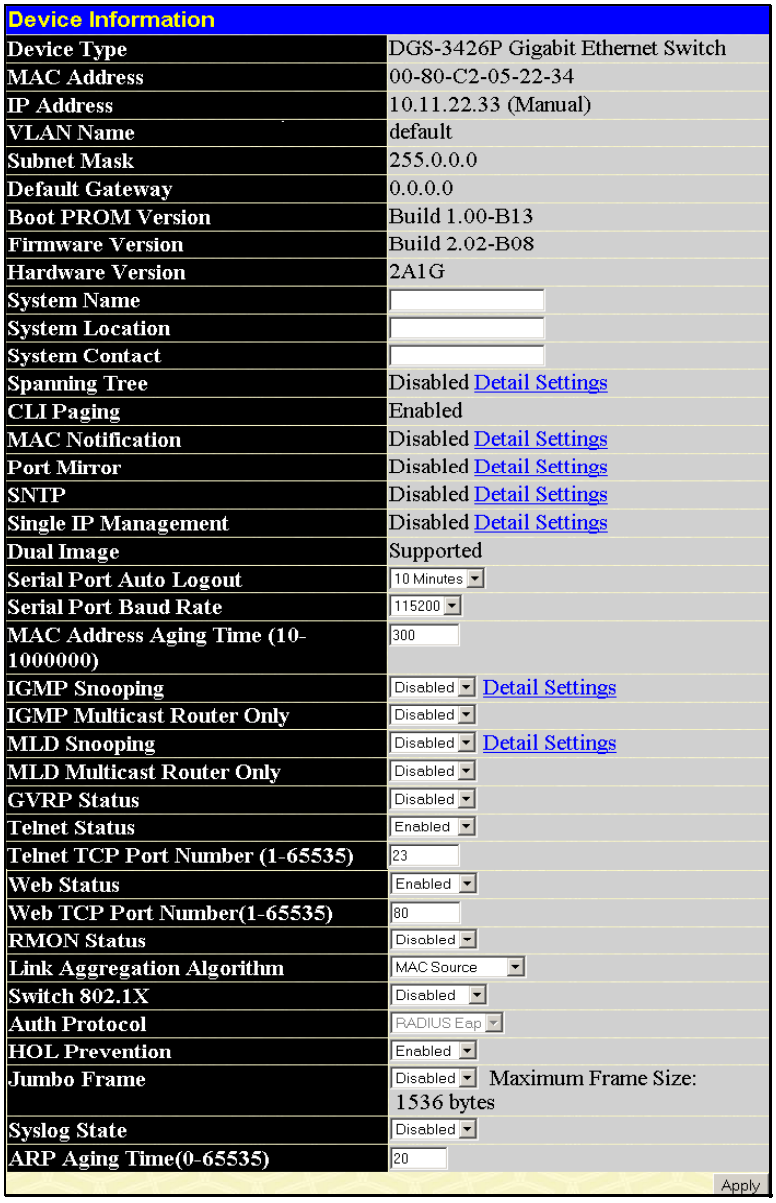


Figure 6- 1. Device Information window

Device Information menu configurable parameters include those described in the table below.

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	This field specifies the baud rate for the serial port on the Switch. The default setting is 115200.
MAC Address Aging Time	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 Time 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 the user to specify use of a multicast router only (see below). To configure IGMP Snooping for individual VLANs, use the IGMP Snooping window under the IGMP Snooping folder.

IGMP Multicast Router Only	This field specifies that the Switch should only forward all multicast traffic to a multicast-enabled router, if enabled. Otherwise, the Switch will forward all multicast traffic to any IP router. The default is *Disabled*.
MLD Snooping	To enable system-wide MLD Snooping capability select *Enabled*. MLD snooping is *Disabled* by default. Enabling MLD snooping allows you to specify use of a multicast router only (see below). To configure MLD Snooping for individual VLANs, use the MLD Snooping window under the MLD Snooping folder.
MLD Multicast Router Only	This field specifies that the Switch should only forward all multicast traffic to a multicast-enabled router, if enabled. Otherwise, the Switch will forward all multicast traffic to any IP router. The default is *Disabled*.
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 TCP port number used for Telnet management of the Switch. 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.
Web TCP Port Number (1-65535)	The TCP port number used for Web-based management of the Switch. The "well-known" TCP port for the Telnet protocol is *80*.
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	MAC Address may enable by port or the Switch's 802.1X function; the default is *Disabled*. This field must be enabled to view and configure certain windows for 802.1X. More information regarding 802.1X, its functions and implementation can be found later in this section, under the Port Access Entity folder. Port-Based 802.1X specifies that ports configured for 802.1X are initialized based on the port number only and are subject to any authorization parameters configured. MAC-based Authorization specifies that ports configured for 802.1X are initialized based on the port number and the MAC address of the computer being authorized and are then subject to any authorization parameters configured.
Auth Protocol	The user may use the pull-down menu to choose between *RADIUS EAP* and *Local* for the 802.1X authentication protocol on the Switch. The default setting is *RADIUS EAP*.
HOL Prevention	If this option is enabled it prevents the forwarding of data to a port that is blocked. Traffic that would normally be sent to the buffer memory of the Switch's TX queue is dropped so that memory usage is conserved and performance across all ports remains high.
Jumbo Frame	This field will enable or disable the Jumbo Frame function on the Switch. The default is Disabled. Max. Jumbo frame size = 9216 bytes if this is enabled.
Syslog State	The user may globally enable or disable the Syslog function here by using the pull-down menu. The default is *Disabled*.
ARP Aging time	The user may set the ARP Aging Time here by entering a time between 0 and 65535 minutes. The default setting is 20 minutes.

Click **Apply** to implement changes made.

IPv6

The xStack DGS-3400 has the capability to support the following:

- IPv6 unicast, multicast and anycast addresses
- Allow for IPv6 packet forwarding
- IPv6 fragmentation and re-assembly
- Processing of IPv6 packet and extension headers
- Static IPv6 route configuration
- IPv6 Neighbor Discovery
- Link-Layer Address resolution, Neighbor Unreachability Detection and Duplicate Address Detection over broadcast mediums (ex: Ethernet)
- Send Router Advertisement
- ICMPv6 functionality

The following sections will briefly explain IPv6, its functionality and how IPv6 is implemented on this Switch.

Overview

IP version 6 is the logical successor to IP version 4. It was known that IPv4 could not support the amount of addresses that would eventually be needed for not only each person, but each device that would require an IP address, and therefore a system with a larger pool of IP addresses was required. IPv6 has addressed that issue, along with other issues that enhance routing over the network, provide better security and improve Quality of Service for Internet users. Some of the improvements made were:

Expanding the Capabilites for IP Addressing – IPv6 has increased the size of the IP address from 32 bits to 128 bits. As a result, the addressing hierarchy has been greatly expanded, more nodes now have the capability of having a unique IP address and the method of assigning an IP address to an interface has become cleaner and quicker. Unicast and multicast addresses still exist but in a purer form and multicast addresses now have a scope field which increases the scalability of multicast routing. Also, an anycast address has been added, which will send packets to the closest node which is a part of a group of nodes, thereby eliminating a specified device for a particular group.

Simplifying the Packet Header – The IPv6 packet header has been simplified from IPv4 as some headers have been modified or dropped altogether, which improves processing speed and cost. The IPv6 header now has a fixed length of 40 bytes consisting of an 8-byte header and two 16-byte IP addresses (source and destination).

Extensions and Options Enhancement – Packet header option fields encoding has been enhanced to allow for proficient forwarding of packets due to lesser restrictions on packet option length and encoding method. This enhancement will also allow new option fields to be integrated into the IPv6 system without hassles and limitations. These optional headers are placed between the header and the payload of a packet, if they are necessary at all.

Authentication and Privacy Extension Support – New authentication capabilities use extensions for data integrity and data confidentiality for IPv6.

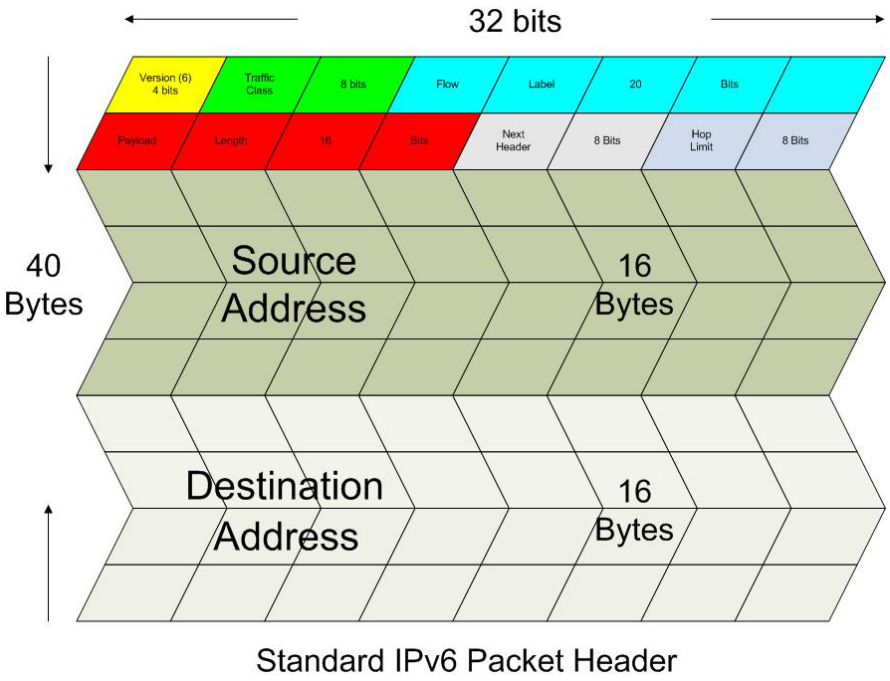
Flow Labeling – This new capability allows packets to be streamlined into certain traffic “flows” if labeled by the sender. In this way, services such as “real time services or non-default quality of service can receive special attention for improved flow quality.

Packet Format

As in IPv4, the IPv6 packet consists of the packet header and the payload, but the difference occurs in the packet header which has been amended and improved for better packet flow and processing. The following will outline and detail the IPv6 enhancements and parts of the IPv6 packet, with special attention to the packet header.

IPv6 Header

The IPv6 packet header has been modified and simplified from IPv4. The header length, identification, flags, fragment offset and header checksum have all been removed in the IPv6 header due to lack of necessity or improvement to a better function of the header. The minimum header length is now 20 bytes but may be increased to as much as 60 bytes, using 4-byte increment extensions. The following picture is an example of an IPv6 packet header.



Standard IPv6 Packet Header

Eight fields make up the basic IPv6 packet header:

Version – This 4-bit field defines the packet version, which is IPv6 and is defined as the number 6.

Traffic Class – This 1-byte field replaces the Type of Service field used in IPv4 and is used to process real-time data and other data requiring special packet management. This field defines the Class of Service priority of an IPv6 packet.

Flow Label – This 20-bit field is used to facilitate the handling of real-time traffic. Hosts sending data can place a flow label into this field to identify a sequence of packets that have an identical set of options. In this way, router can process these packets more efficiently once the flow class has been identified and the rest of the packet header no longer needs to be fully processed, just the flow label and the source address. All flow label packets must have identical source and destination addresses.

Payload Length – Known as the datagram length in IPv4, this 16-bit field specifies the length of the IPv6 data carried after the header of the packet. Extension headers are considered part of the payload and are included in the length specified here.

Next Header – This 8-bit field is used to identify the header immediately following the IPv6 header. When this field is set after the hop by-hop header, it defines the extension header that will appear after the destination address. Each extension header must be preceded by a Next Header field. Integers used to define extension headers in the next Header field use the same values as IPv4 (ex: 6=TCP, 17=UDP, etc.).

Hop Limit - Similar to the TTL field in IPv4, this 8-bit field defines the number of hops remaining after the packet has been processed by a node, instead of the number of seconds left to live as on an IPv4 network. This field will decrement by one after every node it passes and the packet will be discarded once this field reaches zero.

Source Address – This 16-byte field defines the IPv6 address of the source node sending the packet.

Destination Address – This 16-byte field defines the IPv6 address of the destination node receiving the packet. This may or may not be the final destination node of this packet, depending on the routing header, if present.

Extension Headers

Extension headers are used to identify optional parameters regarding IPv6 packets such as routing, fragmentation of packets or authentication parameters. The types of extension headers supported are Hop-by-Hop, Routing, Fragment, Destination Options, Authentication and Encapsulating Security Payload. These extension headers are placed between the IPv6 packet header and the payload and are linked together by the aforementioned Next Header, as shown below.

IPv6 header **Next Header = TCP**	**TCP header + data**

IPv6 header **Next Header = Routing**	**Routing Header** **Next Header = TCP**	**TCP header + data**

IPv6 header **Next Header = Destination Options**	**Destination Options Header** **Next Header = Routing**	**Routing Header** **Next Header = TCP**	**TCP header + data**

Each header has a specific place in the header chain and must follow the following order:

- IPv6 Header
- Hop-By-Hop Header (Must follow the IPv6 header)
- Destination Options
- Routing Header
- Fragment Header
- Authentication Header
- Encapsulating Security Payload Header
- Destination Options Header
- Upper Layer Header

There may be zero, one or more extension headers in the IPv6 header, they must be processed in order and they are to be in increments of 8 octets in the IPv6 packet. Nodes that do not recognize the field of the extension header will discard the packet and send a relevant ICMPv6 message back to the source.

Packet Fragmentation

At times, packets are sent out to a destination that exceed the size of the Path MTU, so the source node is required to split these packets into fragments in individual packets which will be rebuilt when it reaches its final destination. Each of the packets that will be fragmented is given an Identification value, by the source node. It is essential that each of these Identification values is different than any other fragmented packet recently sent that include the same source and destination address. The original packet is divided into two parts, a fragmentable part and an unfragmentable part. The unfragemntable part of the packet consists of the IPv6 header and any extension headers present, up to the routing extension header. The fragmentable part has the payload plus any extension headers that must be processed by the final destination node. This part will be divided into multiple packets that are of a size that can be accepted by the Path MTU. The IPv6 header is then included with this fragmented part and sent to its destination. Once all parts of the fragmented packet reach its destination, they are reassembled using the Fragment Identification value, provided that the source and destination addresses are identical.

Address Format

To address the problem of finding a larger pool of IP addresses for IPv6, the size and format of the IPv4 format needed to be changed. Quadrupling the size of the address, from 32 bits to 128 bits, and encoding addresses using the hexadecimal form were used to solve the problem. In IPv4, the format of the address looked like xxx.xxx.xxx.xxx, where the x's represent integers from 0-9 (ex. 136.145.225.121). Now in IPv6, the format of the address resembles xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx where a set of xxxx represents a 16-bit hexadecimal value (ex. 2D83:0C76:3140:0000:0000:020C:417A:3214). Although this address

looks long and cumbersome, there are some compression rules that will shorten the format of the IPv6 address to make it more compatible to the user.

One such compression rule that is used is to remove leading zeros from any 16-bit hexadecimal value. This is only for zeros that begin the value, not for zeros within the value or ones that are ending the value. Therefore, if we take the previous example IPv6 address and use the compression rules, our IPv6 address would look like this:

2D83:0C76:3140:**0000:0000:020C**:417A:3214 → 2D83:C76:3140:**0:0:20C**:417A:3214

The second compression method is to change a string of zero bits into two colons. At times, there may be strings of empty values in the IPv6 address that are unused for this address, but they are necessary for the format of other IPv6 addresses with alternate purposes. To compress these zero strings, the format "**::"** is used to represent multiple zero fields in the address. This double colon can only be used once in the IPv6 address because when a computer finds a colon, it will expand this field with as many zeros as is necessary to reach the 128-bit address size. If two strings of zeros are present, separated by another non-zero field, a zero must be used to represent one of the two zero fields. So, if we reduce our example using this compression, it would look like this:

2D83:0C76:3140**:0000:0000:020C:**417A:3214 → 2D83:C76:3140**:0:0:20C:**417A:3214 →2D83:C76:3140**::20C:**417A:3214

When IPv4 and IPv6 nodes are mixed in a network, the IPv6 notation overcomes the difficulty of using an IPv4 address by converting it to the IPv6 format using zeros at the beginning of the IPv4 address. For example, an IP address of 192.168.1.1 is represented in IPv6 format x:x:x:x:d.d.d.d where the x's are a string of zeros and the d's represent the normal IPv4 address. (ex. 0:0:0:0:192.168.1.1 or condensed ::192.168.1.1 or hex form ::C0A8:1:1).

Types

IPv6 addresses are classified into three main categories, unicast, multicast and anycast.

Unicast – This address represents a single interface on an IPv6 node. Any packet with a unicast address as its destination address will only be sent to that specific node. Two types of unicast addresses are mainly used for IPv6.

- *Link-Local* – Defined by the IPv6 address prefix FE80::/10, link-local addresses allow for communication to occur between devices on a local link. These addresses are used in neighbor discovery and stateless autoconfiguration.
- *Global Aggregateable* - Defined using a global routing prefix in the range of 2000::/3 to E000::/3, global addresses are aggregated using these routing prefixes to produce unique IPv6 addresses, which will limit global routing table entries. The MAC address of the device is used to produce this address in this form:

  Global Routing Prefix + Site Level Aggregator + MAC address (first 3 bits) + FFFE + MAC Address (last 3 bits)

  So if your MAC address looks like 00-0C-6E-6B-EB-0C, your IPv6 address may resemble 2000::C:6E:6B:FF:FE:EB:0C/64.

Multicast – Like IPv4, multicast addresses are used to send packets to multiple destinations on a network. These interfaces must be a part of the multicast group. IPv6 multicast prefixes begin with the prefix FF00::/8. FF represents the binary 1111 1111 which identifies a multicast address. The first zero, which is a 4-bit integer, represents the lifetime of the packet. An entry of zero in this field represents a permanent multicast address and an entry of one represents a temporary multicast address. The second zero, which is also a 4-bit integer, defines the scope of the multicast address. This scope defines to what places the multicast address is valid. For example, a value of 1 defines the node, 2 defines the link, 5 defines a site, 8 defines a organization and so on. Not all integers are in use for the scope field. An example of this would be FF02 where the 2 represents a multicast packet going to all the nodes on a local link.

Anycast – The anycast address will send messages to the nearest node of a particular group. This address is assigned to multiple interfaces in the group but only the node with the closest proximity will receive the message. These anycast addresses are allocated from the unicast address space and therefore have no real defined prefix to distinguish it from other IPv6 addresses. The main purpose of the anycast address is to identify a set of routers owned by an organization providing Internet service. It could also be used to identify a set of routers connected to a particular subnet or permitting entrance to a specific routing domain.

Two other special types of addresses exist in IPv6. The **unspecified address** has a value of 0:0:0:0:0:0:0:0 which is comparable to the 0.0.0.0 address in IPv4. This address is used to indicate the lack of a valid IP address on a node and may be used by a device when booting and requesting address configuration notification. In its IPv6 condensed form, it appears as "**::**" and should not be statically or dynamically assigned to an interface, nor should it be the destination address of an IPv6 packet, or located within the routing header.

The second type of special address is the **loopback address** which is represented by 0:0:0:0:0:0:0:1, or ::1 in its compressed form. It is akin to the 127.0.0.1 address in IPv4 and is used in troubleshooting and testing IP stacks. This address, like the unspecified address, and should not be statically or dynamically assigned to an interface.

ICMPv6

Network professionals are already very familiar with ICMP for IPv4, which is an essential tool in the IPv4 network, relaying messages about network problems and the general condition of the network. ICMPv6 is the successor to the IPv4 version and performs many of the same basic functions as its precursor, yet is not compatible with ICMPv4. ICMPv6 has made improvements over its forerunner, with such enhancements as managing multicast group memberships and allowing for neighbor discovery by resolving link-layer addresses attached to the same link and identifying changes in those addresses. ICMP can also discover routers, determine which neighbors can be reached and map IP addresses to MAC addresses within the network. ICMPv6 is a vital part of the IPv6 network and must be implemented on every IPv6 node for operations to function normally.

Two kinds of ICMP messages are apparent on the IPv6 network:

Error Messages – ICMP error messages are sent out on the network when packet sizes exceed the path MTU (Maximum Transfer Unit), when the hop count of the IPv6 packet has been surpassed, when messages cannot reach their intended destination and when there are parameter problems within the IPv6 packet.

Informational Messages – ICMP informational messages send out packets describing current network information valuable to devices on the network. A common and useful ICMPv6 informational message is the ping program use to discover the availability a device, by using a ping request and reply format. Other informational messages include Path MTU discovery, which is used to determine the maximum size of data packets that can be allowed to be transferred, and Neighbor Discovery messages, which discover routers that can forward packets on the network. Neighbor discovery will be discussed further in the next section.

Neighbor Discovery

Neighbor discovery is a new feature incorporated in IPv6. In IPv4, no means were available to tell if a neighbor could be reached. Now, combining ICMP messages and ARP, neighbors can be detected and their layer 2 addresses (MAC Address) can be identified. This feature can also discover neighboring routers that can forward packets and keep track of the reachability of routers, as well as if changes occur within link-layer addresses of nodes on the network or identical unicast addresses are present on the local link.

The functionality of the Neighbor Discovery feature is based on ICMPv6 packets, Neighbor Solicitation and Router Advertisement messages circulating on the network. When a node wishes to determine link layer addresses of other nodes on the same link, it produces a Neighbor Solicitation message to be circulated on the local link. When received by a neighbor, this neighbor will produce Router Advertisements immediately to be returned. These Router Advertisements will contain a multicast address as the destination address and have an ICMP type of 134 (the specified number for Router Advertisements), as well as having the link-layer address of the node sending the advertisement. Router Advertisement messages may be periodic, specified in the advertisement by having the all-nodes multicast address FF02::1, or sent out as a result of receiving a Neighbor Solicitation message, specified in the advertisement by having the address of the interface that first sent the solicitation message. Once confirmation of the Neighbor has been reached, packets can now be exchanged on the link.

Neighbor Unreachability Detection

At times on the network, problems occur in reaching the Neighbor node or getting a response from the Neighbor. A neighbor is considered reachable when it has received and processed packets sent to it, and in return sends a packet back notifying a affirmative response. This response may come in the form of an indication from an upper-layer protocol, like TCP, noting that progress is being made, or in response from a Neighbor Solicitation message in the form of a Router Advertisement message. If responses are not received from the node, it is considered unreachable and a Destination Unreachable message is received in the form of an ICMP packet. This Destination Unreachable ICMP packet will contain the reason for the fault, located in the code field of the ICMP header. Five possible reasons for the failure can be stated:

1. There is no route or destination (Code 0).
2. Communication has been administratively prohibited, such as a firewall or filter (Code 1)
3. Beyond the scope of the source address, when the multicast scope of the source address is smaller than the scope of the destination address (Code 2)
4. The address is unreachable (Code 3)
5. The port is unreachable (Code 4)

Duplicate Address Detection (DAD)

DAD messages are used to specify that there is more than one node on a local link possessing the same IP address. IPv6 addresses are only leased for a defined period of time. When that time expires, the address will become invalid and another address must be addressed to the node. To ensure that this new address is unique on the local link, a node runs a DAD process to determine the uniqueness of the new address. This is done through the use of a Neighbor Solicitation message containing a Tentative address. This message will detect if another node on the local link has this Tentative address. If the Tentative address is found on another node, that node will send out a Neighbor Advertisement message, the process will be terminated, and manual configuration will be necessary. If no answer is forthcoming regarding this Neighbor Solicitation message containing the tentative address, the address is allotted to the node and connectivity is established.

Assigning IP Addresses

For IPv4 addresses, users may only assign one address per interface and only one address may be used on a particular VLAN. Yet, IPv6 addresses are different. All IPv6 interfaces on the switch must have at least one IPv6 link-local unicast address, if the user is employing the IPv6 addressing scheme. Multiple IPv6 addresses may be configured for IPv6 interfaces, regardless of type, whether it is unicast, multicast or anycast. The scope of the address has some bearing on the assigning multiple addresses to a single interface as well. If multiple physical interfaces are considered as one interface on the Internet layer, multiple unicast addresses may be alloted to multiple physical interfaces, which would be beneficial for load sharing on these interfaces. This is dependent on these unicast addresses having a scope smaller than the link-local address, if these unicast addresses are not the source or destination address for IPv6 packets to or from address that are not IPv6 neighbors of the interface in question.

IP Interface Setup

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 6- 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 6- 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.

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 *xStack DGS-3400 Series CLI 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 Administration folder.

To configure the Switch's IPv4 address:

Open the **Administration** 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.

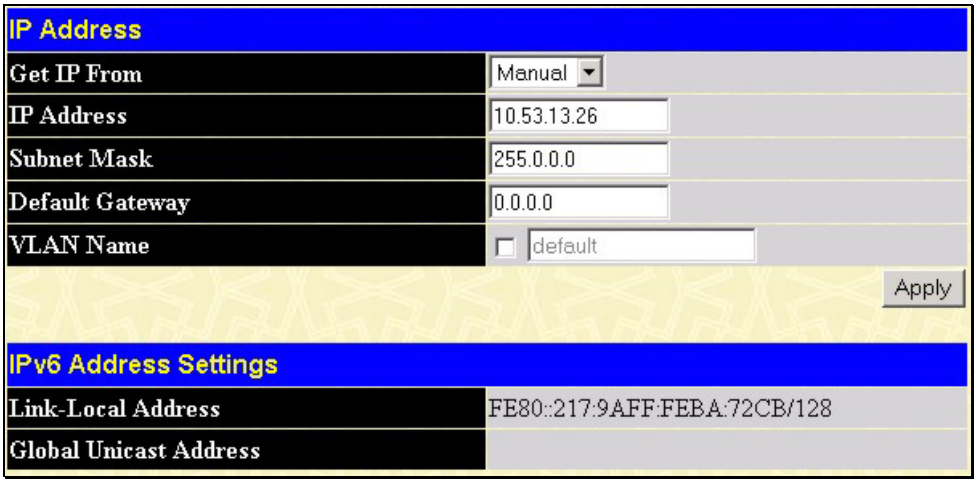


Figure 6- 2. IP Address Settings window

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 accessing the Switch from a different subnet from the one it is installed on, enter the IP address of the **Default Gateway**. If managing the Switch from the subnet on which it is installed, the user may leave the default address (0.0.0.0) in this field.
4. If the Switch has no previously configured VLANs, the user can use the *default* **VLAN Name**. The *default VLAN* contains all of the Switch ports as members. If the Switch has previously configured VLANs, the user 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 the method the Switch assigns 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 gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.
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 implement changes made.

This window also contains the current IPv6 setup on the Switch. Configuring IPv6 interfaces can be done in under the **Interface Settings** heading, by clicking the link **IPv6 Interface Settings**, which will be discussed in the next section.

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. The default Switch IP address can be changed to meet the specification of your networking address scheme.

The IP address for the Switch must be set before the Web-based manager can manage the switch. 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, the user 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.

Successful entry of the command will produce a "**Success"** message**,** indicating that the command execution was correctly. The user may now utilize this address to configure or manage the Switch through Telnet, the Command Line Interface (CLI) or the Web-based management (GUI).

Interface Settings

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 xStack DGS-3400 Series CLI Manual or return to Section 4 of this manual for more information. To change IP settings using the web manager users must access the IP Address menu located in the Administration folder. Open the **Administration** folder and click the **Interface Settings** menu link. The web manager contains two folders for which to setup IP interfaces on the switch, one for IPv4 addresses, named **IPv4 Interface Settings**, and one for IPv6 addresses, named **IPv6 Interface Settings**.

IPv4 Interface Settings

After clicking the **IPv4 Interface Settings** link, the following window will be displayed for the user to view.

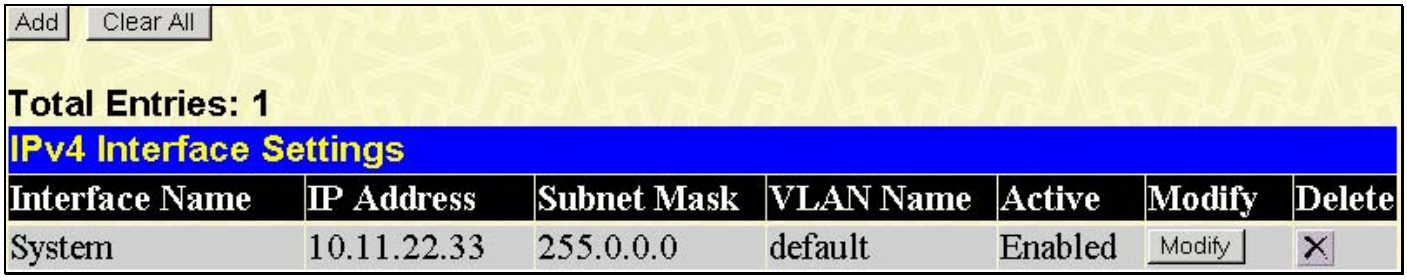


Figure 6- 3. IPv4 Interface Settings window

To manually assign the Switch's IPv4 address and its related configurations, click the **Add** button, revealing the following window to configure.

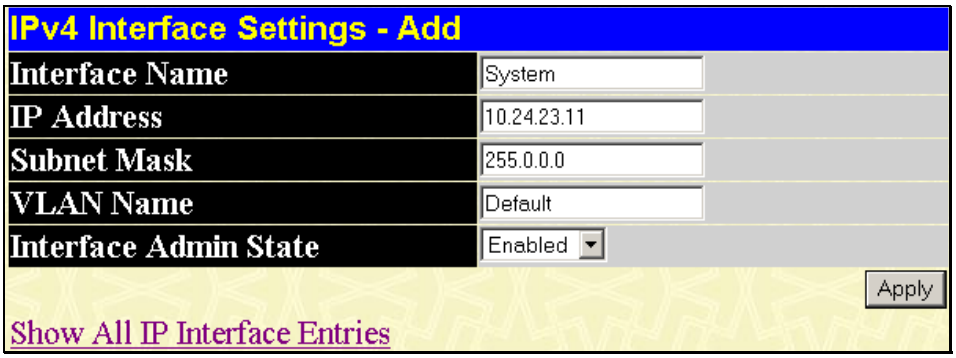


Figure 6- 4. IPv4 Interface Settings - Add

To modify an existing Interface, click that interface's hyperlinked **Interface Name**, which will produce this window:

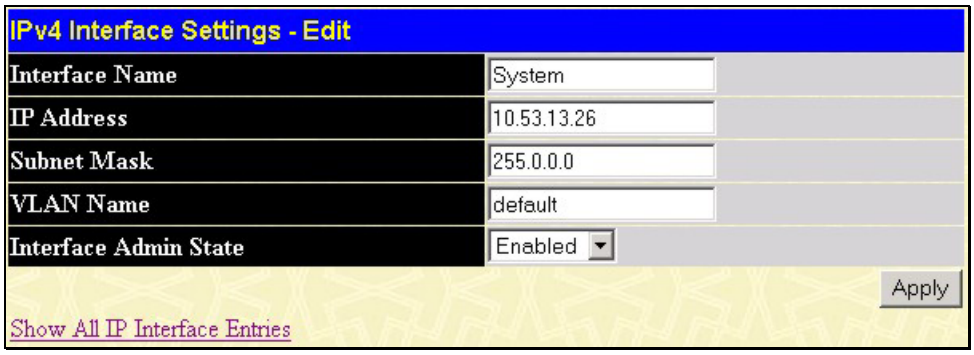


Figure 6- 5. IPv4 Interface Settings - Modify

Enter a name for the new interface to be added in the **Interface Name** field (if 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 **Interface Admin State** pull-down menu to *Enabled* and click **Apply** to enter to make the IP interface effective. To view entries in the **IP Interface Settings**, click the Show All IP Interface Entries hyperlink. Use the **Save Changes** dialog box from the **Save Services** folder to enter the changes into NV-RAM.

The following fields can be set or modified:

Parameter	Description
Interface Name	This field displays the name for the IP interface or it is used to add a new interface created by the user. The default IP interface is named “System”.
IP Address	This field allows the entry of an IPv4 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 states the VLAN Name directly associated with this interface.
Interface Admin. State	Use the pull-down menu to enable or disable configuration on this interface.

Click **Apply** to implement changes made.

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.

IPv6 Interface Settings

The following window is used to setup IPv6 interfaces and addresses for the switch. To access this window, open the **Interface Settings** link and click the **IPv6 Interface Settings** link, which will display the following window to configure.

Figure 6- 6. IPv6 Interface Settings window

To add a new IPv6 interface, click the **Add** button, which will display the following window.

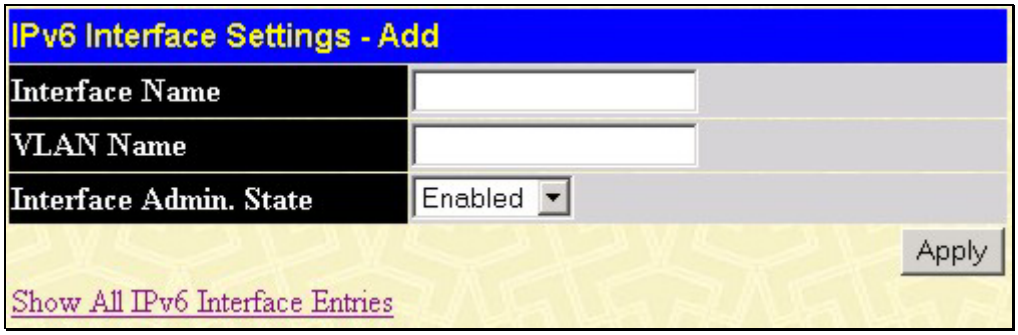


Figure 6- 7. IPv6 Interface Settings – Add

To add an Interface, enter an **Interface Name** in the field provided, along with a corresponding **VLAN Name**, set the **Interface Admin. State** to *Enabled* and click **Apply**. Newly created interfaces will appear in the **IPv6 Interface Settings** window, as shown in Figure 6-4 (Triton).

To change the settings for a configured Interface, click the corresponding **Modify** button, which will display the following window for the user to configure.

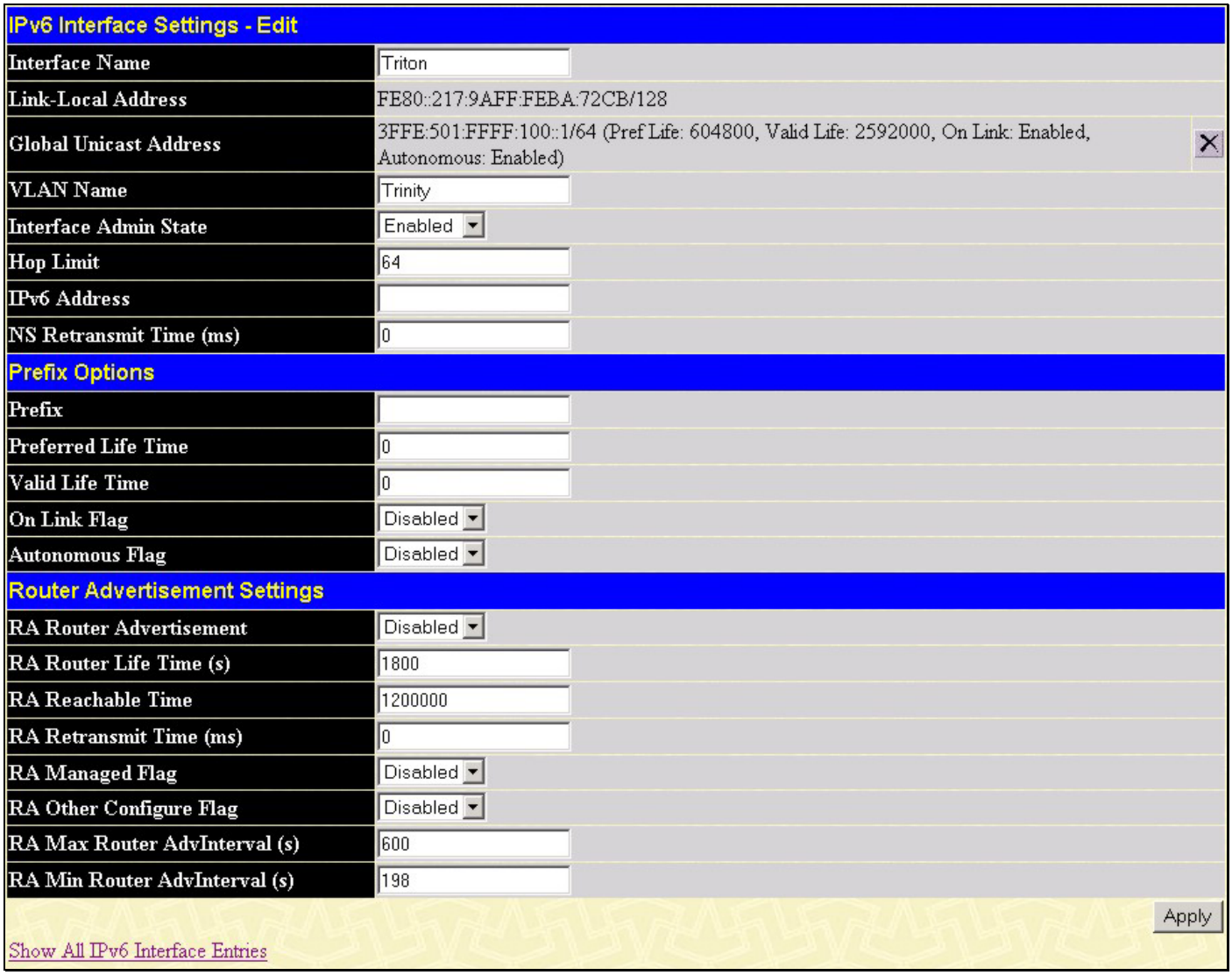


Figure 6- 8. IPv6 Interface Settings – Edit

The following fields may be viewed or modified. Click **Apply** to set the changes made.

Parameter	Description
Interface Name	This field displays the name for the IP interface or it is used to add a new interface or change an existing interface name. The default IP interface is named “System”. The Interface field is used for addresses on the link-local network. It is recommended that the user enter the specific interface for a link-local IPv6 address. For Global Ipv6 addresses, this field may be omitted.
Link-local Address	This field displays the IPv6 address created automatically by the Switch, based on the MAC Address of the Switch. This is a site local address used only for local routing.
Global Unicast Address	This field is the unicast address that will be used by the Switch for packets coming from outside the site-local address, or the public IPv6 address, when connected directly to the Internet.
VLAN Name	This field states the VLAN Name directly associated with this interface.
Interface Admin State	Use the pull-down menu to enable or disable configuration on this interface.
Hop Limit	This field sets the number of nodes that this Router Advertisement packet will pass before being dropped. This number is set to depreciate by one after every node it reaches and will be dropped once the Hop Limit reaches 0. The user may set the Hop Limit between 1 and 255 with a default value of 64.

IPv6 Address	Use this field to set a Global Unicast Address for the Switch. This address will be used to access the network outside of the local link.
NS Retransmit Time	Use this field to set the interval, in seconds that this Switch will produce Neighbor Solicitation packets to be sent out over the local network. This is used to discover IPv6 neighbors on the local link. The user may select a time between 0 and 65535 milliseconds. Very fast intervals, represented by a low number, are not recommended for this field.
Prefix Options	
Prefix	Use this field to set a prefix for Global Unicast IPv6 addresses to be assigned to other nodes on the link-local network. This prefix is carried in the Router Advertisement message to be shared on the link-local network. The user must first have a Global Unicast Address set for the Switch.
Preferred Life Time	This field states the time that this prefix is advertised as being preferred on the link local network, when using stateless address configuration. The user may configure a time between 0 and 4294967295 milliseconds, with a default setting of 604800 milliseconds.
Valid Life Time	This field states the time that this prefix is advertised as valid on the link local network, when using stateless address configuration. The user may configure a time between 0 and 4294967295 milliseconds.
On Link Flag	Setting this field to *Enabled* will denote, within the IPv6 packet, that the IPv6 prefix configured here is assigned to this link-local network. Once traffic has been successfully sent to these nodes with this specific IPv6 prefix, the nodes will be considered reachable on the link-local network.
Autonomous Flag	Setting this field to *Enabled* will denote that this prefix may be used to autoconfigure IPv6 addresses on the link-local network.
Router Advertisement Settings	
RA Router Advertisement	Use this pull-down menu to enable or disable the switch as being capable of accepting solicitation from a neighbor, and thus becoming an IPv6 neighbor. Once enabled, this Switch is now capable of producing Router Advertisement messages to be returned to querying neighbors.
RA Router Lifetime	This time represents the validity of this interface to be the default router for the link-local network. A value of 0 represents that this Switch should not be recognized as the default router for this link-local network. The user may set a time between 0 and 9000 seconds with a default setting of 1800 seconds.
RA Reachable Time	This field will set the time that remote IPv6 nodes are considered reachable. In essence, this is the Neighbor Unreachability Detection field once confirmation of the access to this node has been made. The user may set a time between 0 and 36000000 milliseconds with a default setting of 1200000 milliseconds. A very low value is not recommended.
RA Retransmit Time	Used to set an interval time between 0 and 4294967295 milliseconds for the dispatch of router advertisements by this interface over the link-local network, in response to a Neighbor Solicitation message. If this Switch is set as the default router for this local link, this value should not exceed the value stated in the **Life Time** field previously mentioned. Setting this field to zero will specify that this switch will not specify the Retransmit Time for the link-local network. (therefore it will be specified by another router on the link-local network. The default value is 0 milliseconds.
RA Managed Flag	Use the pull-down menu to enable or disable the Managed flag. When enabled, this will trigger the router to use a stateful autoconfiguration process to get both Global and link-local IPv6 addresses for the Switch. The default setting is *Disabled*.
RA Other Configure Flag	Use the pull-down menu to enable or disable the Managed flag. When enabled, this will trigger the router to use a stateful autoconfiguration process to get configuration information that is not address information, yet is important to the IPv6 settings of the Switch. The default setting is *Disabled*.

RA Max Router AdvInterval	Used to set the maximum interval time between the dispatch of router advertisements by this interface over the link-local network. This entry must be no less than 4 seconds (4000 milliseconds) and no more than 1800 seconds. The user may configure a time between 4 and 1800 seconds with a default setting of 600 seconds.
RA Min Router AdvInterval	Used to set the minimum interval time between the dispatch of router advertisements by this interface over the link-local network. This entry must be no less then 3 seconds and no more than .75 (3/4) of the MaxRtrAdvInterval. The user may configure a time between 3 and 1350 seconds with a default setting of 198 seconds.

Stacking

From firmware release v2.00 of this Switch, the xStack DGS-3400 series now supports switch stacking, where a set of twelve switches can be combined to be managed by one IP address through Telnet, the GUI interface (web), the console port or through SNMP. Each switch of this series has either two or three stacking slots located at the rear of the device, which can be used to add 10-gigabit DEM-410CX or DEM-410X stacking modules, sold separately. After adding these stacking ports, the user may connect these ports together using copper or fiber stacking cables (also sold separately) in one of two possible topologies.

Duplex Ring – As shown in Figure 6-9, the Duplex Ring stacks switches in a ring or circle format where data can be transferred in two directions. This topology is very resilient because if there is a break in the ring, data can still be transferred through the stacking cables between switches in the stack.

Duplex Chain – As shown in Figure 6-10, The Duplex Chain topology stacks switches together in a chain-link format. Using this method, data transfer is only possible in one direction and if there is a break in the chain, then data transfer will obviously be affected.

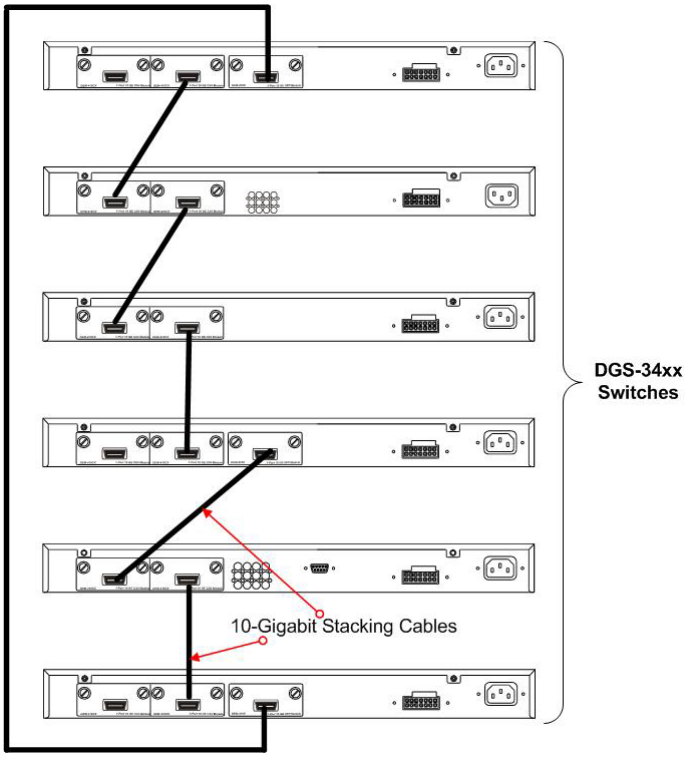


Figure 6- 9. Switches stacked in a Duplex Ring

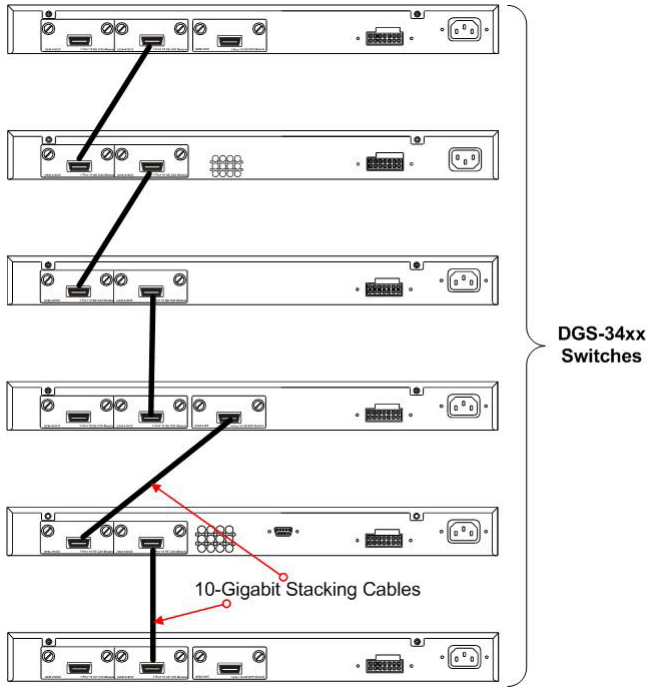


Figure 6- 10. Switches stacked in a Duplex Chain

Within each of these topologies, each switch plays a role in the Switch stack. These roles can be set by the user per individual Switch, or if desired, can be automatically determined by the switch stack. Three possible roles exist when stacking with the xStack DGS-3400 series.

NOTE: Only ports 26 and 27 of the DGS-3427 support stacking. Port 25 cannot be used for stacking, and is to be used only as a 10-Gigabit uplink port.

Primary Master – The Primary Master is the leader of the stack. It will maintain normal operations, monitor operations and the running topology of the Stack. This switch will also assign Stack Unit IDs, synchronize configurations and transmit commands to remaining switches in the switch stack. The Primary Master can be manually set by assigning this Switch the highest priority (a lower number denotes a higher priority) before physically assembling the stack, or it can be determined automatically by the stack through an election process, which determines the lowest MAC address. It will then assign that switch as the Primary Master, if all priorities are the same. The Primary master is physically displayed by the seven segment LED to the far right on the front panel of the switch where this LED will flash between its given Box ID and 'H'.

Backup Master – The Backup Master is the backup to the Primary Master, and will take over the functions of the Primary Master if the Primary Master fails or is removed from the Stack. It also monitors the status of neighboring switches in the stack, will perform commands assigned to it by the Primary Master and will monitor the running status of the Primary Master. The Backup Master can be set by the user by assigning this Switch the second highest priority before physically assembling the stack, or it can be determined automatically by the stack through an election process which determines the second lowest MAC address and then will assign that switch as the Backup Master, if all priorities are the same.

Slave – Slave switches constitute the rest of the switch stack and although not Primary or Backup Masters, they can be placed into these roles when these other two roles fail or are removed from the stack. Slave switches perform operations requested by the master, monitor the status of neighbor switches in the stack and the stack topology and adhere to the Backup Master's commands once it becomes a Primary Master. Slave switches will do a self-check to determine if it is to become the Backup Master if the Backup Master is promoted to the Primary Master, or if the Backup Master fails or is removed from the switch stack. If both Primary and Backup masters fail, or are removed from the Switch stack, it will determine if it is to become the Primary Master. These roles will be determined, first by priority and if the priority is the same, the lowest MAC address.

Once switches have been assembled in the topology desired by the user and powered on, the stack will undergo three processes until it reaches a functioning state.

Initialization State – This is the first state of the stack, where the runtime codes are set and initialized and the system conducts a peripheral diagnosis to determine each individual switch is functioning properly.

Master Election State – Once the codes are loaded and initialized, the stack will undergo the Master Election State where it will discover the type of topology used, elect a Primary Master and then a Backup Master.

Synchronization State – Once the Primary Master and the Backup Master have been established, the Primary Master will assign Stacking Unit IDs to switches in the stack, synchronize configurations for all switches and then transmit commands to the rest of the switches based on the users configurations of the Primary Master.

Once these steps have been completed, the switch stack will enter a normal operating mode.

Stack Switch Swapping

The stacking feature of the xStack DGS-3400 supports "hot swapping" of switches in and out of the running stack. Users may remove or add switches to the stack without powering down or largely affecting the transfer of data between switches in the stack, with a few minor provisions.

When switches are "hot inserted" into the running stack, the new switch may take on the Backup Master or Slave role, depending on configurations set on the newly added switch, such as configured priority or MAC address. The new device will not be the Primary Master, if adding one switch at a time to the Stack. Yet, if adding two stacks together that have both previously undergone the election process, and therefore both have a Primary Master and a Backup master, a new Primary Master will be elected from one of the already existing Primary Masters, based on priority or MAC address. This Primary Master will take over all of the Primary Master's roles for all new switches that were hot inserted. This process is done using discovery packets that circulate through the switch stack every 1.5 seconds until the discovery process has been completed.

The "hot remove" action means removing a device from the stack while the stack is still running. The hot removal is detected by the stack when it fails to receive heartbeat packets during its specified interval from a device, or when one of the stacking ports links is down. Once the device has been removed, the remaining switches will update their stacking topology database to reflect the change. Any one of the three roles, Primary Master, Backup Master or Slave, may be removed from the stack, yet different processes occur for each specific device removal.

If a Slave device has been removed, the Primary Master will inform other switches of the hot remove of this device through the use of unit leave messages. Switches in the stack will clear the configurations of the unit removed, and dynamically learned databases, such as ARP, will be cleared as well.

If the Backup Master has been hot removed, a new Backup Master will be chosen through the election process previously described. Switches in the stack will clear the configurations of the unit removed, and dynamically learned databases, such as ARP, will be cleared as well. Then the Backup Master will begin backing up the Primary Master when the database synchronization has been completed by the stack.

If the Primary Master is removed, the Backup Master will assume the Primary Master's role and a new Backup Master will be chosen using the election process. Switches in the stack will clear the configurations of the unit removed, and dynamically learned databases, such as ARP, will be cleared as well. The new Primary Master will inherit the MAC and IP address of the previous Primary Master to avoid conflict within the stack and the network itself.

If both the Primary Master and the Backup Master are removed, the election process is immediately processed and a new Primary Master and Backup Master are determined. Switches in the stack will clear the configurations of the units removed, and dynamically learned databases, such as ARP, will be cleared as well. Static switch configurations still remain in the database of the remaining switches in the stack and those functions will not be affected.

NOTE: If there is a Box ID conflict when the stack is in the discovery phase, the device will enter a special standalone topology mode. Users can only get device information, configure Box IDs, save and reboot. All stacking ports will be disabled and an error message will be produced on the local console port of each device in the stack. Users must reconfigure Box IDs and reboot the stack.

Stacking Mode Settings

To begin the stacking process, users must first enable this device for stacking by using the following window. To view this window, open the **Administration** folder and click **Stacking > Mode Settings**.

Figure 6- 11. Stacking Mode Settings window

Use the pull-down menu, choose Enabled and click Apply to allow stacking of this Switch.

Box Information

The **Box Information** screen is found in the **Administration** folder under the heading **Stacking**. This window is used to configure stacking parameters associated with all switches in the xStack DGS-3400 Series. The user may configure parameters such as box ID, box priority and pre-assigning model names to switches to be entered into the switch stack.

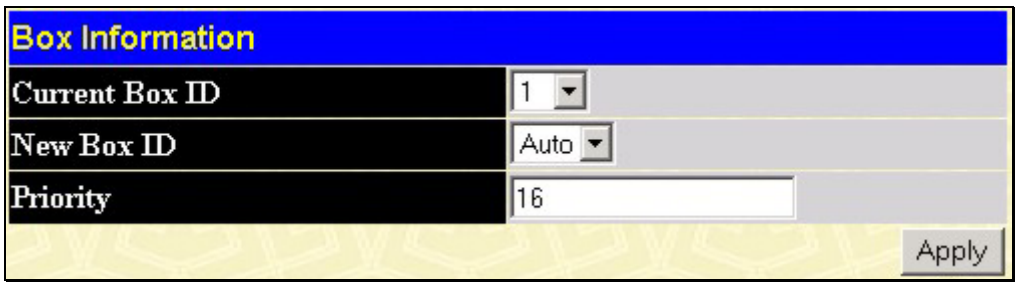


Figure 6- 12. Box Information Configuration window

Parameter	Description
Current Box ID	The Box ID of the switch in the stack to be configured.
New Box ID	The new box ID of the selected switch in the stack that was selected in the **Current Box ID** field. The user may choose any number between 1 and 12 to identify the switch in the switch stack. *Auto* will automatically assign a box number to the switch in the switch 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 Primary Master switch. The Primary Master switch will be used to configure applications of the switch stack.

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

NOTE: Configured box priority settings will not be implemented until users physically save it using the Web GUI or the CLI.

Port Configuration

Click **Administration** > **Port Configuration > Port Configuration** to display the following window:

To configure switch ports:

1. Choose the port or sequential range of ports using the **From**…**To**… port pull-down menus.
2. Use the remaining pull-down menus to configure the parameters described below:

Port Configuration

Unit	From	To	State	Speed/Duplex	Flow Control	Learning	Medium Type	Apply
1	Port 1	Port 1	Enabled	Auto	Disabled	Enabled	Copper	Apply

The Port Information Table-Unit 1

Port	State	Speed/Duplex	Flow Control	Connection	Learning
1	Enabled	Auto	Disabled	Link Down	Enabled
2	Enabled	Auto	Disabled	Link Down	Enabled
3	Enabled	Auto	Disabled	Link Down	Enabled
4	Enabled	Auto	Disabled	1000M/Full/None	Enabled
5	Enabled	Auto	Disabled	Link Down	Enabled
6	Enabled	Auto	Disabled	Link Down	Enabled
7	Enabled	Auto	Disabled	Link Down	Enabled
8	Enabled	Auto	Disabled	Link Down	Enabled
9	Enabled	Auto	Disabled	Link Down	Enabled
10	Enabled	Auto	Disabled	Link Down	Enabled
11	Enabled	Auto	Disabled	Link Down	Enabled
12	Enabled	Auto	Disabled	Link Down	Enabled
13	Enabled	Auto	Disabled	100M/Full/None	Enabled
14	Enabled	Auto	Disabled	Link Down	Enabled
15	Enabled	Auto	Disabled	Link Down	Enabled
16	Enabled	Auto	Disabled	Link Down	Enabled
17	Enabled	Auto	Disabled	Link Down	Enabled
18	Enabled	Auto	Disabled	Link Down	Enabled
19	Enabled	Auto	Disabled	Link Down	Enabled
20	Enabled	Auto	Disabled	Link Down	Enabled
21 (C)	Enabled	Auto	Disabled	Link Down	Enabled
21 (F)	Enabled	Auto	Disabled	Link Down	Enabled
22 (C)	Enabled	Auto	Disabled	Link Down	Enabled
22 (F)	Enabled	Auto	Disabled	Link Down	Enabled
23 (C)	Enabled	Auto	Disabled	Link Down	Enabled
23 (F)	Enabled	Auto	Disabled	Link Down	Enabled
24 (C)	Enabled	Auto	Disabled	Link Down	Enabled
24 (F)	Enabled	Auto	Disabled	Link Down	Enabled

Figure 6- 13. Port Configuration window

The following parameters can be configured:

Parameter	Description
State	Toggle the State field to either enable or disable a given port or group of ports.
Speed/Duplex	Toggle the **Speed/Duplex** field to either select the speed and duplex/half-duplex state of the port. *Auto* denotes auto-negotiation between 10 and 100 Mbps 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* and *100M/Full*, *1000M/Full_M* and *1000M/Full_S*. There is no automatic adjustment of port settings with any option other than Auto. The Switch allows the user to configure two types of gigabit connections; *1000M/Full_M* and *1000M/Full_S*. Gigabit connections only support full duplex connections and take on certain characteristics that are different from the other choices listed. The *1000M/Full_M* (master) and *1000M/Full_S* (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 (*1000M/Full_M)* 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 (*1000M/Full_S)* 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/Filtering for information on entering MAC addresses into the forwarding table. The default setting is Enabled.
Medium Type	If configuring the Combo ports, this defines the type of transport medium to be used, whether copper or fiber.

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

Port Error Disabled

The following window will display the information about ports that have had their connection status disabled, for reasons such as STP loopback detection or link down status. To view this window, click **Port Configuration > Port Error Disabled**.

Port Error Disabled Table

Port	State	Connection	Reason
4	Enabled	Err-Disabled	STP LBD
7	Enabled	Err-Disabled	STP LBD
47	Enabled	Err-Disabled	STP LBD

Figure 6- 14. Port Error Disabled window

The following parameters are displayed:

Parameter	Description
Port	Displays the port that has been error disabled.
Port State	Describes the current running state of the port, whether *Enabled* or *Disabled*.
Connection Status	This field will read the uplink status of the individual ports, whether enabled or Disabled.
Reason	Describes the reason why the port has been error-disabled, such as a STP loopback occurrence.

Port Description

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

First use the **Unit** pull-down menu to choose the switch in the stack to be configured, and then the **From** and **To** pull-down menu to choose a port or range of ports to describe. Users may then enter a description for the chosen port(s). Click **Apply** to set the descriptions in the **Port Description Table**.

If configuring the Combo ports, the **Medium Type** defines the type of transport medium to be used, whether copper or fiber.

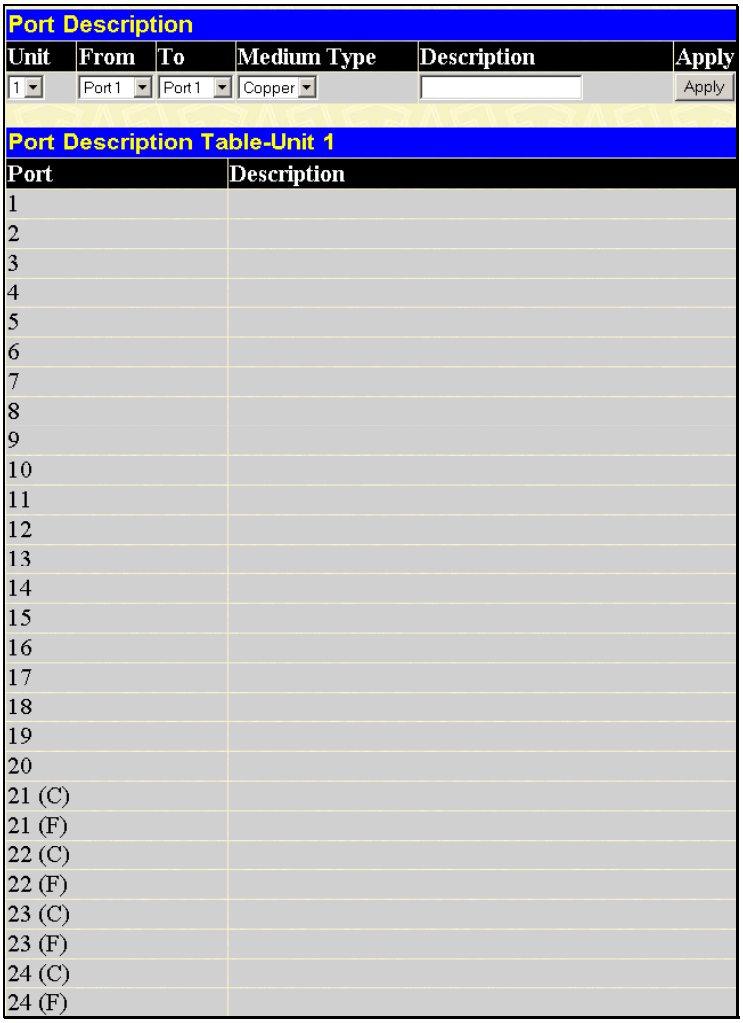


Figure 6- 15. Port Description window

User Accounts

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

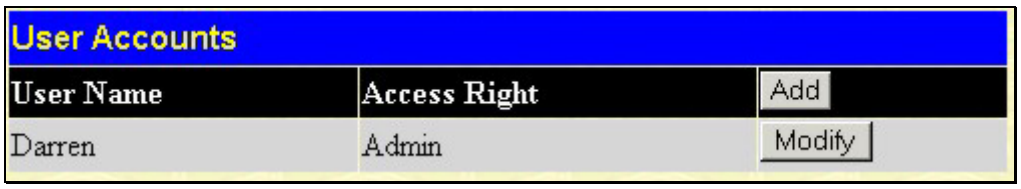


Figure 6- 16. User Accounts Management window

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

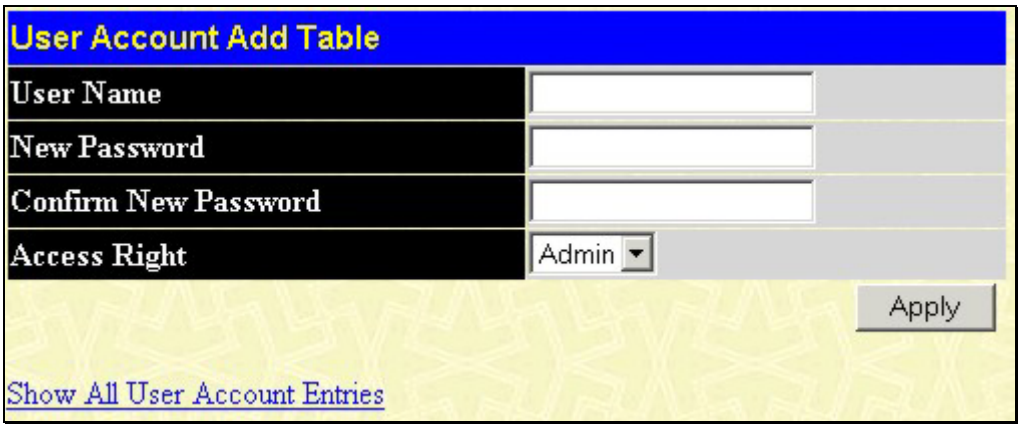


Figure 6- 17. User Accounts - Add

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

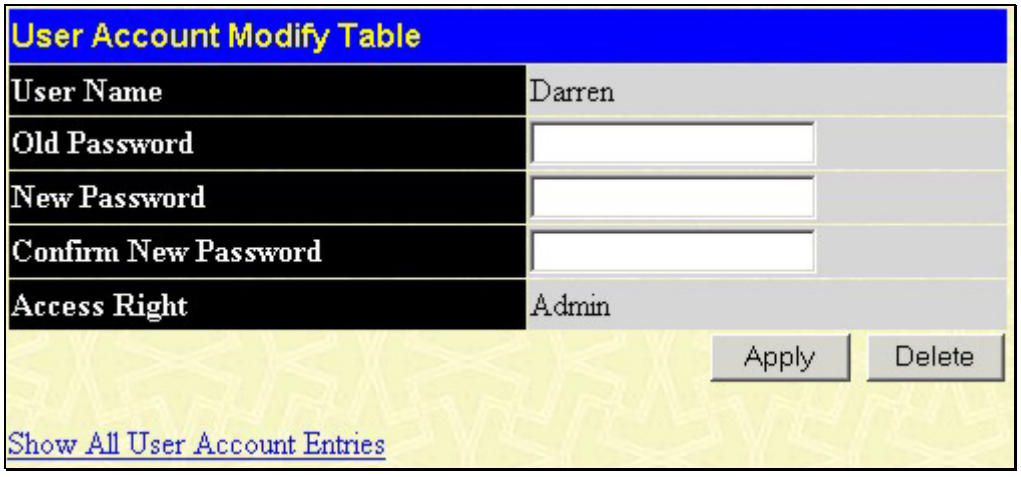


Figure 6- 18. User Accounts Modify Table window - Modify

Modify or delete an existing user account in the **User Account Modify Table**. To delete the user account, click on the **Delete** button. To change the password, type in the *New Password* and retype it in the *Confirm New Password* entry field and click **Apply**. The level of privilege (*Admin* or *User*) can be viewed in the *Access Right* field. Click Show All User Account Entries to return to the **User Accounts** window.

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 **Administration** folder.

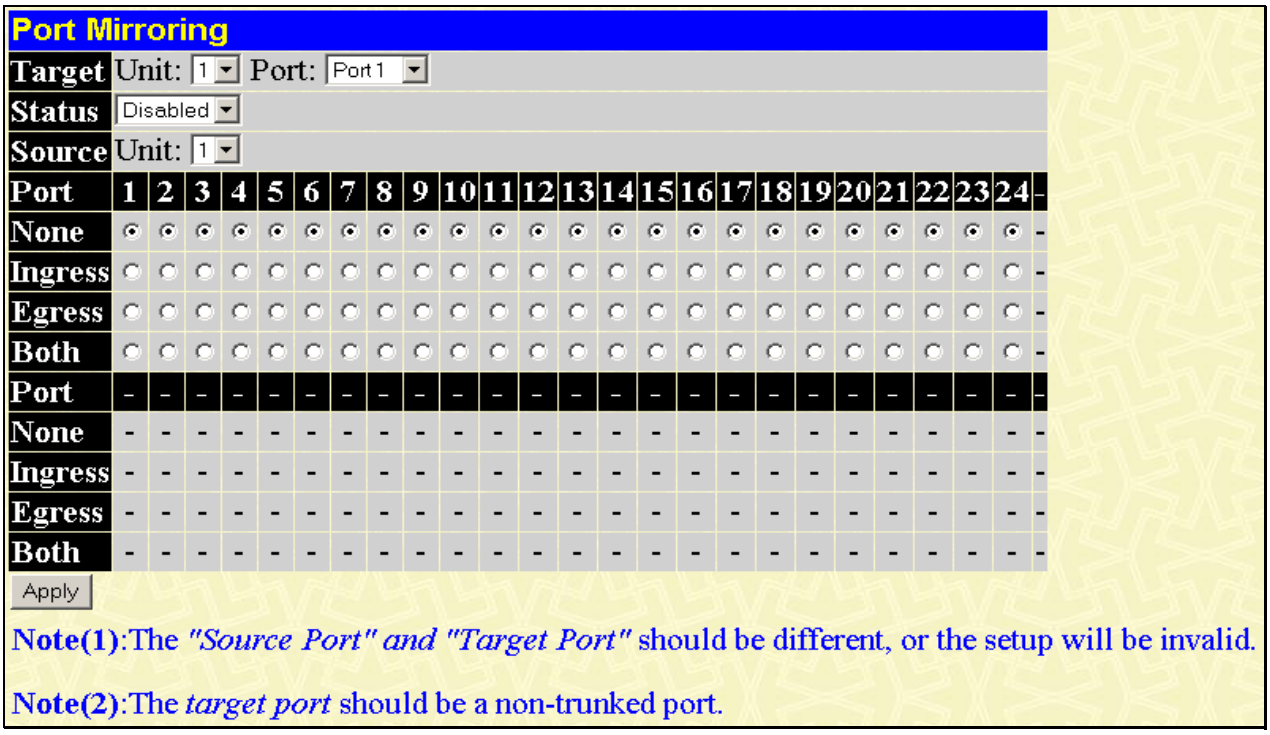


Figure 6- 19. Port Mirroring window

To configure a mirror port:

1. Select the Target Port on the Unit to which frames will be copied, which receives the copies from the source port.
2. Select the Source Direction, Ingress, Egress, or Both and change the Status drop-down menu to *Enabled*.
3. 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.

NOTE: Target mirror ports cannot be members of a trunking group. Attempting to do so will produce an error message and the configuration will not be set.

Mirroing within the Switch Stack

Users may configure mirroring between switches in the switch stack but certain conditions and restrictions apply.

1. When mirroing is configured in the stack, the primary master and the backup master will save and synchronize these mirroring configurations in their respecitve databases. Therefore, if the primary master is removed, the backup master will still hold the mirroing configurations set.

2. If the device hot-removed from the stack holds the target port for the mirroing function, the primary master will disable the mirroing function for the whole stack.
3. Stacking ports cannot be source ports or target mirror ports.

System Log

The Switch can send Syslog messages to up to four designated servers using the **System Log Server**. In the **Administration** folder, click **System Log Settings > System Log Host**, to view the window shown below.

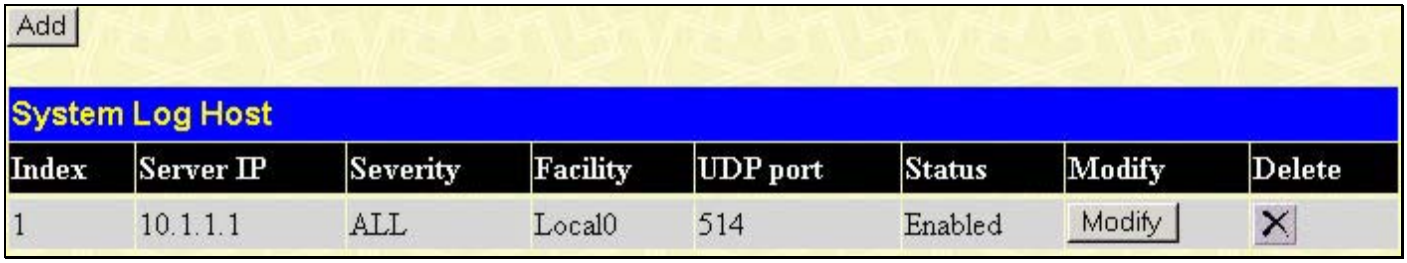


Figure 6- 20. System Log Host list

The parameters configured for adding and editing **System Log Server** settings are the same. See the table below for a description.

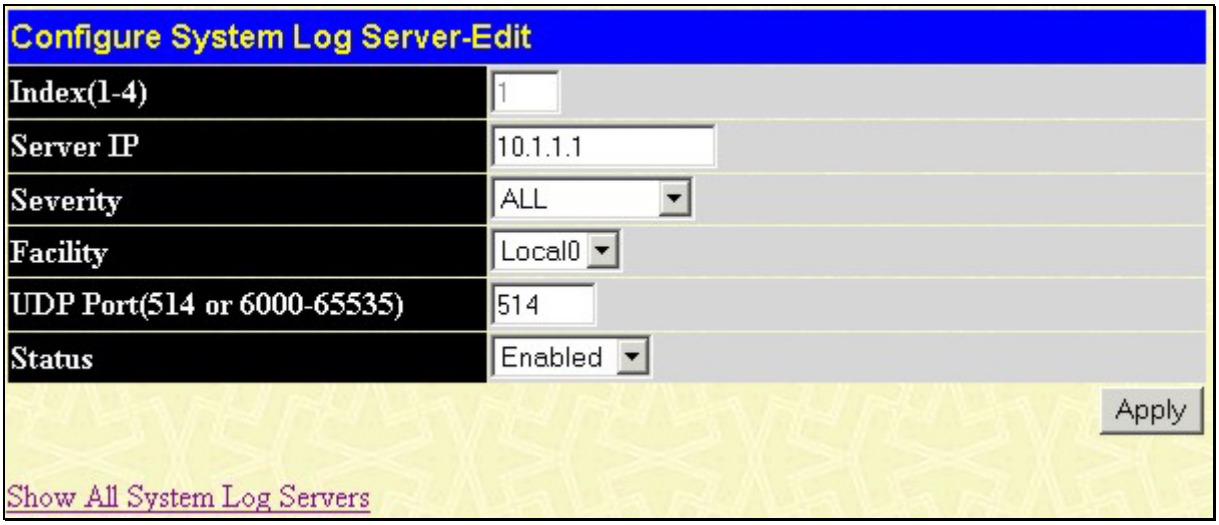


Figure 6- 21. System Log Server menu – Edit

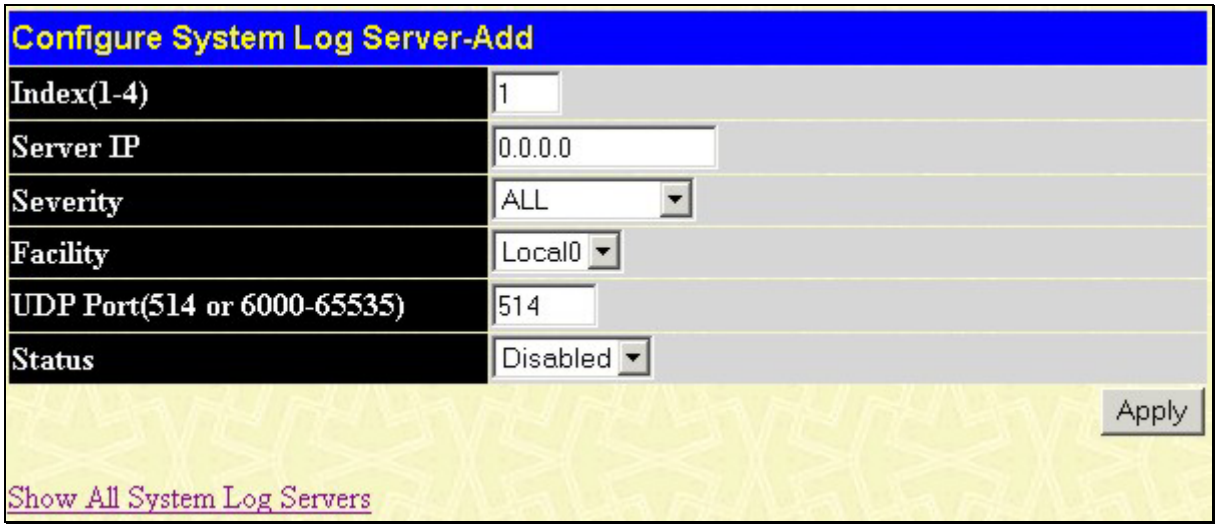


Figure 6- 22. System Log Server menu– Add

Configure the parameters listed below:

Parameter	Description
Index	Syslog server settings index (1-4).
Server IP	The IPv4 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 means the facility values that the Switch currently now.
	Numerical Code / **Facility**
	0 kernel messages 1 user-level messages 2 mail system 3 system daemons 4 security/authorization messages 5 messages generated internally by syslog line printer subsystem 7 network news subsystem 8 UUCP subsystem 9 clock daemon 10 security/authorization messages 11 FTP daemon 12 NTP subsystem 13 log audit 14 log alert 15 clock daemon **16 local use 0 (local0)** **17 local use 1 (local1)** **18 local use 2 (local2)** **19 local use 3 (local3)** **20 local use 4 (local4)** **21 local use 5 (local5)** **22 local use 6 (local6)** **23 local use 7 (local7)**
UDP Port (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 **System Log Server** window, click the corresponding ✕ under the Delete heading of the entry to delete. To return to the **Current System Log Servers** window, click the Show All System Log Servers link.

System Log Save Mode Settings

The **System Log Save Mode Settings** window may be used to choose a method for which to save the switch log to the flash memory of the Switch. To view this window, open the **Administration** folder and then click **System Log > System Log Save Mode Settings.**

Figure 6- 23. System Log Save Mode Settings

Use the pull-down menu to choose the method for saving the switch log to the Flash memory. The user has three options:

Time Interval – Users who choose this method can configure a time interval by which the switch will save the log files, in the box adjacent to this configuration field. The user may set a time between 1 and 65535 minutes. The default setting is one minute.

On Demand – Users who choose this method will only save log files when they manually tell the Switch to do so, using the **Save Services** folder under the **Save Changes** link.

On Trigger – Users who choose this method will have log files saved to the Switch every time a log event occurs on the Switch.

The default setting is **On Demand**. Click **Apply** to save changes made. Click Save Log Now to immediately save log files currently on the switch.

System Severity Settings

The Switch can be configured to allow alerts be logged or sent as a trap to an SNMP agent or both. The level at which the alert triggers either a log entry or a trap message can be set as well. Use the **System Severity Settings** menu to set the criteria for alerts. The current settings are displayed below the System Severity Table. In the **Administration** folder, click **System Severity Settings**, to view the window shown below.

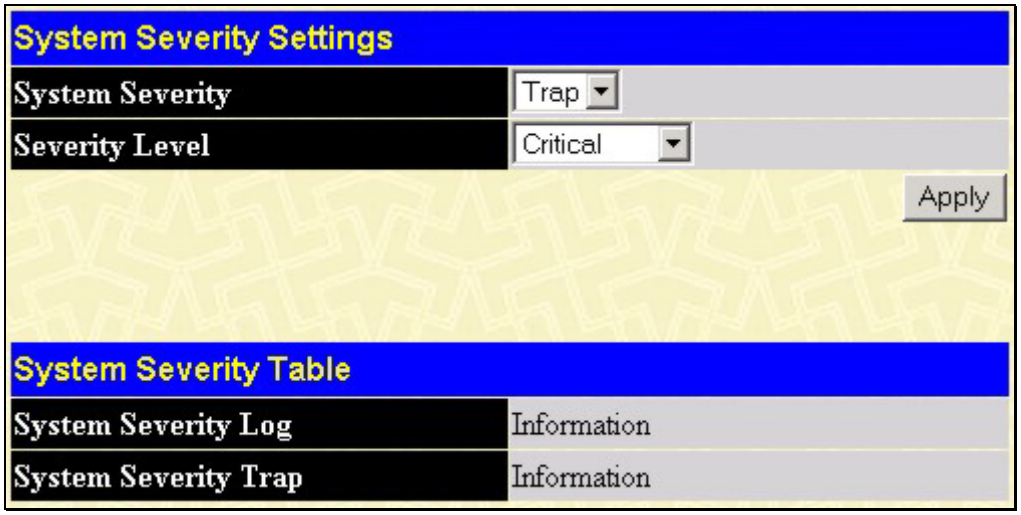


Figure 6- 24. System Severity Settings

Use the drop-down menus to configure the parameters described below.

Parameter	Description
System Severity	Choose how the alerts are used from the drop-down menu. Select *log* to send the alert of the Severity Type configured to the Switch's log for analysis. Choose *trap* to send it to an SNMP agent for analysis, or select *all* to send the chosen alert type to an SNMP agent and the Switch's log for analysis.
Severity Level	Choose what level of alert will trigger sending the log entry or trap message as defined by the Severity Name. Select *critical* to send only critical events to the Switch's log or SNMP agent. Choose *warning* to send critical and warning events to the Switch's log or SNMP agent. Select *information* send informational, warning and critical events to the Switch's log or SNMP agent.

Click **Apply** to implement the new System Severity Settings.

SNTP Settings

Time Settings

To configure the time settings for the Switch, open the **Administration** folder. Then the **SNTP Settings** folder and click on the **Time Settings** link, revealing the following window for the user to configure.

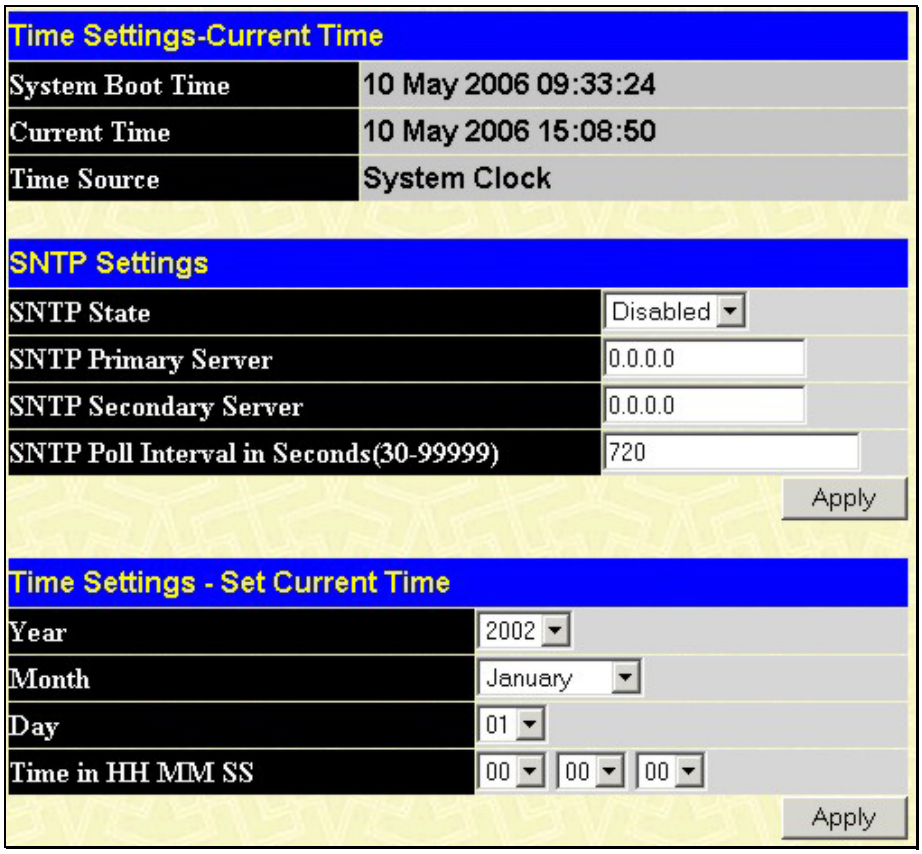


Figure 6- 25. Current Time: Status window

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 *Enabled* or *Disabled* SNTP.
SNTP Primary Server	The IP address of the primary server from which the SNTP information will be taken.
SNTP Secondary Server	The IP address of the secondary server from which the SNTP information will be taken.
SNTP Poll Interval in Seconds (30-99999)	The interval, in seconds, between requests for updated SNTP information.
Current Time: Set Current Time	
Year	Enter the current year, to update the system clock.
Month	Enter the current month, to update the system clock.
Day	Enter the current day, to update the system clock.
Time in HH MM SS	Enter the current time in hours, minutes, and seconds.

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 **Administration** folder, then the **SNTP Settings** folder and click on the **Time Zone and DST** link, revealing the following window.

The following parameters can be set:

Parameter	Description
Time Zone and DST Settings	
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.)

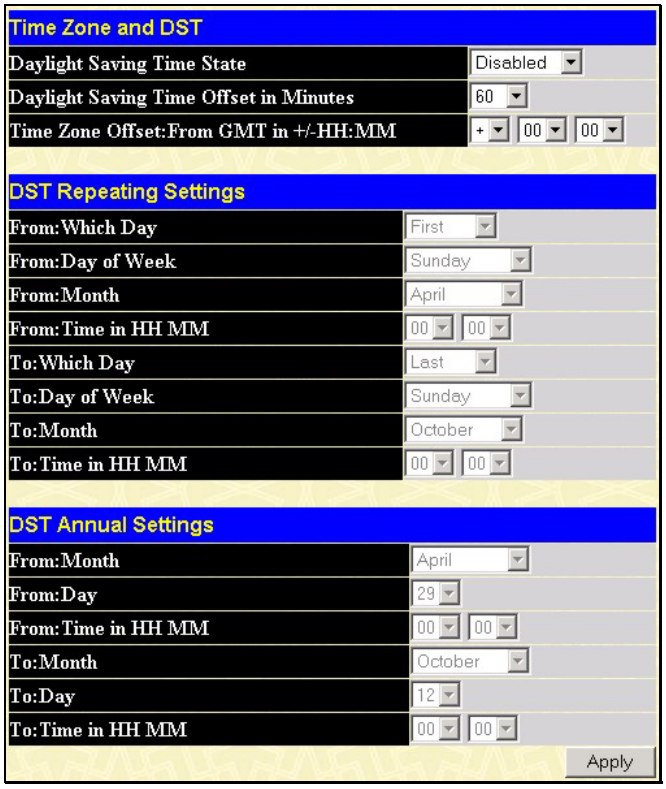


Figure 6- 26. Time Zone and DST Settings window

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 concisely. 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 monthDST 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** window.

MAC Notification Settings

MAC Notification is used to monitor MAC addresses learned and entered into the forwarding database. To globally set MAC notification on the Switch, open the following window by opening the **MAC Notification Settings** in the Administration folder.

Global Settings

The following parameters may be viewed and modified:

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

Port Settings

To change MAC notification settings for a port or group of ports on the Switch, configure the following parameters.

Parameter	Description
Unit	Choose the switch in the switch stack for which to configure these settings.
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.

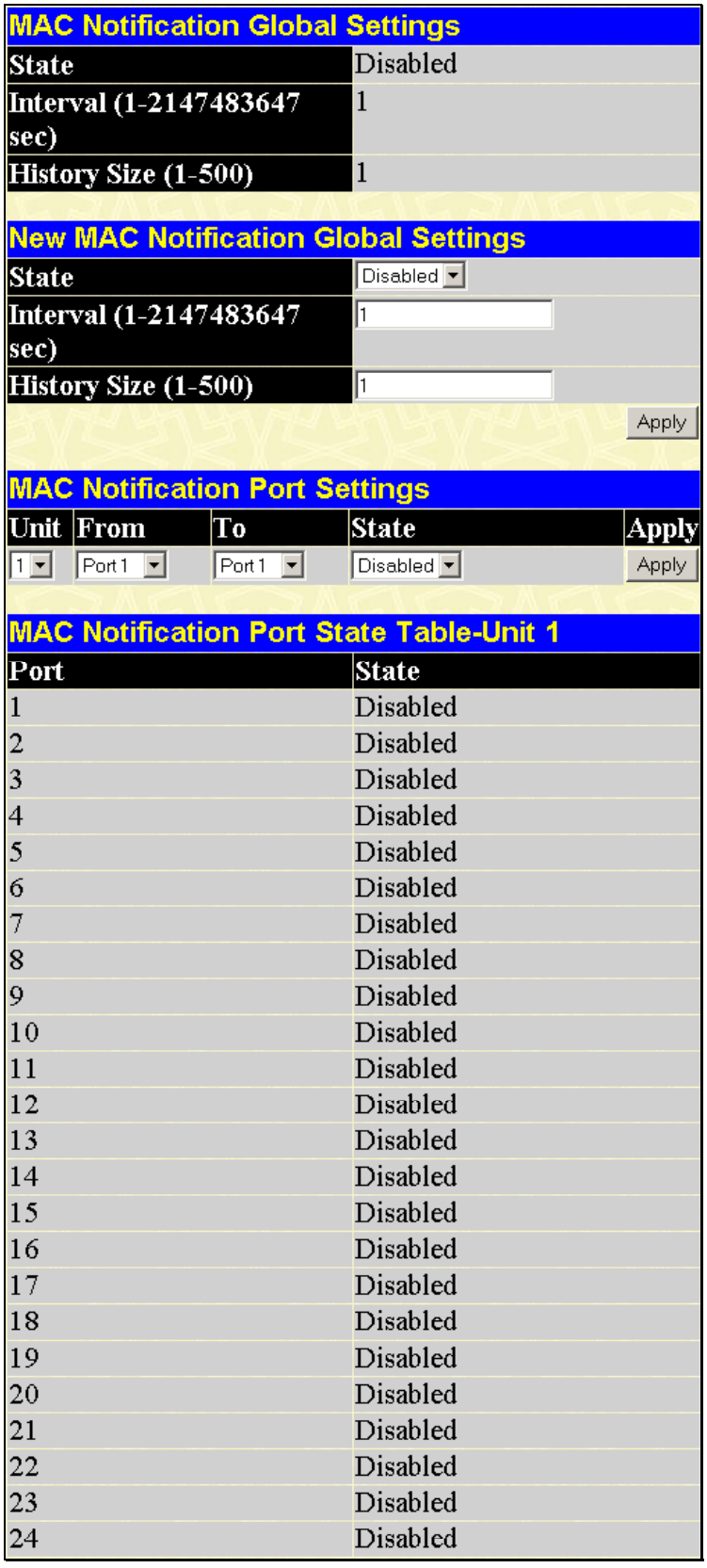


Figure 6- 27. MAC Notification Settings

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 configuration settings can be saved and a history and attack log can be uploaded from the Switch to the TFTP server. The Switch supports dual image storage for configuration and firmware. The firmware and configuration images are indexed by ID number 1 or 2. To change the boot firmware image, use the **Config Firmware Image** menu **Multiple Image Services** sub-directory. The default Switch settings will use Image ID 1 as the boot configuration or firmware. To update the Switch's firmware or configuration file, open the **TFTP Services** hyperlink, located in the **Administration** folder.

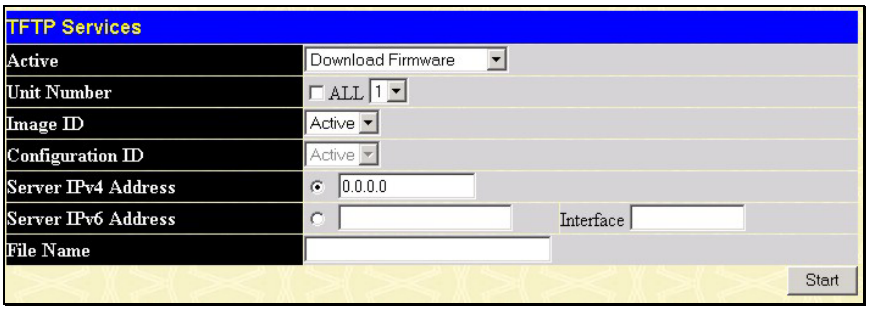


Figure 6- 28. TFTP Services menu

Configure the following parameters and then click **Start** to initiate the file transfer.

Parameter	Description
Active	Select a service for the TFTP server to perform from the drop down window: *Download Firmware* - Enter the IP address of the TFTP server and specify the location of the new firmware on the TFTP server. Click **Start** to record the IP address of the TFTP server and to initiate the file transfer. *Download Configuration* - Enter the IP address of the TFTP server, and the path and filename for the Configuration file on the TFTP server. Click **Start** to record the IP address of the TFTP server and to initiate the file transfer. *Upload Configuration* - Enter the IP address of the TFTP server and the path and filename for the switch settings on the TFTP server. Click **Start** to record the IP address of the TFTP server and to initiate the file transfer. *Upload Log* - 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. *Upload Attack Log* - Enter the IP address of the TFTP server and the path and filename for the attack log on the TFTP server. Click **Start** to record the IP address of the TFTP server and to initiate the file transfer.
Unit Number	Select the switch in the switch stack from which, or to which to upload or download files. Clicking the ALL check box will denote all switches in the switch stack.
Image ID	For firmware downloads, select the Image ID of the firmware. The Switch 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. Choosing *Active* will download the firmware to the Boot Up Image ID, depending on the user's configuration. Information on configuring Image IDs can be found in this section, under the heading **Multiple Image Services**.
Configuration ID	For configuration downloads, select the Image ID of the configuration. The Switch can hold two configuration images in its memory. *Image ID 1* will always be the boot up configuration for the Switch unless specified by the user. Choosing *Active* will download the configuration to the Boot Up Image ID, depending on the user's configuration. Information on configuring Image IDs can be found in this section, under the heading **Multiple Image Services**.
Server IPv4 Address	Enter the IPv4 address of the server from which to download firmware.
Server IPv6 Address	Enter the IPv6 address of the server from which to download firmware. The Interface field is used for addresses on the link-local network. It is recommended that the user enter the specific interface for a link-local IPv6 address. For Global IPv6 addresses, this field may be omitted.
File Name	Enter the path and filename of the firmware or configuration file to upload or download.

Multiple Image Services

The **Multiple Image Services** folder allows users of the Switch 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** menu.

Firmware Information

The following screen allows the user to view information about current firmware images stored on the Switch. To access the following screen, click **Administration > Multiple Image Services > Firmware Information**.

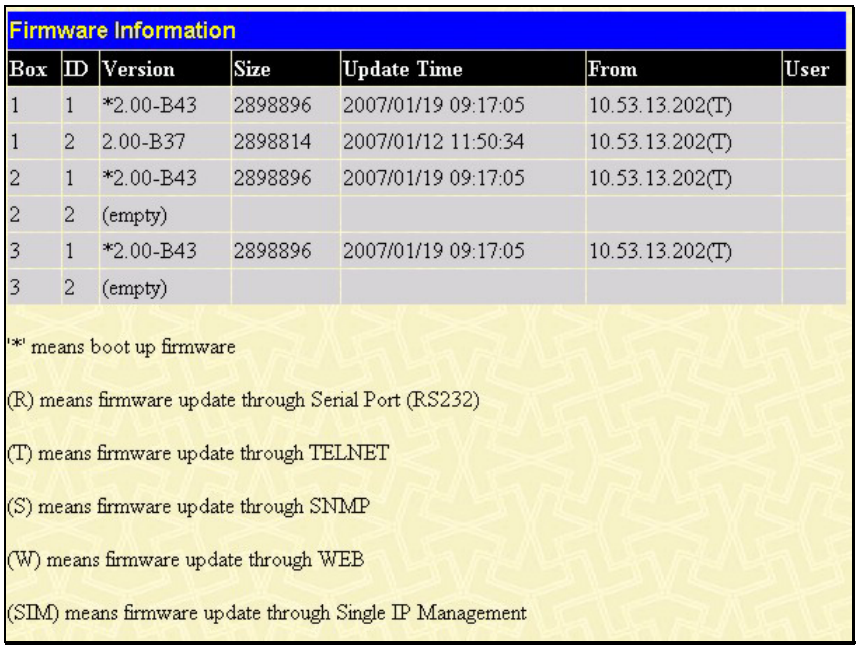


Figure 6- 29. Firmware Information window

This window holds the following information:

Parameter	Description
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 five ways firmware may be downloaded to the Switch. Boot Up files are denoted by an asterisk (*) next to the file. 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 management interface. SIM – If the IP address has this letter attached to it, it denotes a firmware upgrade through the Single IP Management feature.
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 following window is used to configure firmware set in 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. The user may select a boot up firmware image for the Switch in the switch stack by using the **Image** pull-down window to select it, change the **Action** to *Boot* and click **Apply**. To delete a firmware image, select it using the **Image** pull-down menu, change the **Action** field to *Delete* and click **Apply**.

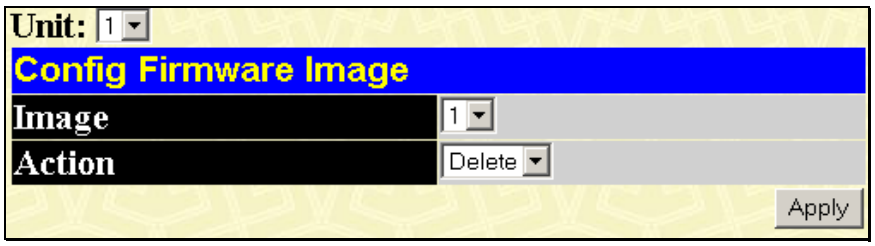


Figure 6- 30. Config Firmware Image window

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.

IPv4 Ping Test

The following window is used to Ping an IPv4 address. To locate this window, open the **Administration** folder and click **Ping Test > IPv4 Ping Test.**

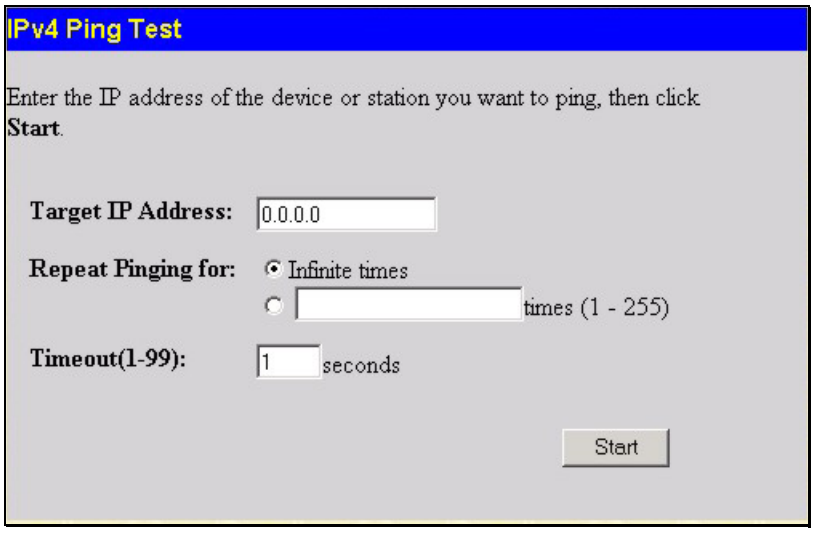
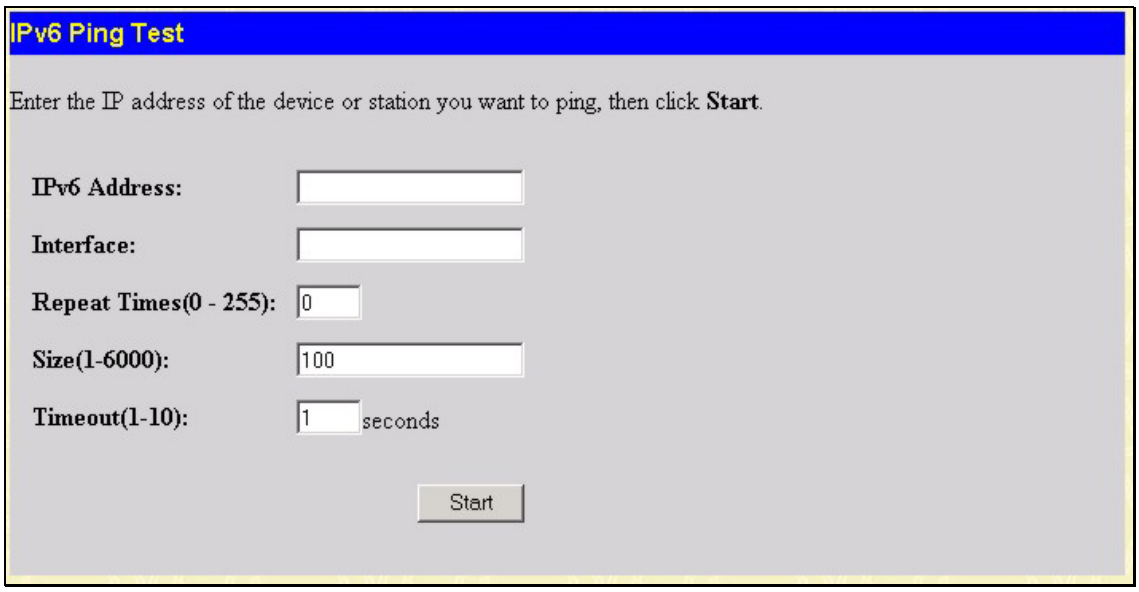


Figure 6- 31. Ping Test window

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.

IPv6 Ping Test

The following window is used to Ping an IPv6 address. To locate this window, open the **Administration** folder and click **Ping Test > IPv6 Ping Test.**



This window allows the following parameters to be configured to ping an IPv6 address.

Parameter	Description
IPv6 Address	Enter an IPv6 address to be pinged.
Interface	The Interface field is used for addresses on the link-local network. It is recommended that the user enter the specific interface for a link-local IPv6 address. For Global IPv6 addresses, this field may be omitted.
Repeat Times	Enter the number of times desired to attempt to ping the IPv6 address configured in this window. Users may enter a number of times between 0 and 255.
Size	Use this field to set the datagram size of the packet, or in essence, the number of bytes in each ping packet. Users may set a size between 1 and 6000 bytes with a default setting of 100 bytes.
Timeout	Select a timeout period between 1 and 10 seconds for this Ping message to reach its destination. If the packet fails to find the IPv6 address in this specified time, the Ping packet will be dropped.

Click **Start** to initialize the Ping program.

Safeguard Engine

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the switch load beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth. The Safeguard Engine has two operating modes, which can be configured by the user, **Strict** and **Fuzzy**. In Strict mode, when the Switch either (a) receives too many packets to process or (b) exerts too much memory, it will enter the **Exhausted** mode. When in this mode, the Switch will drop all ARP and IP broadcast packets and packets from untrusted IP addresses for a calculated time interval. Every five seconds, the Safeguard Engine will check to see if there are too many packets flooding the Switch. If the threshold has been crossed, the Switch will initially stop all ingress ARP and IP broadcast packets and packets from untrusted IP addresses for five seconds. After another five-second checking interval arrives, the Switch will again check the ingress flow of packets. If the flooding has stopped, the Switch will again begin accepting all packets. Yet, if the checking shows that there continues to be too many packets flooding the Switch, it will stop accepting all ARP and IP broadcast packets and packets from untrusted IP addresses for double the time of the previous stop period. This doubling of time for stopping these packets will continue until the maximum time has been reached, which is 320 seconds and every stop from this point until a return to normal ingress flow would be 320 seconds. For a better understanding, examine the following example of the Safeguard Engine.

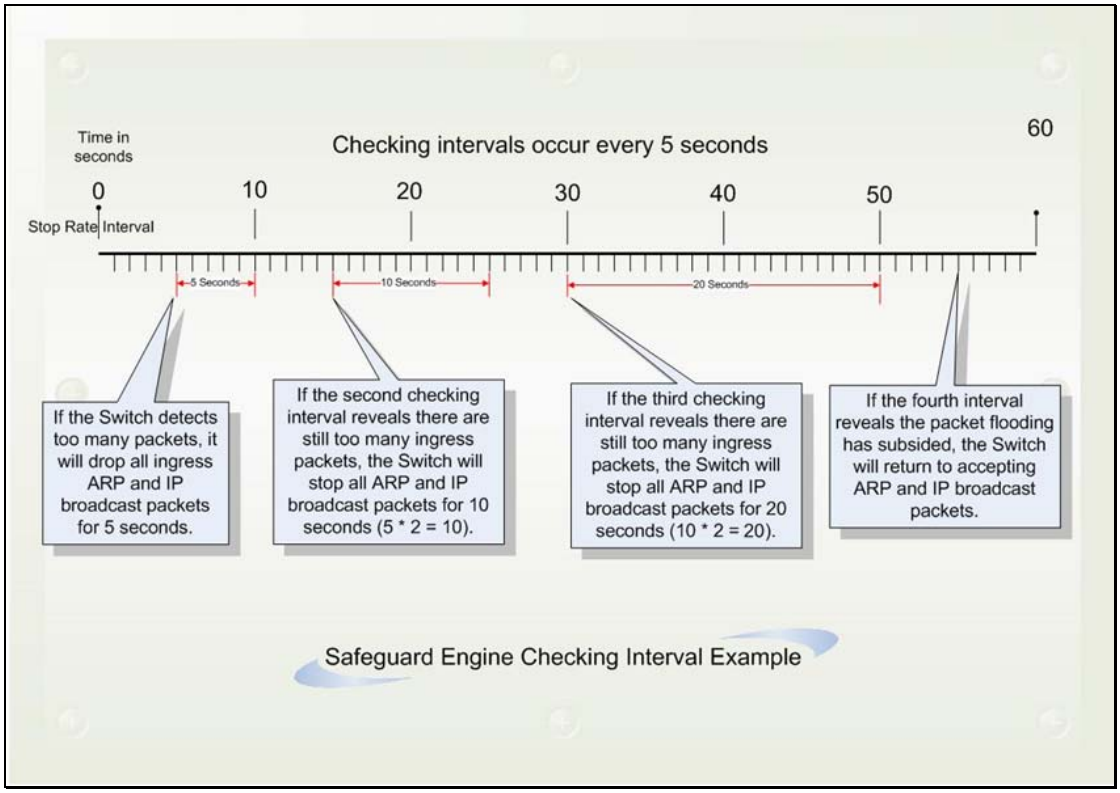


Figure 6- 32. Safeguard Engine example

For every consecutive checking interval that reveals a packet flooding issue, the Switch will double the time it will discard ingress ARP and IP broadcast packets and packets from untrusted IP addresses. In the example above, the Switch doubled the time for dropping ARP and IP broadcast packets when consecutive flooding issues were detected at 5-second intervals. (First stop = 5 seconds, second stop = 10 seconds, third stop = 20 seconds) Once the flooding is no longer detected, the wait period for dropping ARP and IP broadcast packets will return to 5 seconds and the process will resume.

In Fuzzy mode, once the Safeguard Engine has entered the Exhausted mode, the Safeguard Engine will decrease the packet flow by half. After returning to Normal mode, the packet flow will be increased by 25%. The switch will then return to its interval checking and dynamically adjust the packet flow to avoid overload of the Switch.

NOTICE: When Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

Safeguard Engine Settings

To enable Safeguard Engine or configure advanced Safeguard Engine settings for the Switch, click **Administration > Safeguard Engine > Safeguard Engine Settings**, which will open the following window.

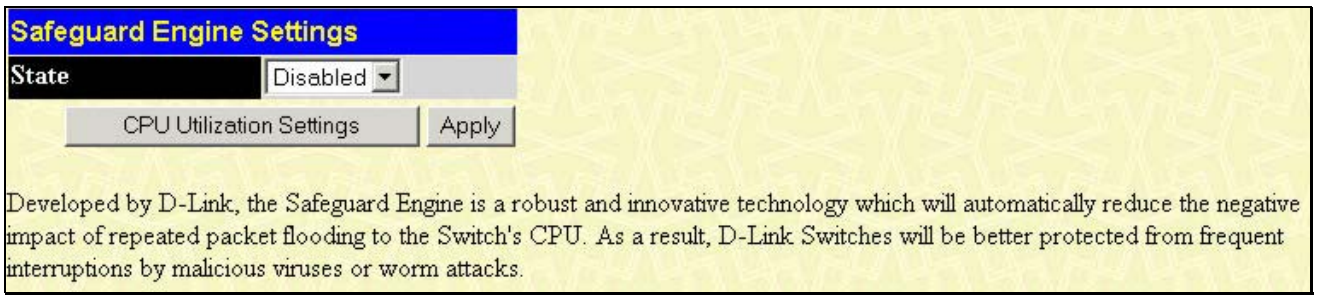


Figure 6- 33. Safeguard Engine State menu

To enable the Safeguard Engine option, select *Enabled* with the drop-down **State** menu and click the **Apply** button.

To configure the advanced settings for the Safeguard Engine, click the **CPU Utilization Settings** button to view the following menu.

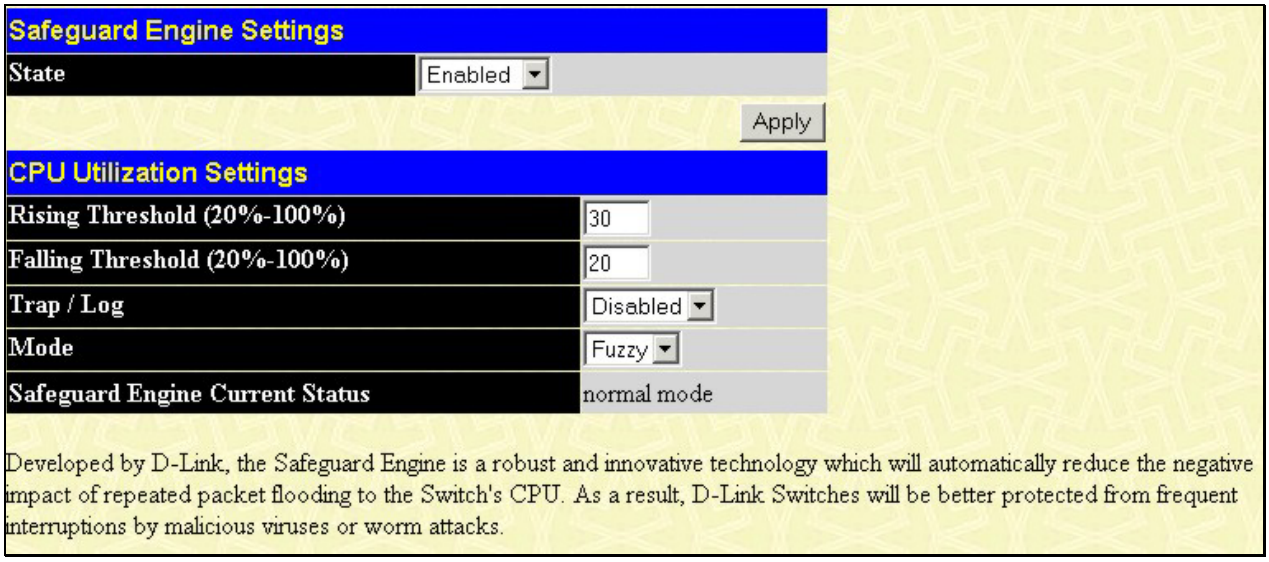


Figure 6- 34. Safeguard Engine CPU Utilization Settings menu

To configure, set the following parameters and click **Apply**.

Parameter	Description
State	Use the pull-down menu to globally enable or disable Safeguard Engine settings for the Switch.
Rising	Used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into Safeguard Engine state, based on the parameters provided in this window.
Falling	Used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.
Trap / Log	Use the pull-down menu to enable or disable the sending of messages to the device's SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate.
Mode	Used to select the type of Safeguard Engine to be activated by the Switch when the CPU utilization reaches a high rate. The user may select: *Fuzzy* – If selected, this function will instruct the Switch to minimize the IP and ARP traffic flow to the CPU by dynamically allotting an even bandwidth to all traffic flows. *Strict* – If selected, this function will stop accepting all ARP packets not intended for the Switch, and will stop receiving all unnecessary broadcast IP packets, until the storm has subsided. The default setting is Fuzzy mode.

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 Table** go to **Administration** > **Static ARP Settings**.

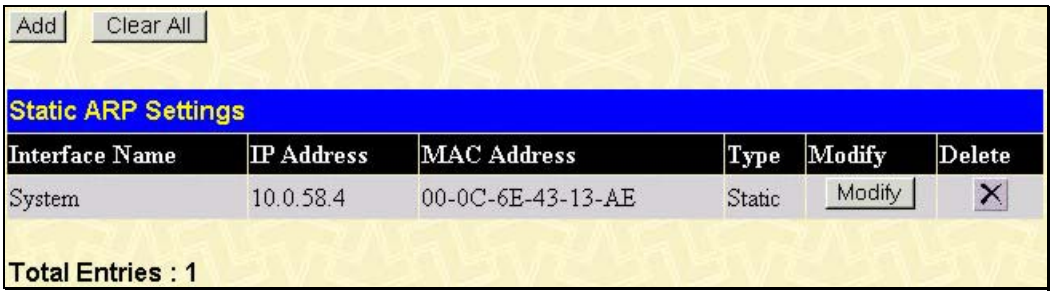


Figure 6- 35. Static ARP Settings window

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

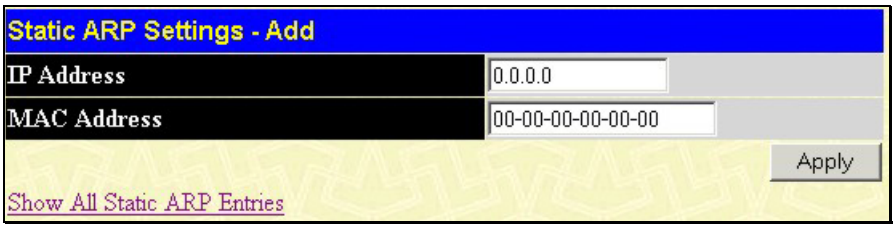


Figure 6- 36. Static ARP Settings – Add window

To modify a current entry, click the corresponding **Modify** button of the entry to be modified, revealing the following screen to configure:

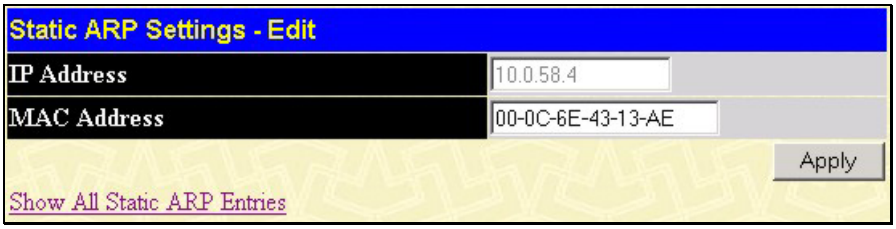


Figure 6- 37. Static ARP Settings – Edit window

The following fields can be set or viewed:

Parameter	Description
IP Address	The IP address of the ARP entry. This field cannot be edited in the Static ARP Settings – Edit window.
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.

IPv6 Neighbor

IPv6 neighbors are devices on the link-local network that have been detected as being IPv6 devices. These devices can forward packets and keep track of the reachability of routers, as well as if changes occur within link-layer addresses of nodes on the network or if identical unicast addresses are present on the local link. The following two windows are used to view IPv6 neighbors, and add or delete them from the Neighbor cache.

IPv6 Neighbor Settings

The following window is used to view and configure current IPv6 neighbors of the Switch. To view this window, open the **Administration** folder and click **IPv6 Neighbor > IPv6 Neighbor Settings**.

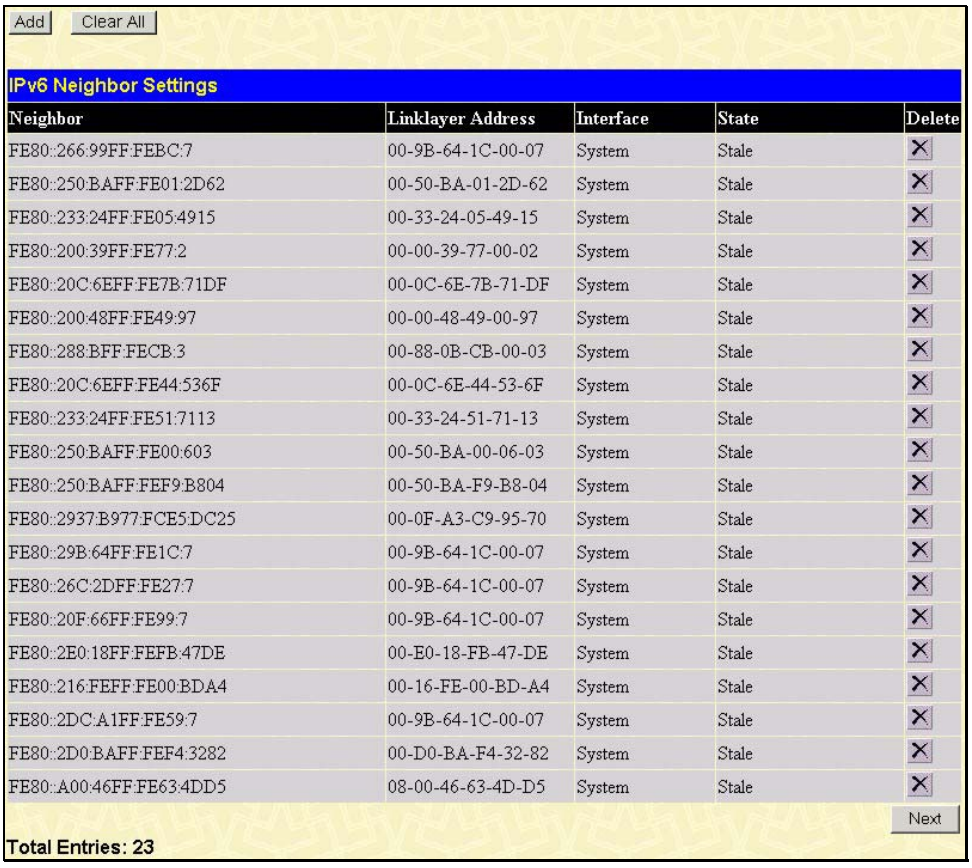


Figure 6- 38. IPv6 Neighbor Settings window

The following fields can be viewed:

Parameter	Description
Neighbor	Displays the IPv6 address of the neighbor device.
Link Layer Address	Displays the MAC Address of the corresponding IPv6 device.
Interface	Displays the Interface name associated with this IPv6 address.
State	Displays the running state of the corresponding IPv6 neighbor. The user may see six possible entries in this field, which are *Incomplete, Stale, Probe, Reachable, Delay or Static*.

To remove an entry, click the *Delete* button for the entry being removed. To completely clear the **IPv6 Neighbor Settings**, click the **Clear All** button. To add a new entry, click the **Add** button, revealing the following screen to configure:

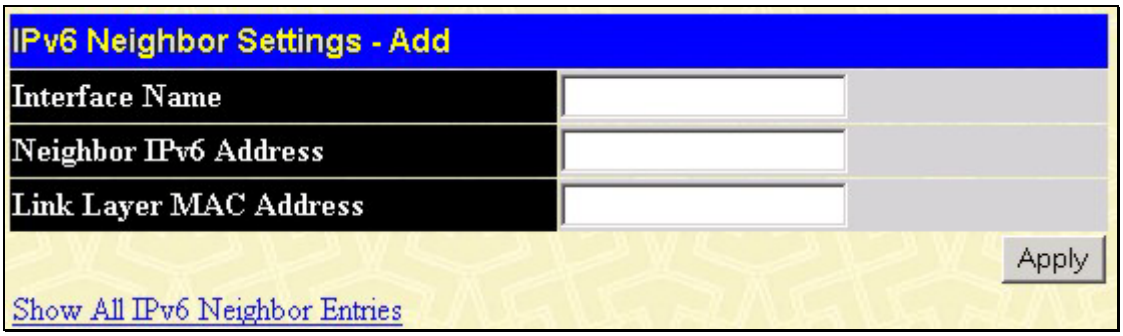


Figure 6- 39. IPv6 Neighbor Settings – Add window

The following fields can be set or viewed:

Parameter	Description
Interface Name	Enter the name of the Interface associated with this entry, if any. The Interface field is used for addresses on the link-local network. It is recommended that the user enter the specific interface for a link-local IPv6 address. For Global IPv6 addresses, this field may be omitted.
Neighbor IPv6 Address	The IPv6 address of the neighbor entry. Specify the address using the hexadecimal IPv6 Address (IPv6 Address is hexadecimal number, for example 1234::5D7F/32).
Link Layer MAC Address	The MAC address of the IPv6 neighbor entry.

After entering the IPv6 Address and MAC Address of the **Static IPv6 ARP** entry, click **Apply** to implement the new entry. To return to the IPv6 Neighbor window, click the Show All IPv6 Neighbor Entries link.

Routing Table

The Switch supports only static routing for IPv4 and IPv6 formatted addressing. Users can create up to 128 static route entries for IPv4 and IPv6 combined. Manually configured static routes can route IP packets, and the local route also can route IP packets. For each device that is a part of the DGS-3400 network, users may only configure one IP address as a static route.

For IPv4 static routes, once a static route has been set, the Switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the switch from that next hop, the route becomes enabled. If a response is not received from the next hop device after three ARP requests have been set, the configured static route will remain in a link-down status.

The Switch also supports a floating static route, which means that the user may create an alternative static route to a different next hop device located in the other network. This secondary next hop device route is considered as a backup static route for when the primary static route is down. If the primary route is lost, the backup route will uplink and its status will become Active.

IPv4 Static/Default Route Settings

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**. To view the following window, click **Administration > Routing Table > IPv4 Static/Default Route Settings**.

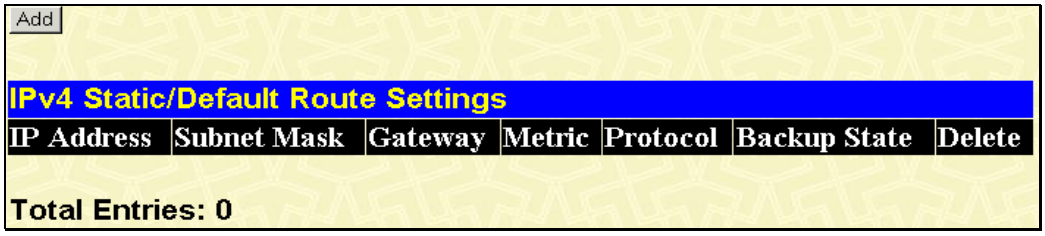


Figure 6- 40. Static/Default Route Settings window

This window shows the following values:

Parameter	Description
IP Address	The IPv4 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.
Metric	Represents the metric value of the IP interface entered into the table. This field may read a number between 1-65535.
Protocol	Represents the protocol used for the Routing Table entry of the IP interface.
Backup State	Represents the Backup state for which this IP interface is configured. This field may read Primary or Backup.
Delete	Click the ✕ button to delete this entry from the IPv4 Static/Default Route Settings table.

To enter an IP Interface into the Switch's **IPv4 Static/Default Route Settings** window, click the **Add** button, revealing the following window to configure.

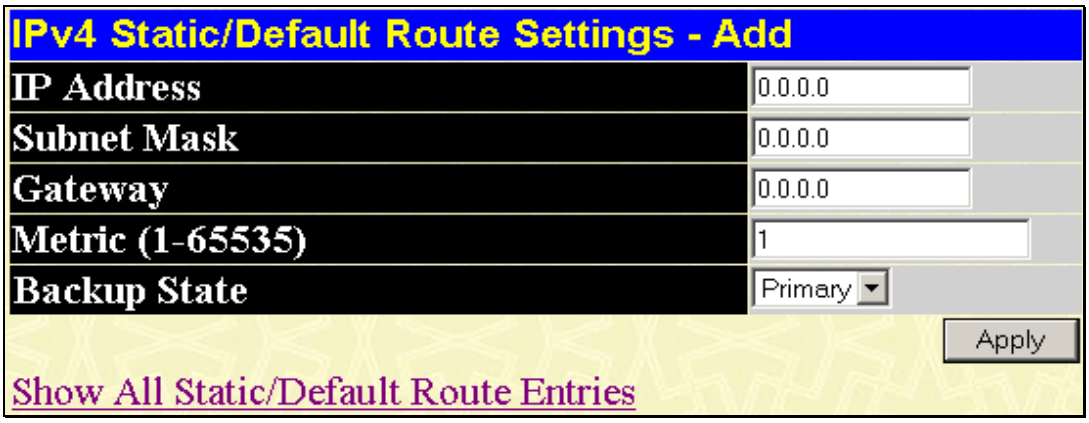


Figure 6- 41. Static/Default Route Settings – Add window

The following fields can be set:

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

Click **Apply** to implement changes made.

IPv6 Static/Default Route Settings

A static entry of an IPv6 address can be entered into the Switch's routing table for IPv6 formatted addresses. To view the following window, click **Administration > Routing Table > IPv6 Static/Default Route Settings**.

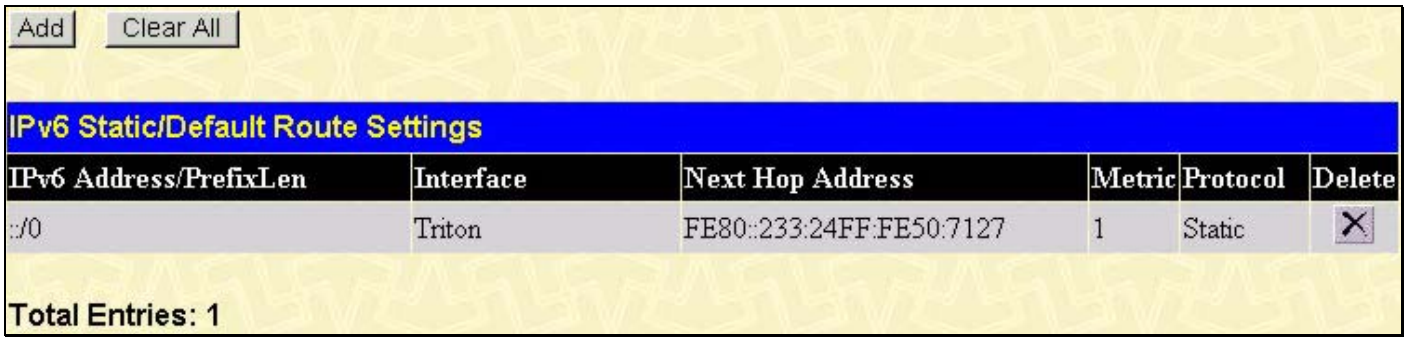


Figure 6- 42. IPv6 Static Route Settings window

This window shows the following values:

Parameter	Description
IPv6 Address/PrefixLen	The IPv6 address and corresponding Prefix Length of the IPv6 static route entry.
Interface	The IP Interface where the static IPv6 route is created.

Next Hop Address	The corresponding IPv6 address for the next hop Gateway address in IPv6 format.
Metric (1-65535)	The metric of the IPv6 interface entered into the table representing the number of routers between the Switch and the IPv6 address above. Metric values allowed are between 1-65535.
Protocol	Represents the status for the IPv6 routing table entry.
Delete	Click the ✕ button to delete this entry from the list.

To enter an IPv6 Interface into the **IPv6 Static Route** list, click the **Add** button, revealing the following window to configure.

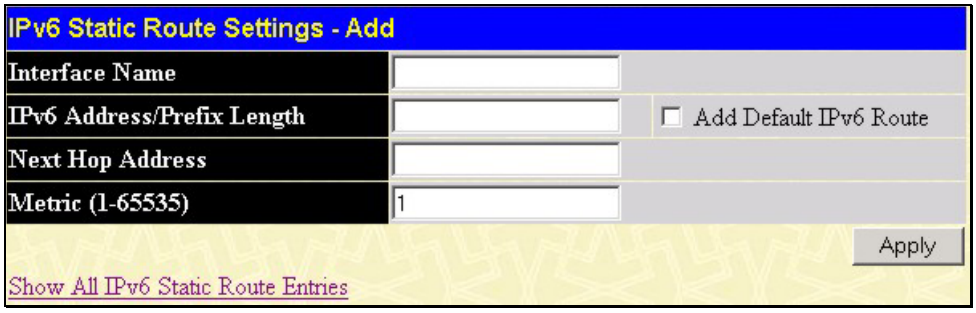


Figure 6- 43. Static/Default Route Settings – Add menu

Click to select the **default** option if this will be the default IPv6 route. Choosing this option will allow the user to configure the default gateway for the next hop router only.

The following fields can be set:

Parameter	Description
Interface	The IP Interface where the static IPv6 route is to be created.
IPv6 Address/Prefix Length	Specify the address and mask information using the format as IPv6 address / prefix length (IPv6 address is hexadecimal number, prefix length is decimal number, for example 1234::5D7F/32). Clicking the default check box will set the IPv6 address as unspecified and the Switch will automatically find the default route. This defines the entry as a 1 hop IPv6 default route.
Next Hop Address	Enter the IPv6 address for the next hop Gateway address in IPv6 format.
Metric (1-65535)	The metric representing the number of routers between the Switch and the IPv6 address above.

Click **Apply** to implement changes made.

DHCP/BOOTP Relay

The relay hops count limit allows the maximum number of hops (routers) that the DHCP/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 BOOTREQUEST 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 *65,536* seconds, with a default value of *0* seconds.

DHCP / BOOTP Relay Global Settings

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

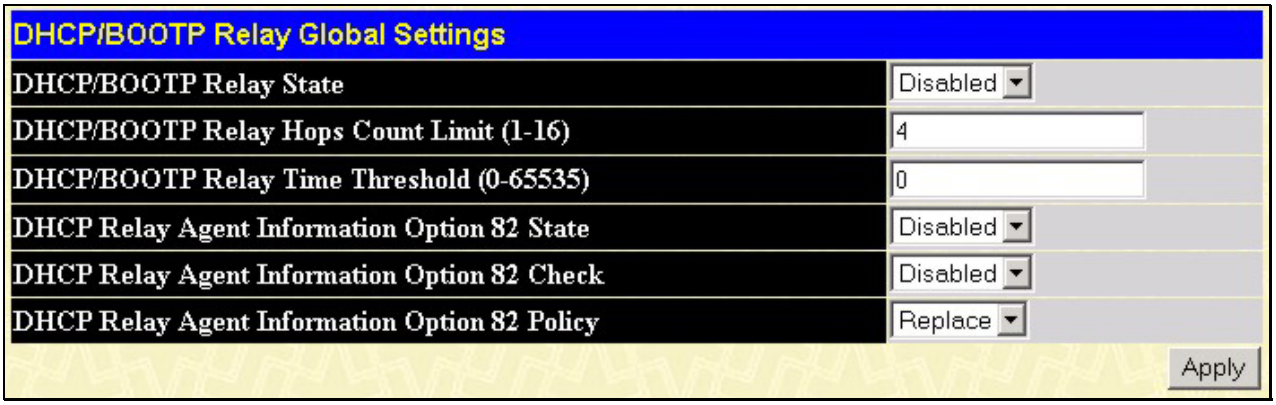


Figure 6- 44. DHCP/ BOOTP Relay Global Settings window

The following fields can be set:

Parameter	Description
Relay State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the DHCP/BOOTP Relay service on the Switch. The default is *Disabled*
Relay Hops Count Limit (1-16)	This field allows an entry between *1* and *16* to define the maximum number of router hops DHCP/BOOTP messages can be forwarded across. The default hop count is *4*.
Relay Time Threshold (0-65535)	Allows an entry between *0* and *65535* seconds, and defines the maximum time limit for routing a DHCP/BOOTP 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 Relay Agent Information Option 82 State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the DHCP Agent Information Option 82 on the Switch. The default is *Disabled.* *Enabled* –When this field is toggled to *Enabled* the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

	Disabled- If the field is toggled to *Disabled* the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.
DHCP Relay Agent Information Option 82 Check	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the Switches ability to check the validity of the packet's option 82 field. *Enabled*– When the field is toggled to *Enable*, the relay agent will check the validity of the packet's option 82 field. If the switch receives a packet that contains the option-82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages. *Disabled*- When the field is toggled to *Disabled*, the relay agent will not check the validity of the packet's option 82 field.
DHCP Relay Agent Information Option 82 Policy	This field can be toggled between *Replace, Drop,* and *Keep* by using the pull-down menu. It is used to set the Switches policy for handling packets when the **DHCP Relay Agent Information Option 82 Check** is set to *Disabled*. The default is *Replace.* *Replace* - The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. *Drop* - The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. *Keep* - The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.

Click **Apply** to implement any changes that have been made.

NOTE: If the Switch receives a packet that contains the option-82 field from a DHCP client and the information-checking feature is enabled, the Switch drops the packet because it is invalid. However, in some instances, users may configure a client with the option-82 field. In this situation, disable the information-check feature so that the Switch does not remove the option-82 field from the packet. Users may configure the action that the Switch takes when it receives a packet with existing option-82 information by configuring the **DHCP Agent Information Option 82 Policy.**

The Implementation of DHCP Information Option 82

The **config dhcp_relay option_82** command configures the DHCP relay agent information option 82 setting of the switch. The formats for the circuit ID sub-option and the remote ID sub-option are as follows:

NOTE: For the circuit ID sub-option of a standalone switch, the module field is always zero.

Circuit ID sub-option format:

1.	2.	3.	4.	5.	6.	7.
1	6	0	4	VLAN	Module	Port
1 byte	1 byte	1 byte	1 byte	2 bytes	1 byte	1 byte

a. Sub-option type
b. Length
c. Circuit ID type
d. Length
e. VLAN: the incoming VLAN ID of DHCP client packet.
f. Module: For a standalone switch, the Module is always 0; For a stackable switch, the Module is the Unit ID.
g. Port: The incoming port number of DHCP client packet, port number starts from 1.

Remote ID sub-option format:

1.	2.	3.	4.	5.
2	8	0	6	MAC address
1 byte	1 byte	1 byte	1 byte	6 bytes

1. Sub-option type
2. Length
3. Remote ID type
4. Length
5. MAC address: The Switch's system MAC address.

Figure 6- 45. Circuit ID and Remote ID Sub-option Format

DHCP/BOOTP Relay Interface Settings

The **DHCP/ BOOTP Relay Interface Settings** allow the user to set up a server, by IP address, for relaying DHCP/ BOOTP information. 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 under the **Apply** heading. The user may add up to four server IPs per IP interface on the Switch. Entries may be deleted by clicking the corresponding ✕ button. To enable and configure DHCP/BOOTP Relay Interface Settings on the Switch, **click L3 Features** > **DHCP/BOOTP Relay** > **DHCP/BOOTP Relay Interface Settings:**

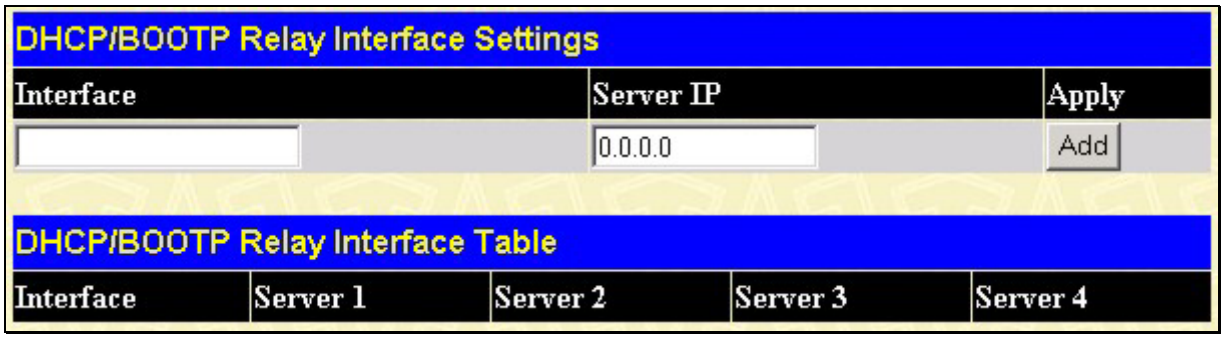


Figure 6- 46. DHCP/BOOTP Relay Interface Settings and Table window

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

Click **Add** to include this Server IP.

DHCP Auto Configuration Settings

This window is used to enable the DHCP Autoconfiguration feature on the Switch. When enabled, the Switch is instructed to receive a configuration file from a TFTP server, which will set the Switch to become a DHCP client automatically on boot up. To employ this method, the DHCP server must be set up to deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be up and running and hold the necessary configuration file stored in its base directory when the request is received from the Switch. For more information about loading a configuration file for use by a client, see the DHCP server and/or TFTP server software instructions. The user may also consult the Upload screen description located in the Maintenance section of this manual.

If the Switch is unable to complete the DHCP auto configuration, the previously saved configuration file present in the Switch's memory will be used.

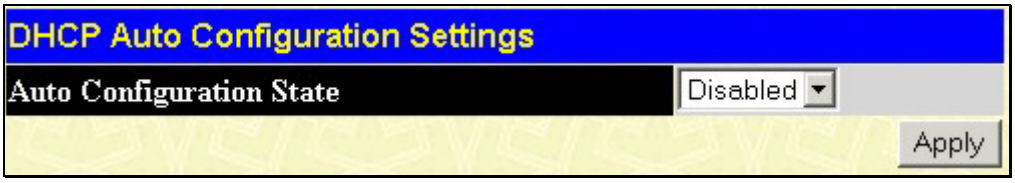


Figure 6- 47. DHCP Auto Configuration Settings window

To enable the **DHCP Auto Configuration State**, use the pull-down menu to choose Enabled and click the **Apply** button.

SNMP Manager

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 xStack DGS-3400 Series supports the SNMP versions 1, 2c, and 3. 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

The Switch in the Management Information Base (MIB) stores management and counter information. 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. Specifying the MIB Object Identifier may also retrieve the proprietary MIB. MIB values can be either read-only or read-write.

The xStack DGS-3400 Series 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 xStack DGS-3400 Series 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 Trap Settings

The following window is used to enable and disable trap settings for the SNMP function on the Switch. To view this window for configuration, click **Administration > SNMP Manager > SNMP Trap Settings**:

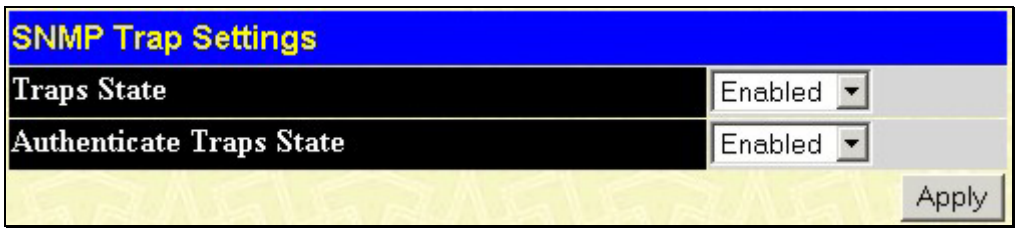


Figure 6- 48. SNMP Trap Settings window

To enable or disable the Traps State and/or the Authenticate Traps State, use the corresponding pull-down menu to change and click **Apply**.

SNMP User Table

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

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

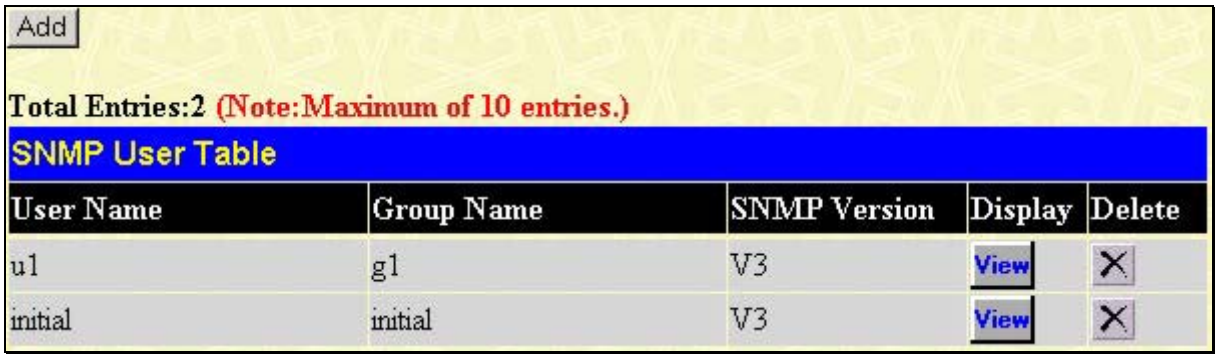


Figure 6- 49. SNMP User Table window

To delete an existing SNMP User Table entry, click the ✕ below the Delete heading corresponding to the entry to delete.

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

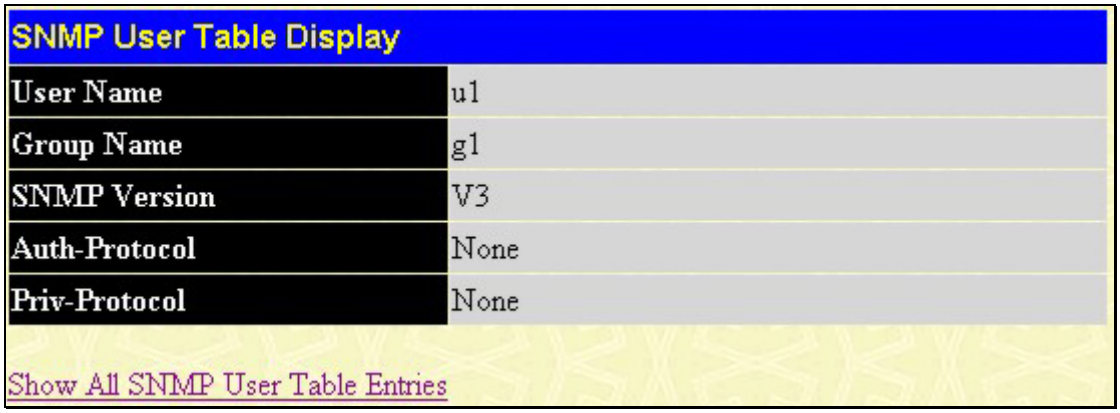


Figure 6- 50. SNMP User Table Display

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 authentication 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 privacy (encryption) 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, click the Show All SNMP User Table Entries link. To add a new entry to the **SNMP User Table Configuration** window, click on the **Add** button on the **SNMP User Table** window. This will open the **SNMP User Table Configuration** window, as shown below.

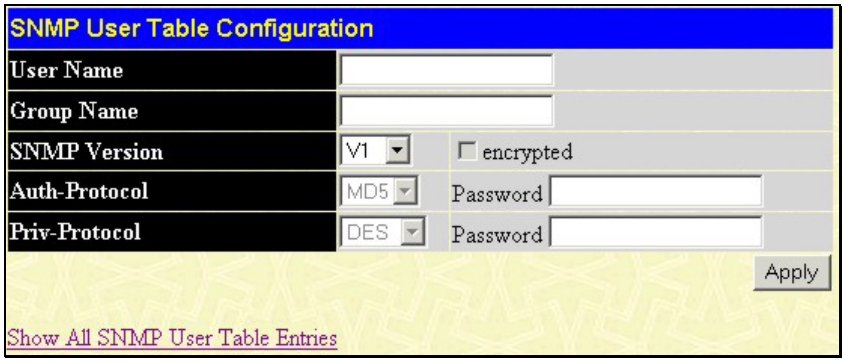


Figure 6- 51. SNMP User Table Configuration window

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* - Indicates that no privacy (encryption) 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 Encrypted 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, 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 **Administration** and click the **SNMP View Table** entry. The following window should appear:

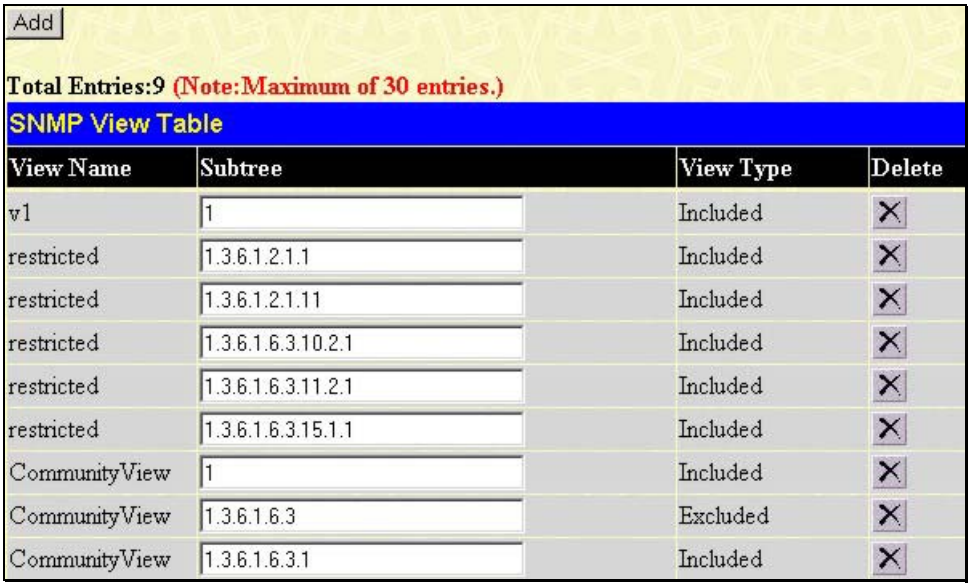


Figure 6- 52. SNMP View Table window

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

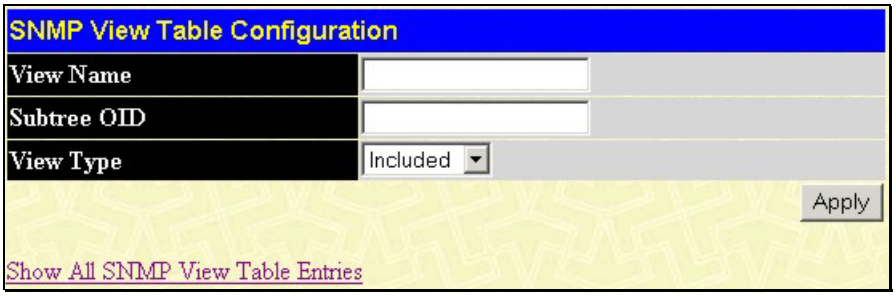


Figure 6- 53. SNMP View Table Configuration window

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

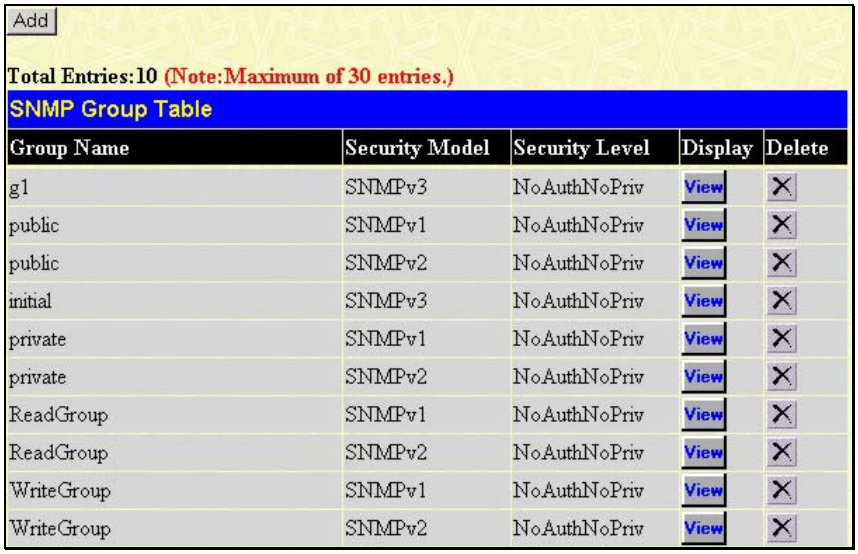


Figure 6- 54. SNMP Group Table window

To delete an existing SNMP Group Table entry, click the corresponding ✕ 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.

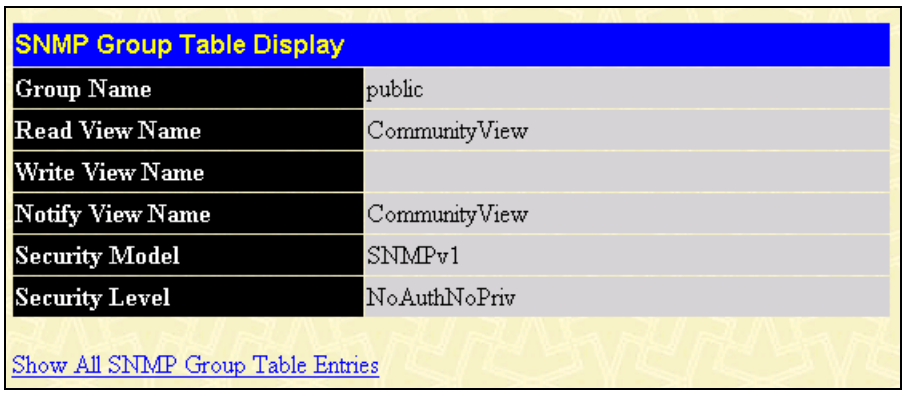


Figure 6- 55. SNMP Group Table Configuration window

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.

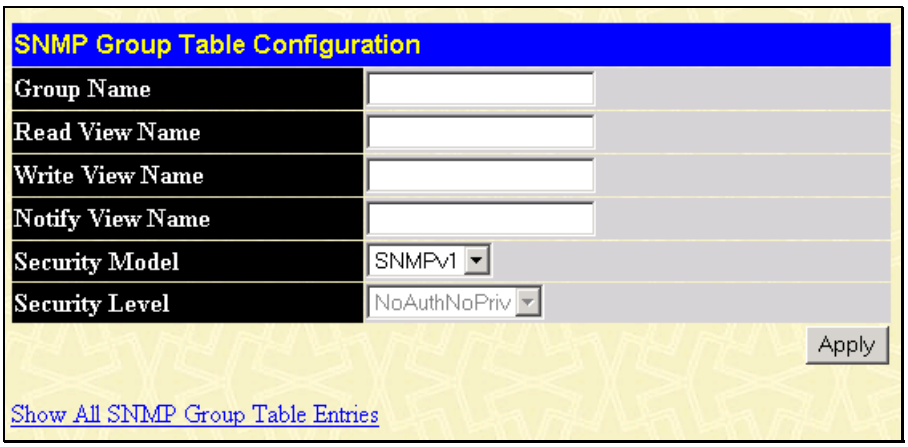


Figure 6- 56. SNMP Group Table Configuration window

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**, 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, (located in the **Administration** folder) and click the **SNMP Community Table** link, which will open the following window:

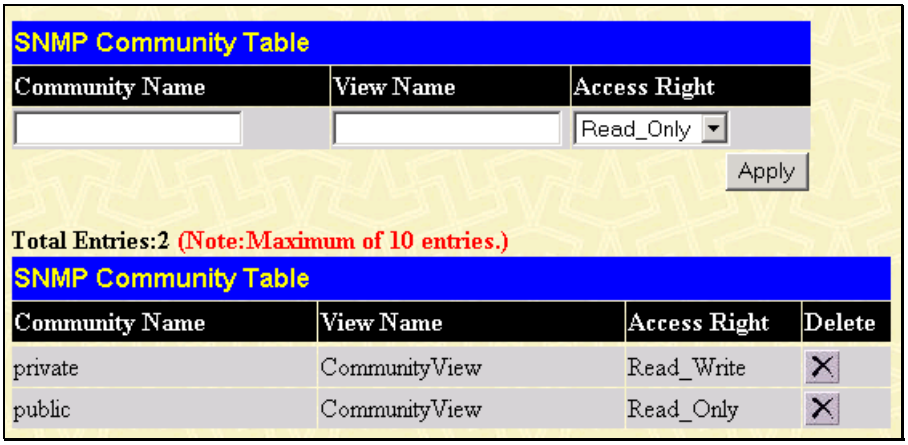


Figure 6- 57. SNMP Community Table Configuration window

The following parameters can set:

Parameter	Description
Community Name	Type an alphanumeric string of up to 32 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 ✕ under the Delete heading, corresponding to the entry to delete.

SNMP Host Table

Use the **SNMP Host Table** window to set up SNMP trap recipients. Open the **SNMP Manager** folder, (located in the **Administration** 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 ✕ under the Delete heading. To display the current settings for an existing **SNMP Group Table** entry, click the blue link for the entry under the Host IP Address heading.

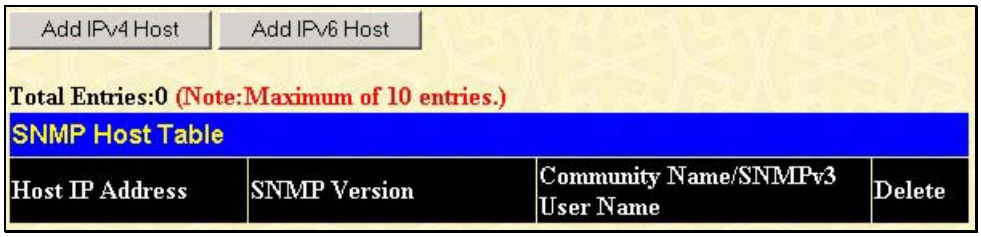


Figure 6- 58. SNMP Host Table window

Users now have the choice of adding an IPv4 or an IPv6 host to the SNMP host table. To add a new IPv4 entry to the Switch's SNMP Host Table, click the **Add IPv4 Host** button in the upper left-hand corner of the window. This will open the **SNMP Host Table Configuration** window, as shown below.

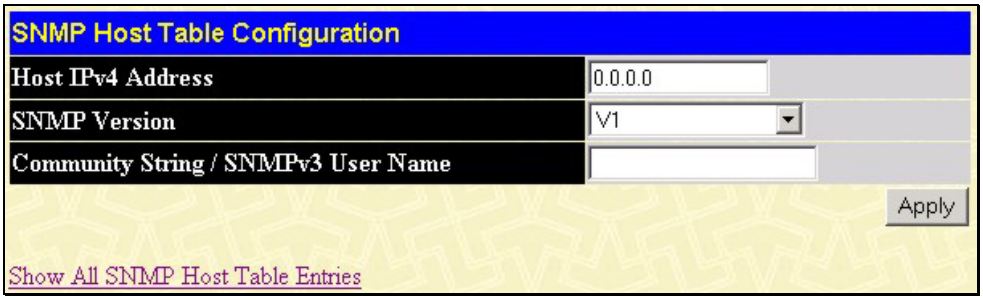


Figure 6- 59. SNMP IPv4 Host Table Configuration window

The following parameters can set:

Parameter	Description
Host IPv4 Address	Type the IPv4 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 an Auth-NoPriv security level. *V3-Auth-Priv* - To specify that the SNMP version 3 will be used, with an Auth-Priv security level.
Community String or SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

To add a new IPv6 entry to the Switch's SNMP Host Table, click the **Add IPv6 Host** button in the upper left-hand corner of the window. This will open the **SNMP Host Table Configuration** window, as shown below.

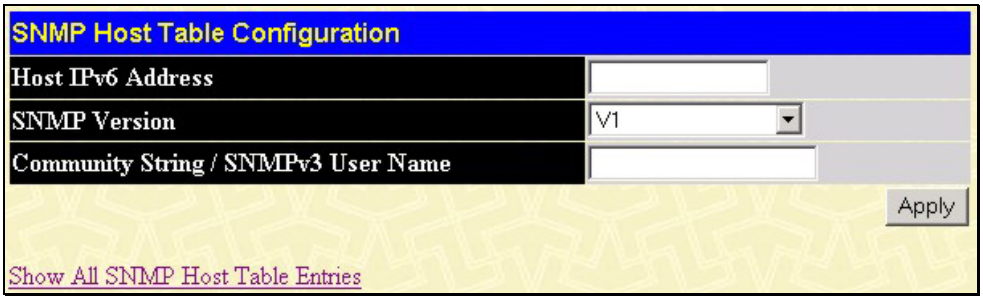


Figure 6- 60. SNMP IPv6 Host Table Configuration window

The following parameters can set:

Parameter	Description
Host IPv6 Address	Type the IPv6 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 an Auth-NoPriv security level. *V3-Auth-Priv* - To specify that the SNMP version 3 will be used, with an Auth-Priv security level.
Community String or SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

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, (located in the **Administration**) folder and click on the **SNMP Engine ID** link. This will open the **SNMP Engine ID Configuration** window, as shown below.

Figure 6- 61. SNMP Engine ID Configuration window

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

IP-MAC-Port Binding

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC addresses with the pre-configured database. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet. The maximum number of IP-MAC binding entries is dependant on chip capability (e.g. the ARP table size) and storage size of the device. For the xStack DGS-3400 Series switches, the maximum number of IP-MAC Binding entries is 500. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

ACL Mode

Due to some special cases that have arisen with the IP-MAC binding, this Switch has been equipped with a special ACL Mode for IP-MAC Binding, which should alleviate this problem for users. When enabled in the **IP-MAC Binding Port** window, the Switch will create two entries in the Access Profile Table as shown below. The entries may only be created if there are at least two Access Profile IDs available on the Switch. If not, when the ACL Mode is enabled, an error message will be prompted to the user. When the ACL Mode is enabled, the Switch will only accept IP packets from a created entry in the IP-MAC Binding Setting window. All others will be discarded.

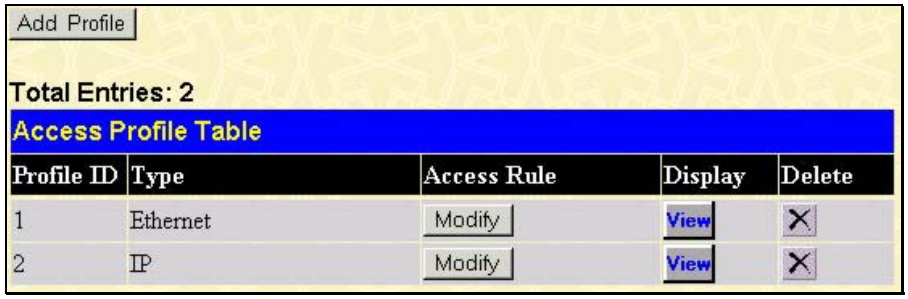


Figure 6- 62. Access Profile Table – IP-MAC-Port ACL Mode Enabled

To view the particular configurations associated with these two entries, click their corresponding **View** button, which will display the following:

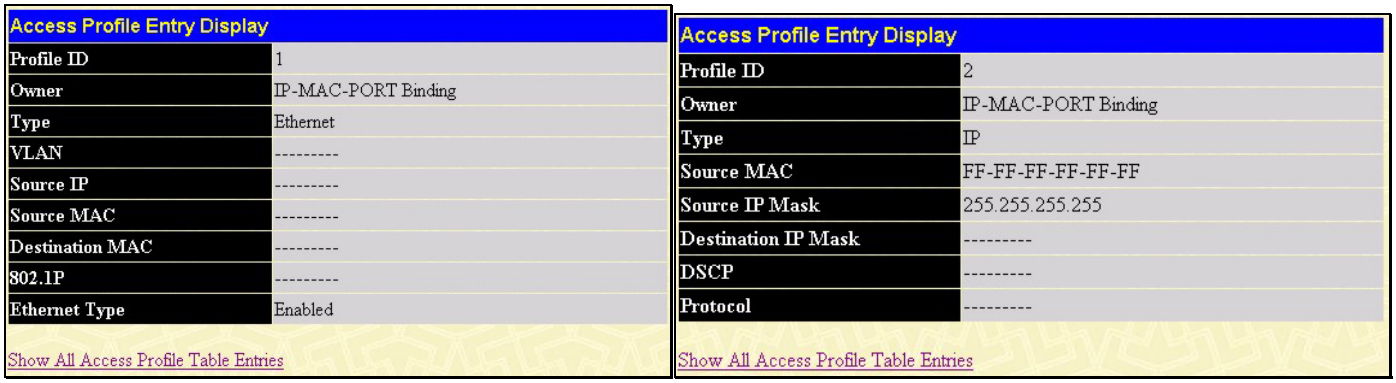


Figure 6- 63. Access Profile Entry Display for IP-MAC ACL Mode Enabled Entries

These two entries cannot be modified or deleted using the Access Profile Table. The user may only remove these two entries by disabling the ACL Mode in the IP-MAC Binding Port window.

Also, rules will be created for every port on the Switch. To view the ACL rule configurations set for the ACL mode, click the corresponding modify button of the entry in the Access Profile Table, which will produce a window similar to the example to the right. The user may view the configurations on a port-by-port basis by clicking the **View** button under the **Display** heading of the corresponding port entry. These entries cannot be modified or deleted, and new rules cannot be added. Yet, these windows will offer vital information to the user when configuring other access profile entries.

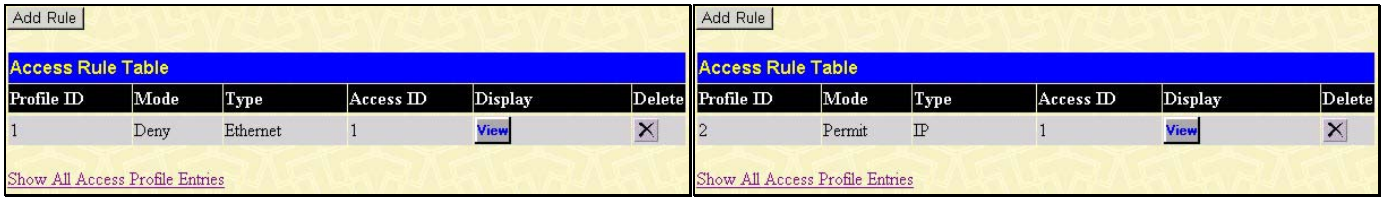


Figure 6- 64. Access Rule Tables for IP-MAC Binding rule

Access Rule Display	
Profile ID	1
Access ID	1
Mode	Deny
Type	Ethernet
Source IP	---------
Priority	------
VLAN Name	------
Source MAC	------
Destination MAC	------
802.1P	------
Ethernet Type	0x800
Port	1:1
Rx Rate(64Kbps)	------

Show All Access Rule Entries

Access Rule Display	
Profile ID	2
Access ID	1
Mode	Permit
Type	IP
Source MAC	00-90-27-39-40-95
Priority	------
Replace DSCP	------
Source IP	10.0.0.128
Destination IP	------
DSCP	------
Protocol	------
Port	1:1
Rx Rate(64Kbps)	No Limit

Show All Access Rule Entries

Figure 6- 65. Access Rule Display windows for IP MAC Binding

NOTE: When configuring the ACL mode function of the IP-MAC binding function, please pay close attention to previously set ACL entries. Since the ACL mode entries will fill the first two available access profiles and access profile IDs denote the ACL priority, the ACL mode entries may take precedence over other configured ACL entries. This may render some user-defined ACL parameters inoperable due to the overlapping of settings combined with the ACL entry priority (defined by profile ID). For more information on ACL settings, please see “Configuring the Access Profile” section mentioned previously in this chapter.

NOTE: Once ACL profiles have been created by the Switch through the IP-MAC binding function, the user cannot modify, delete or add ACL rules to these ACL mode access profile entries. Any attempt to modify, delete or add ACL rules will result in a configuration error as seen in the previous figure.

NOTE: When uploading configuration files to the Switch, be aware of the ACL configurations loaded, as compared to the ACL mode access profile entries set by this function, which may cause both access profile types to experience problems.

IP-MAC Binding Port

To enable or disable IP-MAC binding on specific ports, click **IP-MAC Binding Port** in the **IP-MAC-Port Binding** folder on the **Administration Menu** to open the **IP-MAC Binding Ports Settings** window. Select a port or a range of ports with the **From** and **To** fields. Enable or disable the port with the **State** field. The user must also enable ports in this window to set the ACL Mode for IP-MAC Binding, as previously stated. Click **Apply** to save changes.

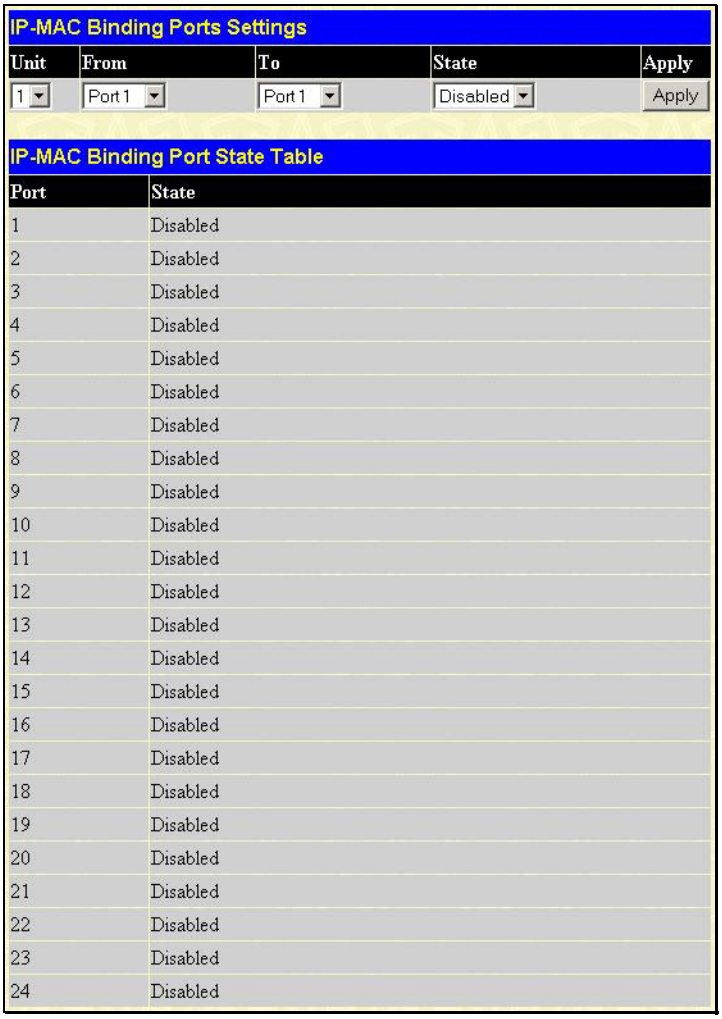


Figure 6- 66. IP-MAC Binding Ports window

IP-MAC Binding Table

The window shown below can be used to create IP-MAC binding entries. Click the **IP-MAC Binding Table** on the **IP-MAC-Port Binding** folder on the **Administration** menu to view the **IP-MAC Binding Settings** window. Enter the IP and MAC addresses of the authorized users in the appropriate fields and click **Add**. To modify either the IP address or the MAC address of the binding entry, make the desired changes in the appropriate field and Click **Modify**. To find an IP-MAC binding entry, enter the IP and MAC addresses and click **Find**. To delete an entry click **Delete**. To clear all the entries from the table click **Delete All**.

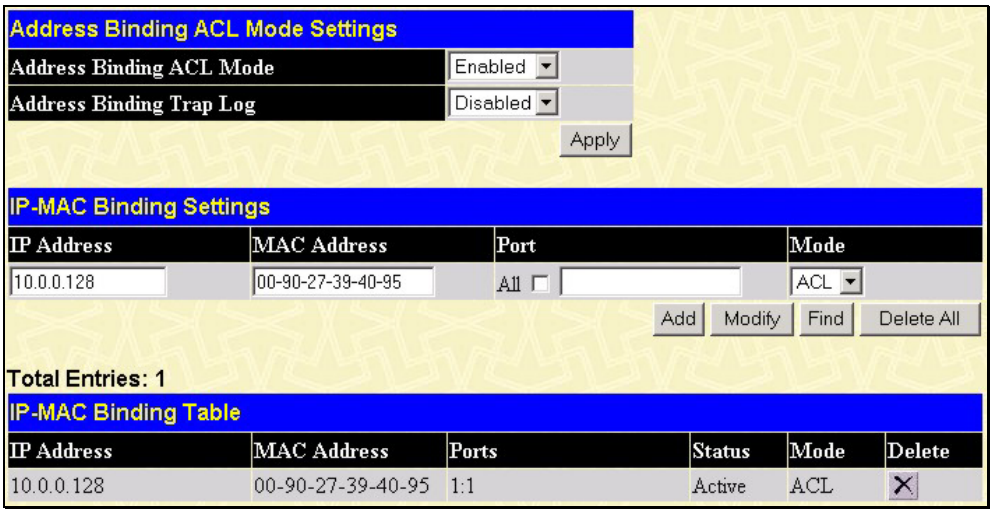


Figure 6- 67. IP-MAC Binding Table window

The following fields can be set or modified:

Parameter	Description
Address Binding ACL Mode	This field will enable and disable the ACL mode for IP-MAC binding on the Switch, without altering previously set configurations. When enabled, the Switch will automatically create two ACL packet content mask entries, which will aid the user in processing certain IP-MAC binding entries created. The ACL entries created when this command is enabled, can only be automatically installed if the Access Profile table has two entries available of the possible 255 entries allowed.
ACL Binding Trap Log	This field will enable and disable the sending of trap log messages for IP-MAC binding. When enabled, the Switch will send a trap log message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC binding configuration set on the Switch.
IP Address	Enter the IP address to bind to the MAC address set below.
MAC Address	Enter the MAC address to bind to the IP Address set above.
All Ports	Click this check box to configure this IP-MAC binding entry (IP Address + MAC Address) for all ports on the Switch.
Ports	Specify the switch ports for which to configure this IP-MAC binding entry (IP Address + MAC Address). Click the All check box to configure this entry for all ports on the Switch.
Mode	The user may set the IP-MAC Binding Mode here by using the pull-down menu. The choices are: *ARP* – Choosing this selection will set a normal IP-MAC Binding entry for the IP address and MAC address entered. *ACL* – Choosing this entry will allow only packets from the source IP-MAC binding entry created here. All other packets with a different IP address will be discarded by the Switch. This mode can only be used if the ACL Mode has been enabled in the IP-MAC Binding Ports window as seen previously.

IP-MAC Binding Blocked

To view unauthorized devices that have been blocked by IP-MAC binding restrictions open the **IP-MAC Binding Blocked** window show below. Click **IP-MAC Binding Blocked** in the **IP-MAC-Port Binding** folder on the **Administration** menu to open the **IP-MAC Binding Blocked** window.

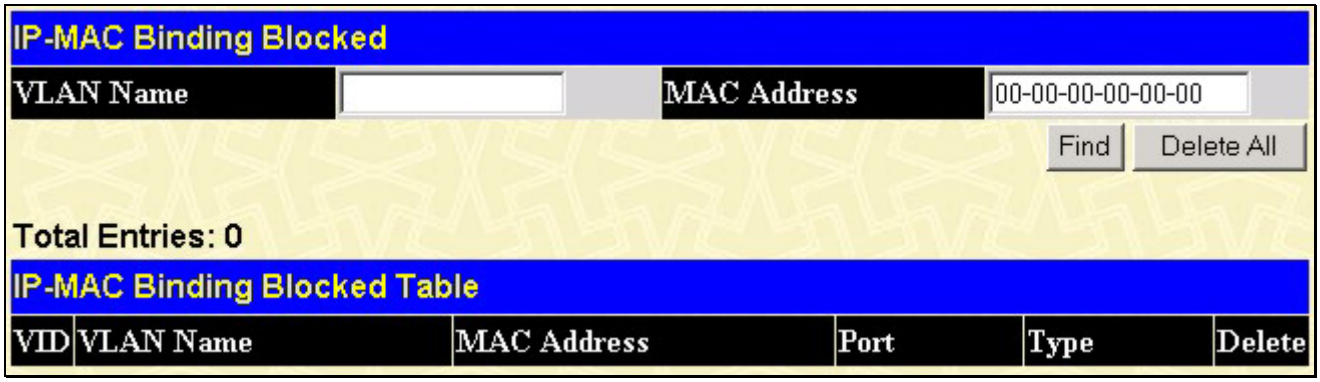


Figure 6- 68. IP-MAC Binding Blocked window

To find an unauthorized device that has been blocked by the IP-MAC binding restrictions, enter the **VLAN** name and **MAC Address** in the appropriate fields and click **Find**. To delete an entry click the delete button next to the entry's MAC address. To delete all the entries in the **IP-MAC Binding Blocked Table** click **Delete All**.

PoE Configuration

The DGS-3426P supports Power over Ethernet (PoE) as defined by the IEEE 802.3af specification. Ports 1-24 can supply 48 VDC power to Power Devices (PDs) over Category 5 or Category 3 UTP Ethernet cables. The DGS-3426P follows the standard PSE (Power Source over Ethernet) pinout *Alternative A*, whereby power is sent out over pins 1, 2, 3 and 6. The DGS-3426P works with all D-Link 802.3af capable devices. The Switch also works in PoE mode with all non-802.3af capable D-Link AP, IP Cam and IP phone equipment via DWL-P50.

The DGS-3426P includes the following PoE features:

- Auto-discovery recognizes the connection of a PD (Power Device) and automatically sends power to it.
- The Auto-disable feature will occur under two conditions: first, if the total power consumption exceeds the system power limit; and second, if the per port power consumption exceeds the per port power limit.
- Active circuit protection automatically disables the port if there is a short. Other ports will remain active.

PDs receive power according to the following classification:

Class	Max power used by PD
0	0.44 to 12.95W
1	0.44 to 3.84W
2	3.84 to 6.49W
3	6.49 to 12.95W

PSE provides power according to the following classification:

Class	Max power supplied by PSE
0	15.4W
1	4.0W
2	7.0W
3	15.4W

To configure the PoE features on the DGS-3426P, click **Administration** > **PoE Configuration**. The **PoE System** window is used to assign a power limit and power disconnect method for the whole PoE system. To configure the **Power Limit** for the PoE system, enter a value between 37W and 370W in the Power Limit field. The default setting is 370W. When the total consumed power exceeds the power limit, the PoE controller (located in the PSE) disconnects the power to prevent overloading the power supply.

PoE System Settings

To configure PoE for the Switch, click **Administration > PoE > PoE System Settings**, which will reveal the following window for the user to configure:

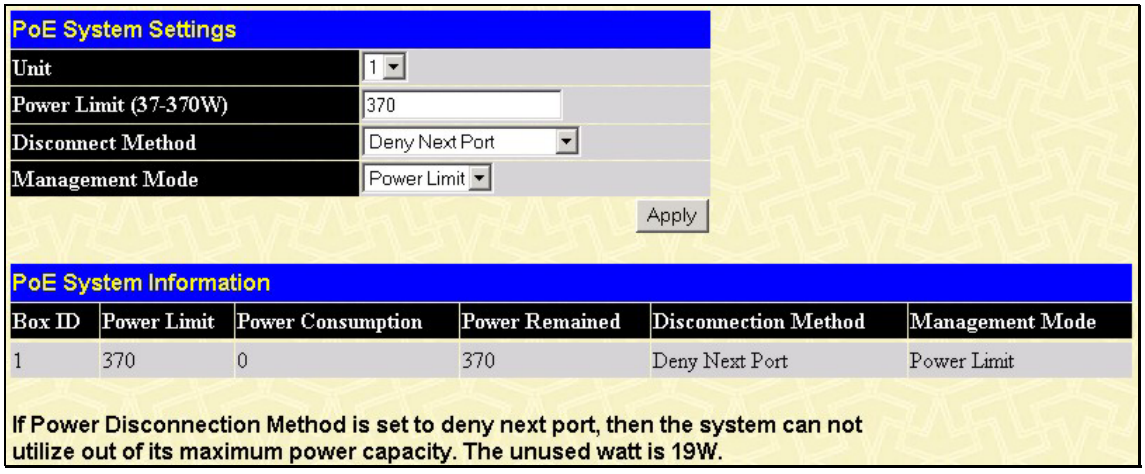


Figure 6- 69. PoE System Settings and Information window

The previous window contains the following fields to configure for PoE:

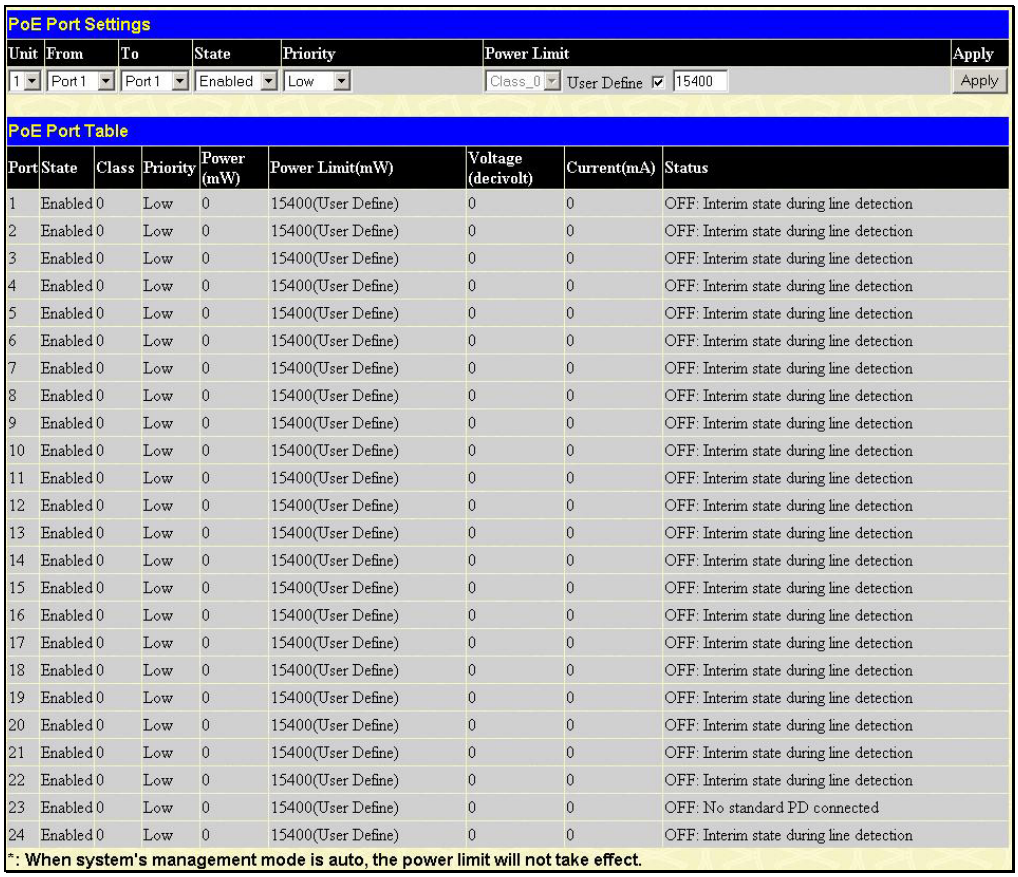
Parameter	Description
Unit	Choose the switch in the switch stack for which to configure the PoE settings. Users should note that not all switches in the xStack DGS-3400 series support PoE yet, when they are configured in a stack, the Primary Master switch will display the PoE settings to be configured for the stack, whether or not the Switch is a PoE supported device. However, only PoE supported switches have the PoE capability in the switch stack.

Power Limit	Sets the limit of power to be used from the Switch's power source to PoE ports. The user may configure a Power Limit between 37 and 370w.
Disconnect Method	The PoE controller uses either **Deny next port** or **Deny low priority port** to offset the power limit being exceeded and keep the Switch's power at a usable level. Use the drop down menu to select a **Power Disconnect Method**. The default for the Power Disconnect Method is **Deny next port**. Both Power Disconnection Methods are described below: **Deny next port** - After the power limit has been exceeded, the next port attempting to power up is denied, regardless of its priority. **Deny low priority port -** After the power limit has been exceeded, the next port attempting to power up causes the port with the lowest priority to shut down to allow the high-priority and critical priority ports to power up.
Management Mode	Use the pull-down menu to set the Management Mode for PoE ports. The user has two choices: *Power Limit* – Choose this option to shut down the port if the power limit on the port exceeds the limit stated by the user in the **Power Limit** field. *Auto* – Choose this field to automatically disconnect the power from a given port when it exceeds the maximum power used, as defined by the PD's (power device) power class, stated previously in this section. When a PD is attached to a port on the Switch, the Power Class is automatically determined. If the PD's power class is unspecified or there is an error in determining the power class, it is given the power class zero (0). Therefore, lets say a PD is connected to a PoE port and the power class determined is 1. If Auto is chosen and the wattage exceeds 3.84 watts, this port will automatically shut down.

Click **Apply** to implement changes made to the PoE System Settings.

PoE Port Settings

The following window will allow the user to configure PoE settings for each port of the device. To open this window, click **Administration > PoE > PoE Port Settings**.



PoE Port Settings

Unit	From	To	State	Priority	Power Limit			Apply
1	Port 1	Port 1	Enabled	Low	Class_0	User Define ☑	15400	Apply

PoE Port Table

Port	State	Class	Priority	Power (mW)	Power Limit(mW)	Voltage (decivolt)	Current(mA)	Status
1	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
2	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
3	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
4	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
5	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
6	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
7	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
8	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
9	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
10	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
11	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
12	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
13	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
14	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
15	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
16	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
17	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
18	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
19	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
20	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
21	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
22	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
23	Enabled	0	Low	0	15400(User Define)	0	0	OFF: No standard PD connected
24	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection

*: When system's management mode is auto, the power limit will not take effect.

Figure 6- 70. PoE Port Settings and Port Table window

The following parameters may be configured or modified for PoE Ports.

Parameter	Description
Unit	Choose the switch in the switch stack for which to configure the PoE port settings. Users should note that not all switches in the xStack DGS-3400 series support PoE yet, when they are configured in a stack, the Primary Master switch will display the PoE settings to be configured for the stack, whether or not the Switch is a PoE supported device. However, only PoE supported switches have the PoE capability in the switch stack.
From… To…	Select a range of ports from the pull-down menus to be enabled or disabled for PoE.
State	Use the pull-down menu to enable or disable ports for PoE.
Priority	Use the pull-down menu to select the priority of the PoE ports. There are three levels of priority, *Critical*, which is the highest, *High* and *Low*. The priority level will affect the order of supplying power to ports. This priority also affects the disconnect method of PoE ports when the *Deny Low Priority* option is chosen, and ports with a higher priority will take power precedence over low priority ports.
Power Limit	Sets the power limit per PoE port based on Class as described above. Once this threshold has been reached on the port, the PoE will go into the Power Disconnect Method, as described above. The user may alternatively set a limit between 1000 and 16800mW by clicking the User Define check box and manually entering a power limit in mW.

Click **Apply** to implement changes made. The port status of all PoE configured ports is displayed in the table in the bottom half of the screen above.

Single IP Management (SIM) Overview

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, which is a member of a SIM group. ***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 1-32), not 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 Management 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 xStack DGS-3400 Series switch 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 of the xStack DGS-3400 Series switch 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 Candidate state.
- CSs 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 xStack DGS-3400 Series switch may join the group 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.

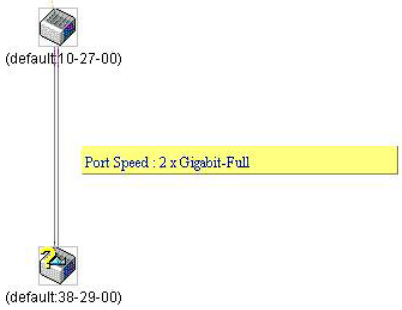
The Upgrade to v1.61

To better improve SIM management, the xStack DES-3400 series switches have been upgraded to version 1.61 in this release. Many improvements have been made, including:

1. The Commander Switch (CS) now has the capability to automatically rediscover member switches that have left the SIM group, either through a reboot or web malfunction. This feature is accomplished through the use of Discover packets and Maintenance packets that previously set SIM members will emit after a reboot. Once a MS has had its MAC address and password saved to the CS's database, if a reboot occurs in the MS, the CS will keep this MS information in its database and when a MS has been rediscovered, it will add the MS back into the SIM tree automatically. No configuration will be necessary to rediscover these switches.

There are some instances where pre-saved MS switches cannot be rediscovered. For example, if the Switch is still powered down, if it has become the member of another group, or if it has been configured to be a Commander Switch, the rediscovery process cannot occur.

2. The topology map now includes new features for connections that are a member of a port trunking group. It will display the speed and number of Ethernet connections creating this port trunk group, as shown in the adjacent picture.



3. This version will support switch upload and downloads for firmware, configuration files and log files, as follows:

Firmware – The switch now supports MS firmware downloads from a TFTP server.

Configuration Files – This switch now supports downloading and uploading of configuration files both to (for configuration restoration) and from (for configuration backup) MS's, using a TFTP server..

Log – The Switch now supports uploading MS log files to a TFTP server.

4. The user may zoom in and zoom out when utilizing the topology window to get a better, more defined view of the configurations.

NOTE: SIM Management does not support IPv6. For users wishing to utilize this function, switches in the SIM group must be configured with IPv4 addresses. IPv6 for SIM management will be supported in a future release of this switch.

Single IP vs. Switch Stacking

Single IP and Switch Stacking are two different entities and should not be equated by users. Within a switch stack, all functions are shared among switches in the stack and this switch stack is treated as one switch. Layer 2 and Layer 3 features, such as VLAN configurations and packet routing can be configured across switches in the stack. For example, mirroring functions can be shared within the stack, so a mirror target port may be on one switch in the stack and the source ports may be on another.

For Single IP Management, switches are separate entities that share a common IP address. Therefore, Layer 2 and Layer 3 functions CANNOT be shared among switches in the Single IP group. The purpose of the Single IP Management function is to share firmware and configuration files among switches within the Single IP Group. To have similar configurations on switches within the Single IP Group, users can upload identical configuration files to the Single IP Group using the **Configuration File Backup/Restore** window located under the the Single IP heading on the switch, and described later in this section. Once this file is entered and uploaded to switches within the group, most configurations should be the same for the switches in the Single IP Group.

SIM Using the Web Interface

All xStack DGS-3400 Series Switches are set as Candidate (CaS) switches as their factory default configuration and Single IP Management will be disabled. To enable SIM for the Switch using the Web interface, go to the **Single IP Management Settings** folder and click the **SIM Settings** link, revealing the following window.

Figure 6- 71. SIM Settings window (disabled)

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

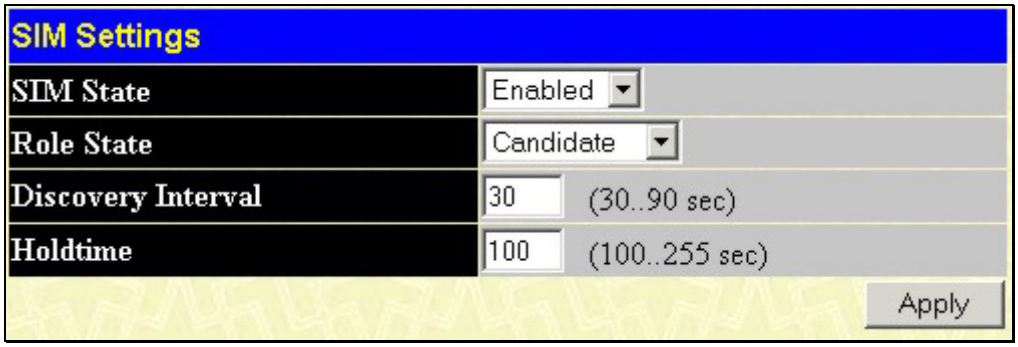


Figure 6- 72. SIM Settings window (enabled)

Parameter	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 DGS-3400 Series. *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**, **Configuration Backup/Restore** and **Upload Log**.

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 Java Runtime Environment on your server should initiate and lead you to the topology window, as seen below.

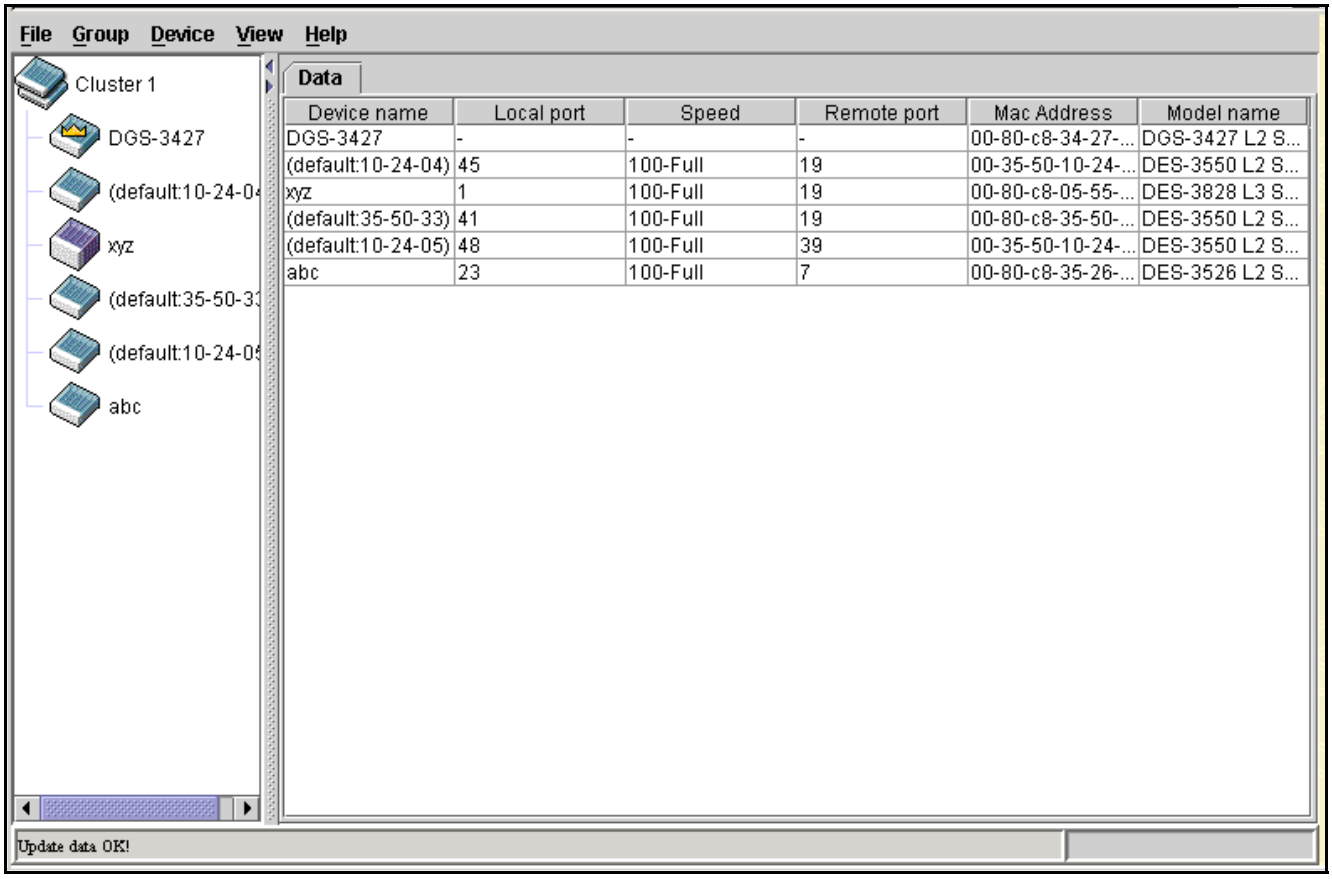


Figure 6- 73. Single IP Management window - Tree View

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 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 to which the CS is connected. 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 screen. The **Topology View** will refresh itself periodically (20 seconds by default).

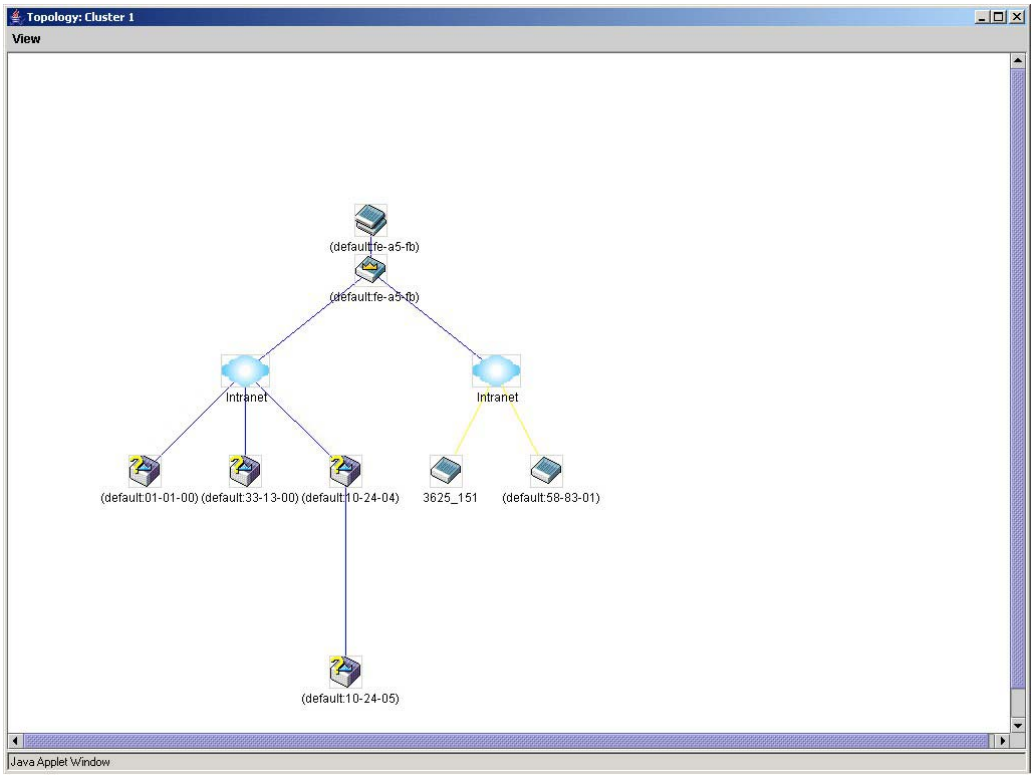
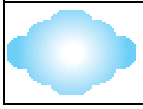


Figure 6- 74. Topology view

This screen will display how the devices within the Single IP Management Group connect 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.

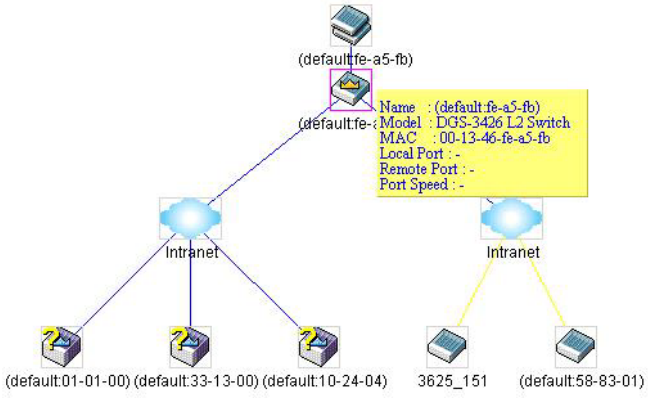


Figure 6- 75. Device Information Utilizing the Tool Tip

Setting the mouse cursor over a line between two devices will display the connection speed between the two devices, as shown below.

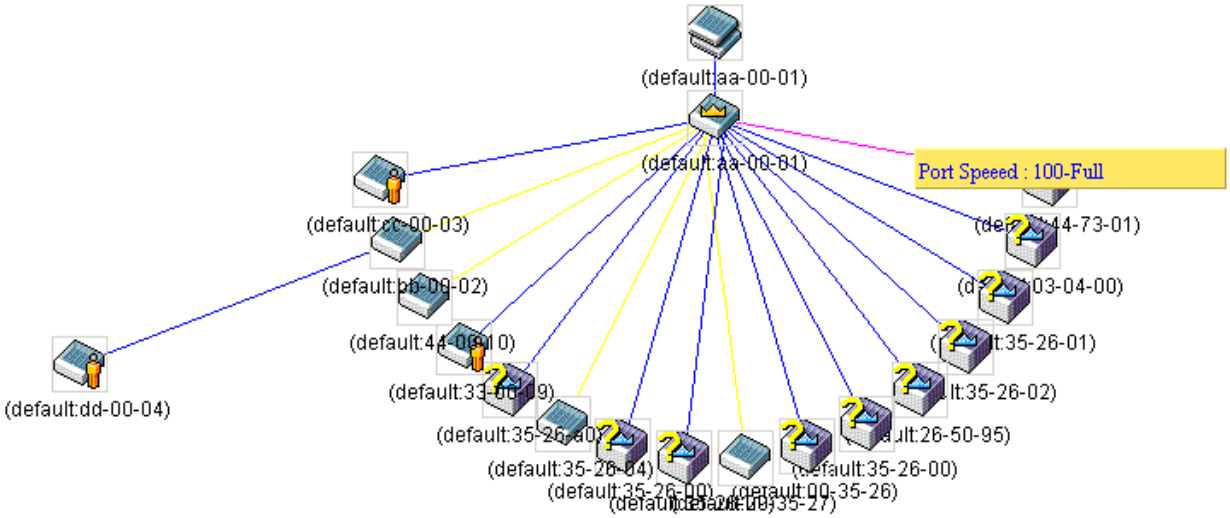


Figure 6- 76. Port Speed Utilizing the Tool Tip

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

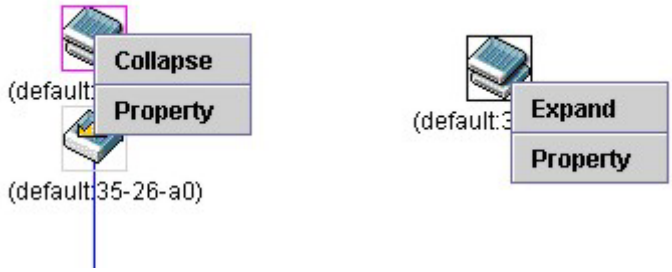


Figure 6- 77. Right Clicking a Group Icon

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.

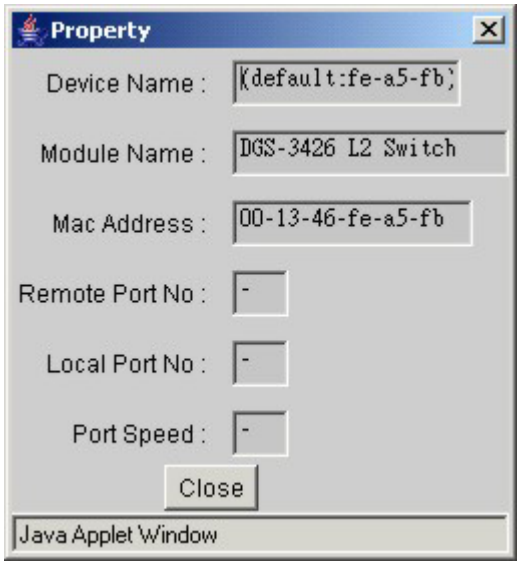


Figure 6- 78. Property window

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

Commander Switch Icon

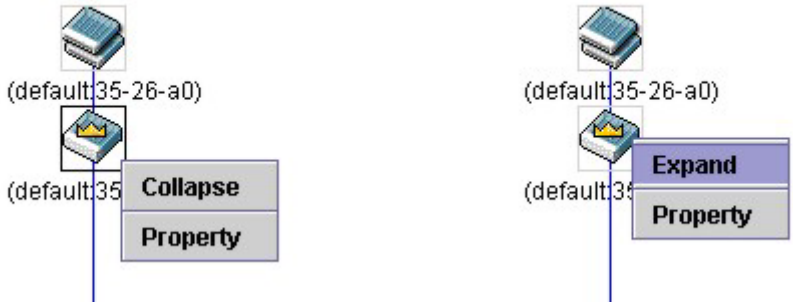


Figure 6- 79. Right Clicking a Commander Icon

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.

Member Switch Icon

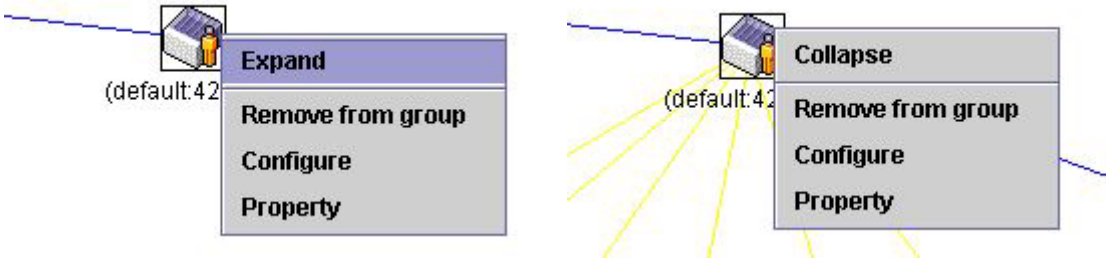


Figure 6- 80. Right Clicking a Member icon

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.

Candidate Switch Icon

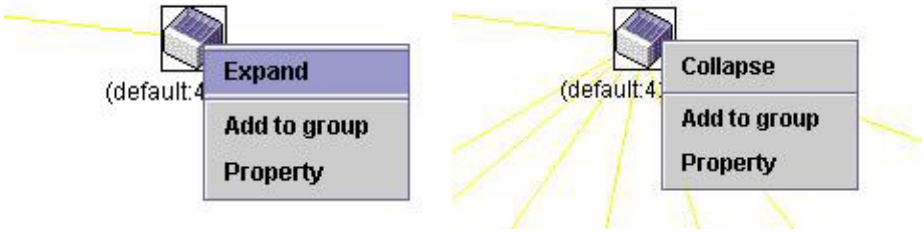


Figure 6- 81. Right Clicking a Candidate icon

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 6- 82. Input password window.

- **Property** - to pop up a window to display the device information.

Menu Bar

The **Single IP Management** window contains a menu bar for device configurations, as seen below.

Figure 6- 83. 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 6- 84. 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.

Section 7

Layer 2 Features

VLANs

Trunking

IGMP Snooping

MLD Snooping

Spanning Tree

Forwarding and Filtering

The following section will aid the user in configuring security functions for the Switch. The Switch includes various functions for VLAN, Trunking, IGMP Snooping, MLD Snooping, Spanning Tree, and Forwarding & Filtering, all discussed in detail in the following section.

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 comply 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 7, 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.

Strict mode and weighted round robin system are 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 7, 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 DGS-3400 Series

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 xStack DGS-3400 Series 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.

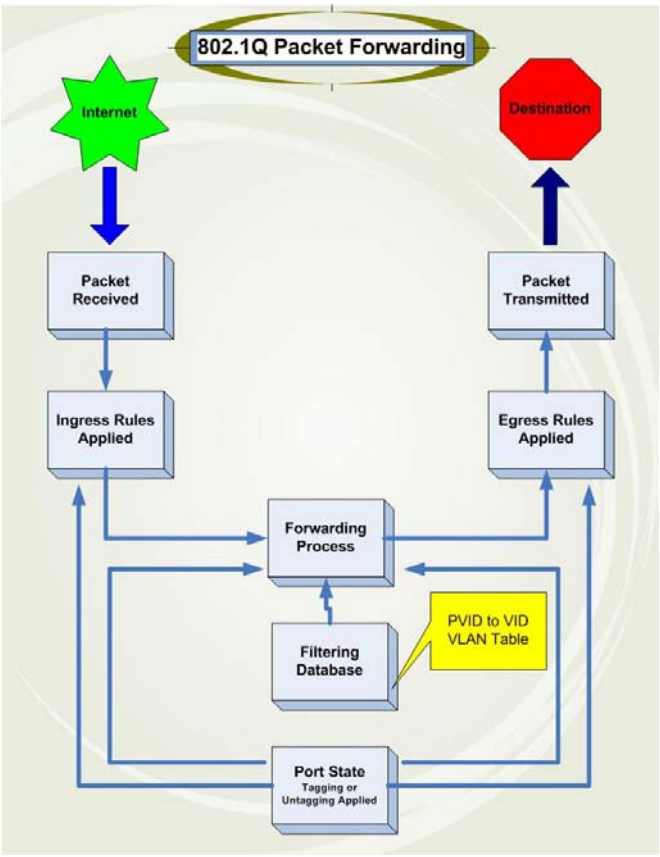


Figure 7- 1. IEEE 802.1Q Packet Forwarding

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.

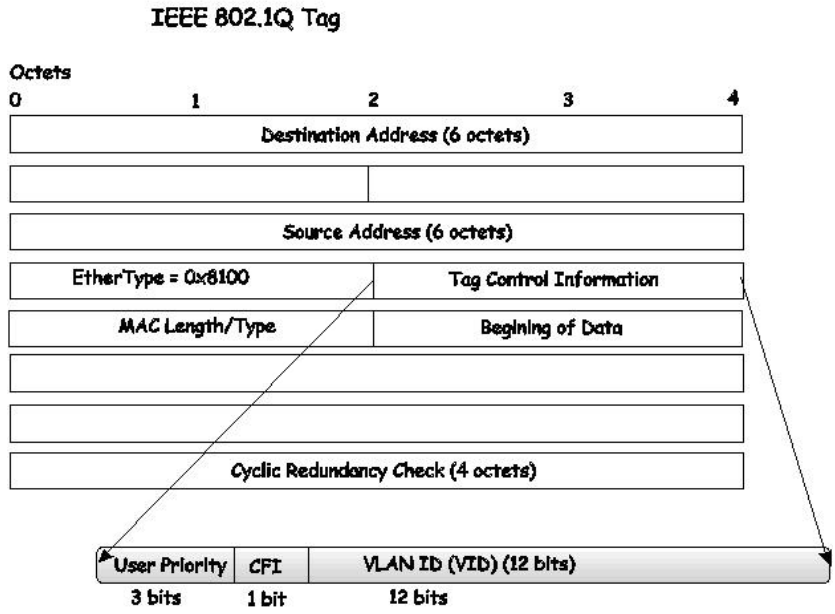


Figure 7- 2. IEEE 802.1Q Tag

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.

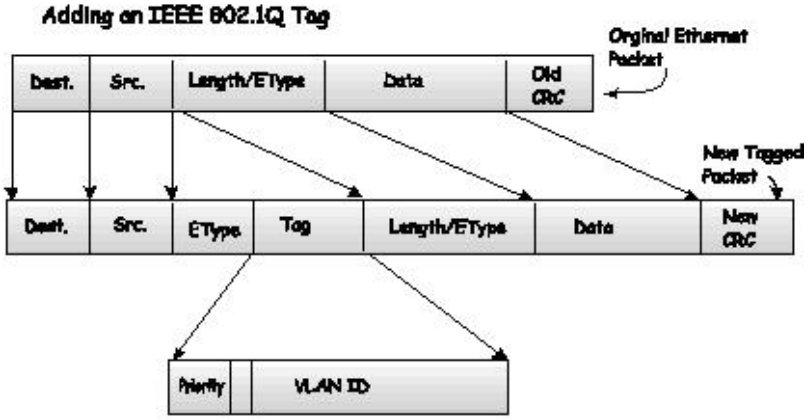


Figure 7- 3. Adding an IEEE 802.1Q Tag

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. Other 802.1Q compliant devices on the network to make packet-forwarding decisions can then use the VLAN information in the tag.

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 7- 1. 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.

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, first set the port trunk group(s), and then configure the VLAN settings. To change the port trunk grouping with VLANs already in place it is unnecessary 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 xStack DGS -3400 Switch Series 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 fourteen (14) pre-defined protocols for configuration. The user may also choose a protocol that is not one of the fourteen defined protocols by properly configuring the *userDefined* protocol VLAN. The supported protocols for the protocol VLAN function on this switch include IP, IPX, 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 Hexadecimal Form
IP over Ethernet	0x0800
IPX 802.3	0xFFFF
IPX 802.2	0xE0E0
IPX SNAP	0x8137
IPX over Ethernet2	0x8137
DEC LAT	0x6004
SNA 802.2	0x0404
netBios	0xF0F0
XNS	0x0600
VINES	0x0BAD
IPv6	0x86DD
AppleTalk	0x809B
RARP	0x8035
SNA over Ethernet2	0x80D5

Table 7- 2. 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 which to forward packets.

Static VLAN Entry

In the **Layer 2 Features** folder, click **VLAN > Static VLAN Entries** to open the following window:

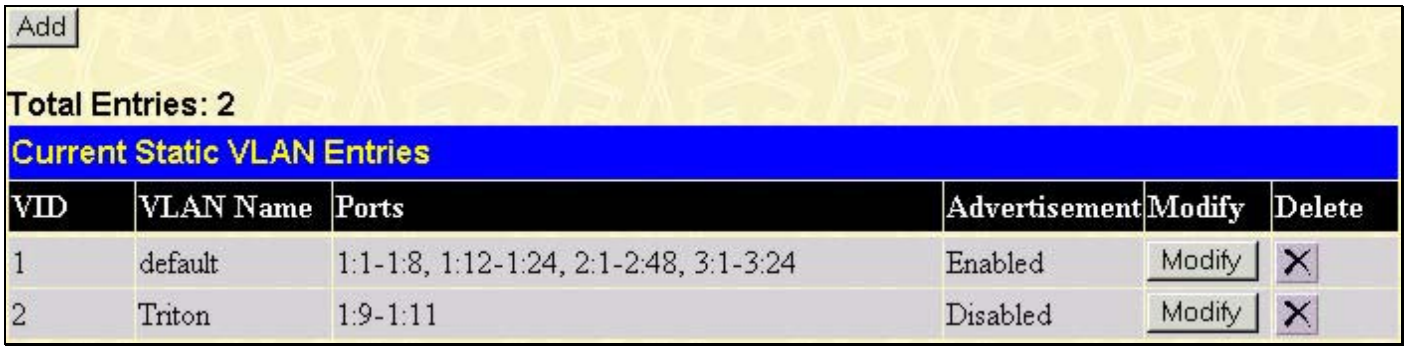


Figure 7- 4. Current Static VLAN Entries window

The **Current Static VLAN Entries** 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 **Current Static VLAN Entries** window. 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.

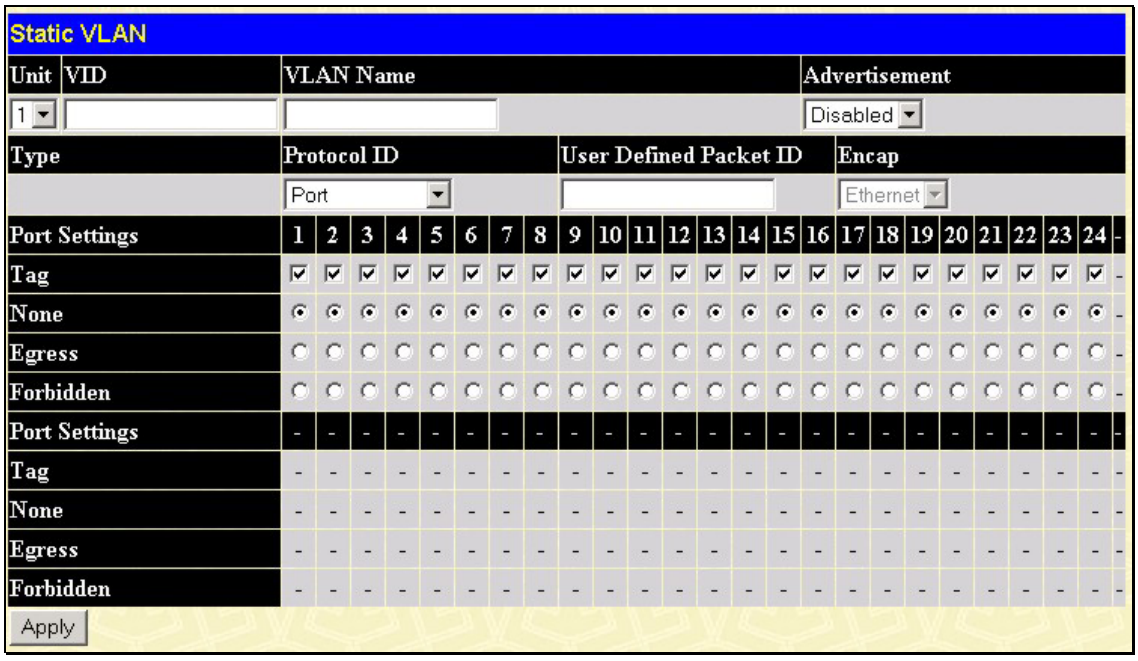


Figure 7- 5. Static VLAN window - Add

To return to the **Current 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 to modify. A new menu 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 menu.

NOTE: The Switch supports up to 4k static VLAN entries.

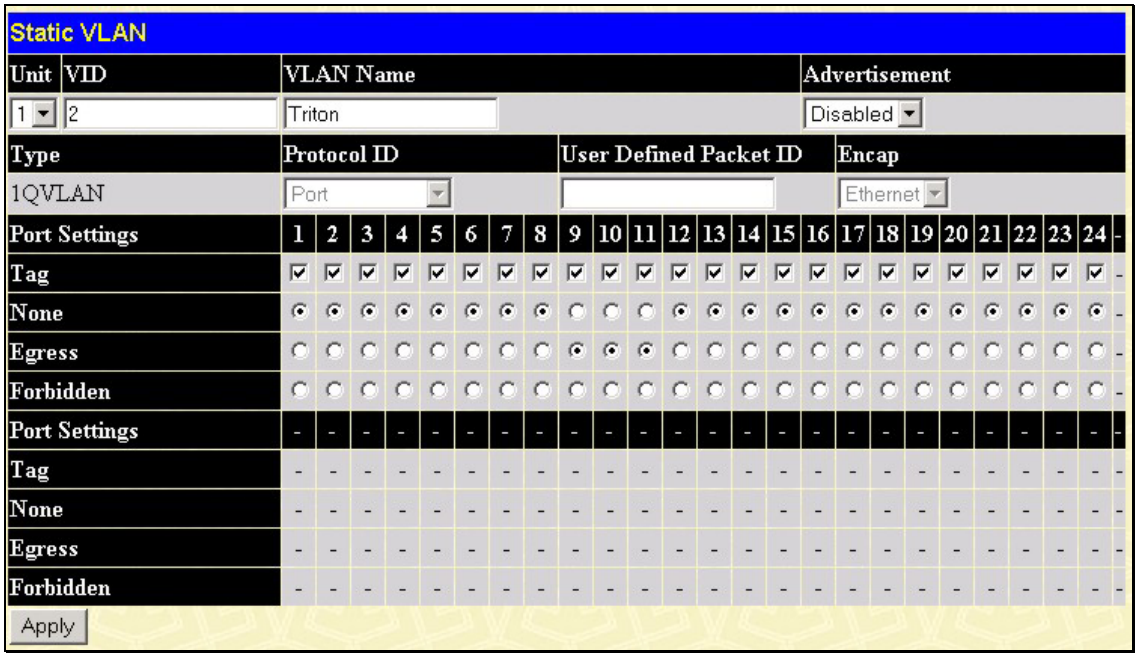


Figure 7- 6. Static VLAN window - Modify

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

Parameter	Description
Unit	Select the switch in the switch stack for which to configure VLANs.
VID (VLAN ID)	Allows the entry of a VLAN ID in the Add window, or displays the VLAN ID of an existing VLAN in the Modify window. 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 window, or for editing the VLAN name in the Modify window.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Type	Displays the type of protocol associated with this VLAN.
Protocol ID	The following parameters allow for the creation of protocol-based VLANs. The Switch supports 14 pre-configured protocol-based VLANs plus one user-defined protocol based VLAN and one user defined packet ID setting where the administrator may configure the settings for the appropriate protocol or ID for forwarding 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. *IPX 802.3* - 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). *IPX 802.2* - 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). *IPX SNAP* - 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). *IPX Ethernet2* - 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 Ethernet II Protocol. *Apple Talk* - 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. *DEC LAT* - 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. *SNA 802.2* - 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. *SNA Ethernet2* - 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) Ethernet II Protocol. *Net Bios* - 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 Integrated 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. *User Defined* - 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 hexadecimal form (ffff) to define the packet identification. *(The user only need enter the final four integers of the hexadecimal format to define the packet ID – {hex 0x0 0xffff})* This field is only operable if *userDefined* is selected in the Protocol ID field. *Encap [Ethernet | LLC | SNAP | All]* – 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 hexadecimal 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 **Administration** menu, open the **VLAN** folder and click **GVRP Settings**. 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.

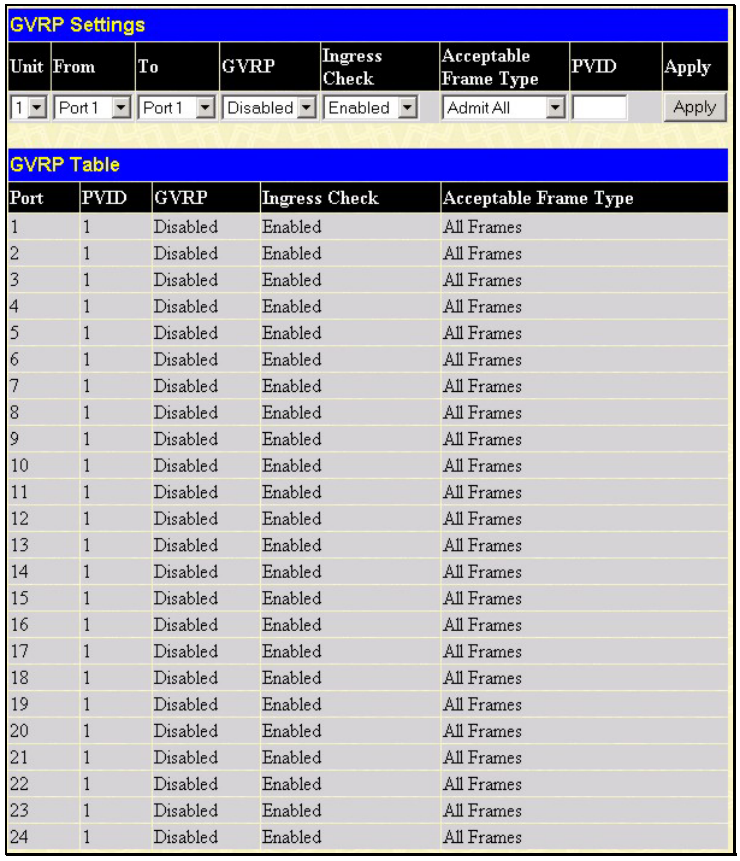


Figure 7- 7. GVRP Settings window

Click **Apply** to implement changes made. See table below for description of parameters.

The following fields can be set:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
From/To	These two fields allows the range of ports that will be included in the Port-based VLAN created using the 802.1Q Port Settings window, to be specified.
GVRP	The GARP 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 *Enabled* 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 mean both tagged and untagged frames will be accepted. *Admit_All* is enabled by default.
PVID	The read-only field in the 802.1Q Port Table 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 the port receives a packet, 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.

Double VLANs

Double or Q-in-Q VLANs allow network providers to expand their VLAN configurations to place customer VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for their customers, which will connect two or more customer LAN points without over-complicating configurations on the client's side. Not only will over-complication be avoided, but also now the administrator has over 4000 VLANs in which over 4000 VLANs can be placed, therefore greatly expanding the VLAN network and enabling greater support of customers utilizing multiple VLANs on the network.

Double VLANs are basically VLAN tags placed within existing IEEE 802.1Q VLANs which we will call SPVIDs (Service Provider VLAN IDs). These VLANs are marked by a TPID (Tagged Protocol ID), configured in hex form to be encapsulated within the VLAN tag of the packet. This identifies the packet as double-tagged and segregates it from other VLANs on the network, therefore creating a hierarchy of VLANs within a single packet.

Here is an example Double VLAN tagged packet.

Destination Address	Source Address	SPVLAN (TPID + Service Provider VLAN Tag)	802.1Q CEVLAN Tag (TPID + Customer VLAN Tag)	Ether Type	Payload

Consider the example below:

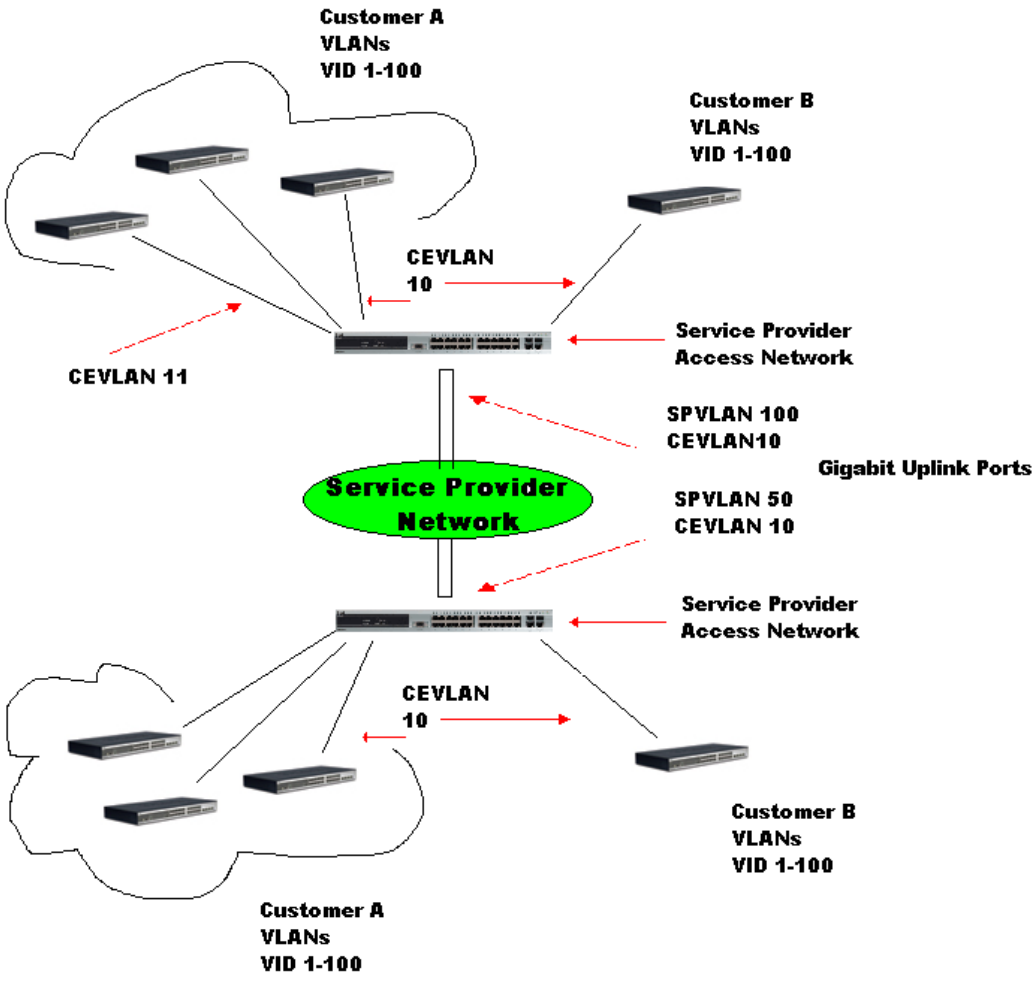


Figure 7- 8. Double VLAN Example

In this example, the Service Provider Access Network switch (Provider edge switch) is the device creating and configuring Double VLANs. Both CEVLANs (Customer VLANs) 10 and 11, are tagged with the SPVID 100 on the Service Provider Access Network and therefore belong to one VLAN on the Service Provider's network, thus being a member of two VLANs. In this way, the Customer can retain its normal VLAN and the Service Provider can congregate multiple Customer VLANs within one SPVLAN, thus greatly regulating traffic and routing on the Service Provider switch. This information is then routed to the Service Provider's main network and regarded there as one VLAN, with one set of protocols and one routing behavior.

Regulations for Double VLANs

Some rules and regulations apply with the implementation of the Double VLAN procedure.

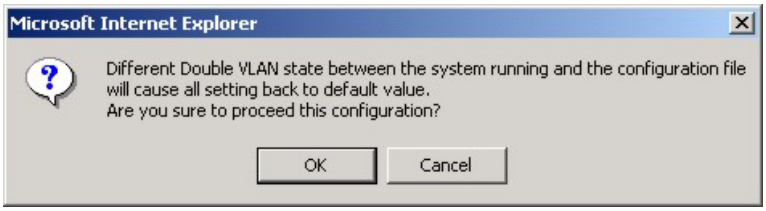
1. All ports must be configured for the SPVID and its corresponding TPID on the Service Provider's edge switch.
2. All ports must be configured as Access Ports or Uplink ports. Access ports can only be Ethernet ports while Uplink ports must be Gigabit ports.
3. Provider Edge switches must allow frames of at least 1522 bytes or more, due to the addition of the SPVID tag.
4. Access Ports must be an un-tagged port of the service provider VLANs. Uplink Ports must be a tagged port of the service provider VLANs.
5. The switch cannot have both double and normal VLANs co-existing. Once the change of VLAN is made, all Access Control lists are cleared and must be reconfigured.
6. Once Double VLANs are enabled, GVRP must be disabled.
7. All packets sent from the CPU to the Access ports must be untagged.
8. The following functions will not operate when the switch is in Double VLAN mode:
    - Guest VLANs
    - Web-based Access Control
    - IP Multicast Routing
    - GVRP
    - All Regular 802.1Q VLAN functions

Double VLAN

In the **L2 Features** menu, open the **VLAN** folder and click **Double VLAN Settings**, which will display the following window to enable the Double VLAN feature.

Figure 7- 9. Double VLAN State Settings

Choose *Enabled* using the pull-down menu and click **Apply**. The user will be prompted with the following warning window. Click **OK** to continue.



After being prompted with a success message, the user will be presented with this window to configure for Double VLANs.

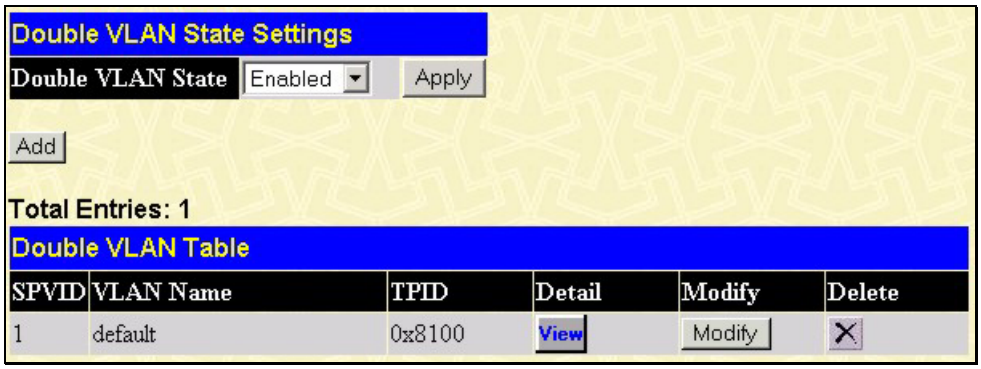


Figure 7- 10. Double VLAN Table

Parameters shown in the previous window are explained below:

Parameter	Description
Double VLAN State	Use the pull-down menu to enable or disable the Double VLAN function on this Switch. Enabling the Double VLAN will return all previous VLAN configurations to the factory default settings and remove Static VLAN configurations from the GUI.
SPVID	The VLAN ID number of this potential Service Provider VLAN.
VLAN Name	The name of the VLAN on the Switch.
TPID	The tagged protocol ID of the corresponding VLAN that will be used in identification of this potential Double VLAN, written in hex form.

The user may view configurations for a Double VLAN by clicking its corresponding View button, which will display the following read-only window.

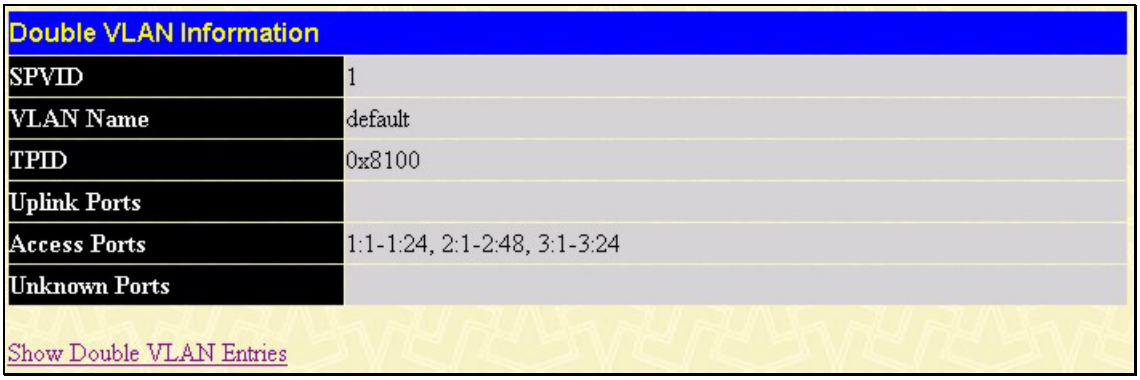


Figure 7- 11. Double VLAN Information window

Parameters shown in the previous window are explained below:

Parameter	Description
SPVID	The VLAN ID number of this potential Service Provider VLAN.
VLAN Name	The name of the VLAN on the Switch.
TPID	The tagged protocol ID of the corresponding VLAN that will be used in identification of this potential Double VLAN, written in hex form.
Uplink Ports	These ports are set as uplink ports on the Switch. Uplink ports are for connecting Switch VLANs to the Service Provider VLANs on a remote source. Only gigabit ports can be configured as uplink ports.
Access Ports	These are the ports that are set as access ports on the Switch. Access ports are for connecting Switch VLANs to customer VLANs. Gigabit ports cannot be configured as access ports.
Unknown Ports	These are the ports that are a part of the VLAN but have yet to be defined as Access or Uplink ports.

To create a Double VLAN, click the **Add** button, revealing the following window for the user to configure.

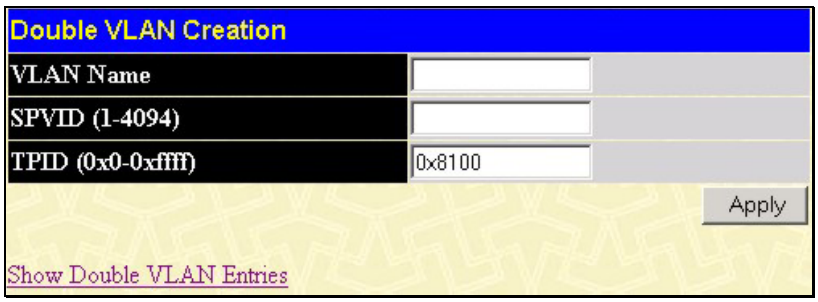


Figure 7- 12. Double VLAN Creation

To create a Double VLAN, enter the following parameters and click **Apply**.

Parameter	Description
VLAN Name	Enter the pre-configured VLAN name to create as a Double VLAN.
SPVID	Enter the VID for the Service Provider VLAN with an integer between 1 and 4094.
TPID	Enter the TPID in hex form to aid in packet identification of the Service Provider VLAN.

Click **Apply** to implement changes made.

To configure the parameters for a previously created Service Provider VLAN, click the Modify button of the corresponding SPVID in the **Double VLAN Table** as shown in Figure 7-10. The following window will appear for the user to configure.

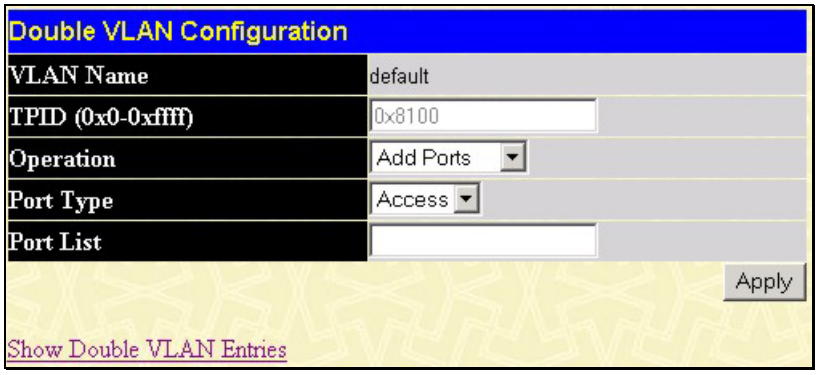


Figure 7- 13. Double VLAN Configuration

To configure a Double VLAN, enter the following parameters and click **Apply**.

Parameter	Description
VLAN Name	The name of the pre-configured VLAN name to be configured.
TPID	The tagged protocol ID. Enter the new TPID in hex form to aid in packet identification of the Service Provider VLAN.
Operation	Allows one of the following three acts to be performed: *Add ports* – Will allow users to add ports to this Service Provider VLAN using the Port List field below. *Delete ports* – Will allow users to remove ports from the Service Provider VLAN configured, using the Port List field below. *Config TPID* – Will allow users to configure the Tagged Protocol ID of the Service Provider VLAN, in hex form.
Port Type	Allows the user to choose the type of port being utilized by the Service Provider VLAN. The user may choose: *Access* - Access ports are for connecting Switch VLANs to customer VLANs. Gigabit ports cannot be configured as access ports. *Uplink* - Uplink ports are for connecting Switch VLANs to the Provider VLANs on a remote source. Only gigabit ports can be configured as uplink ports.
Port List	Use the From and To fields to set a list of ports to be placed in, or removed from, the Service Provider VLAN. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3 - 2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Entering *all* will denote all ports on the Switch.

Trunking

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. DGS-3400 Series supports up to 32 port trunk groups with 2 to 8 ports in each group. A potential bit rate of 8000 Mbps can be achieved.

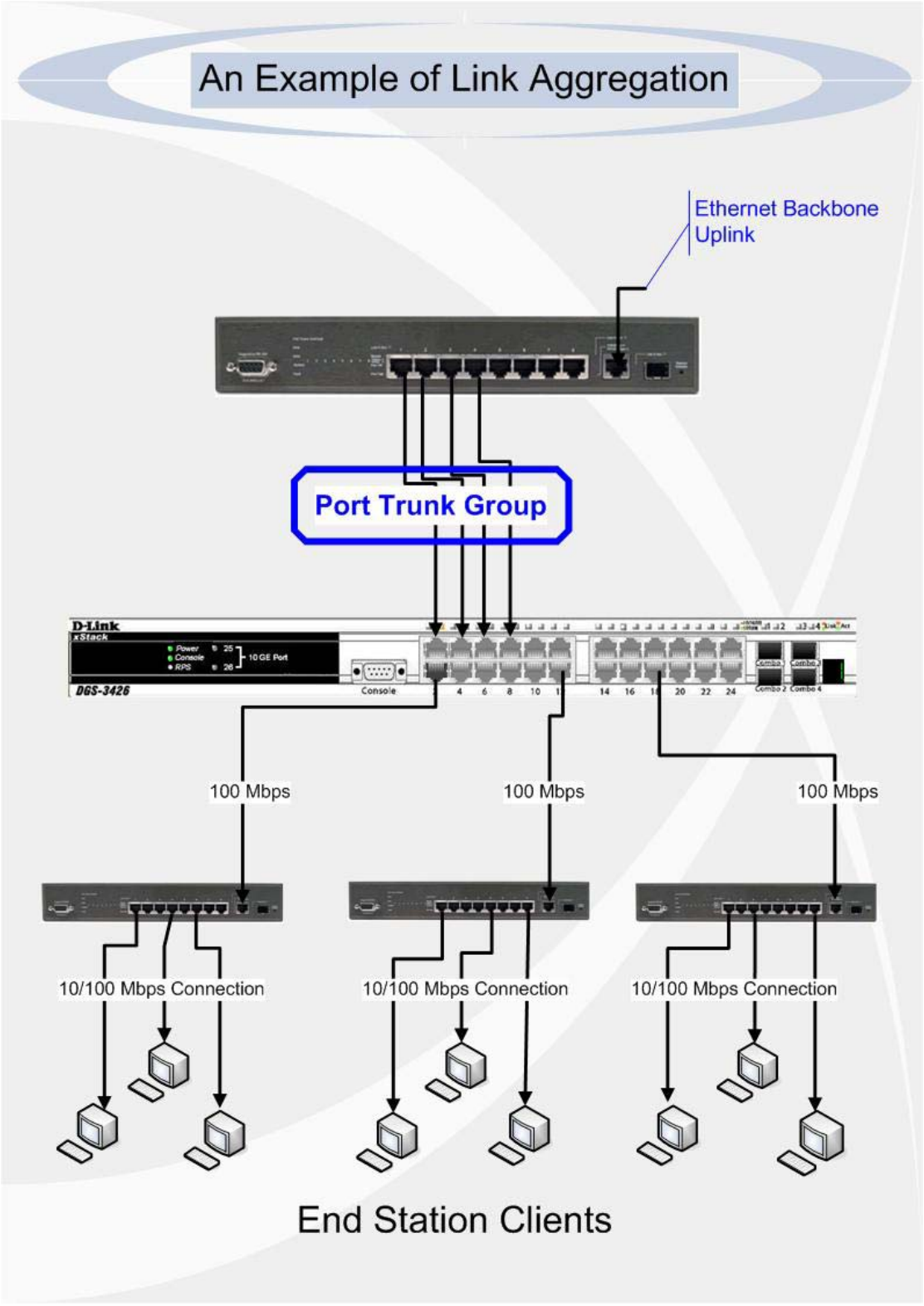


Figure 7- 14. Example of Port Trunk Group

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 linked ports of the link aggregation group.

NOTE: Trunking may be done across switches in the switch stack without any limitations.

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). The (optional) Gigabit ports can only belong to a single link aggregation group. 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 LACP 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.

Link Aggregation

To configure port trunking, click on the **Link Aggregation** hyperlink in the **Trunking** folder under **L2 Features** to bring up the following window:

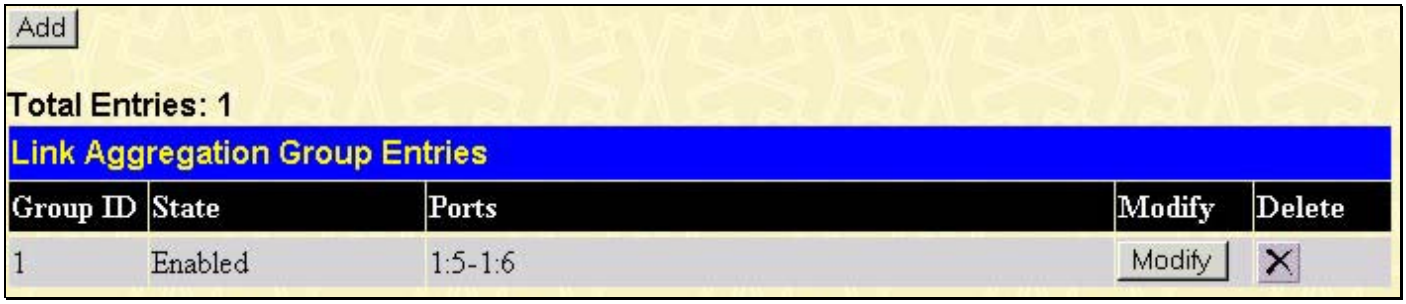


Figure 7- 15. Link Aggregation Group Entries table

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 Hyperlinked Group ID. To delete a port trunk group, click the corresponding ✕ under the Delete heading in the Link Aggregation Group Entries table.

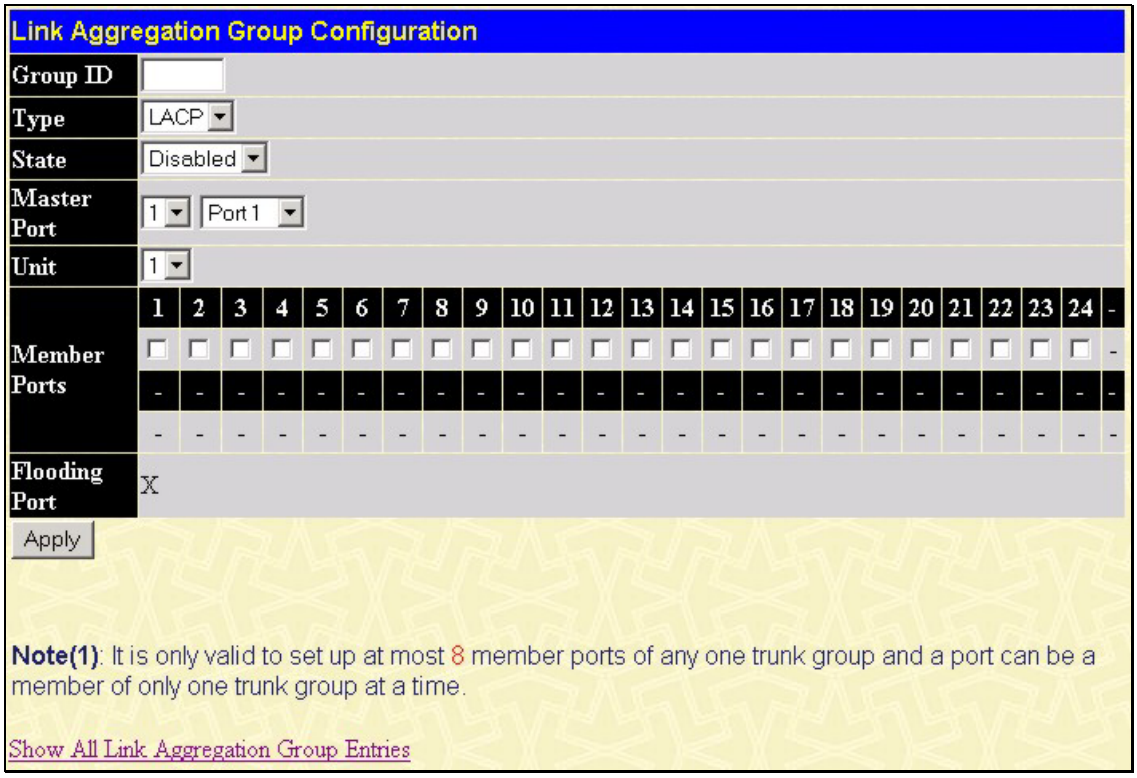


Figure 7- 16. Link Aggregation Settings – Add

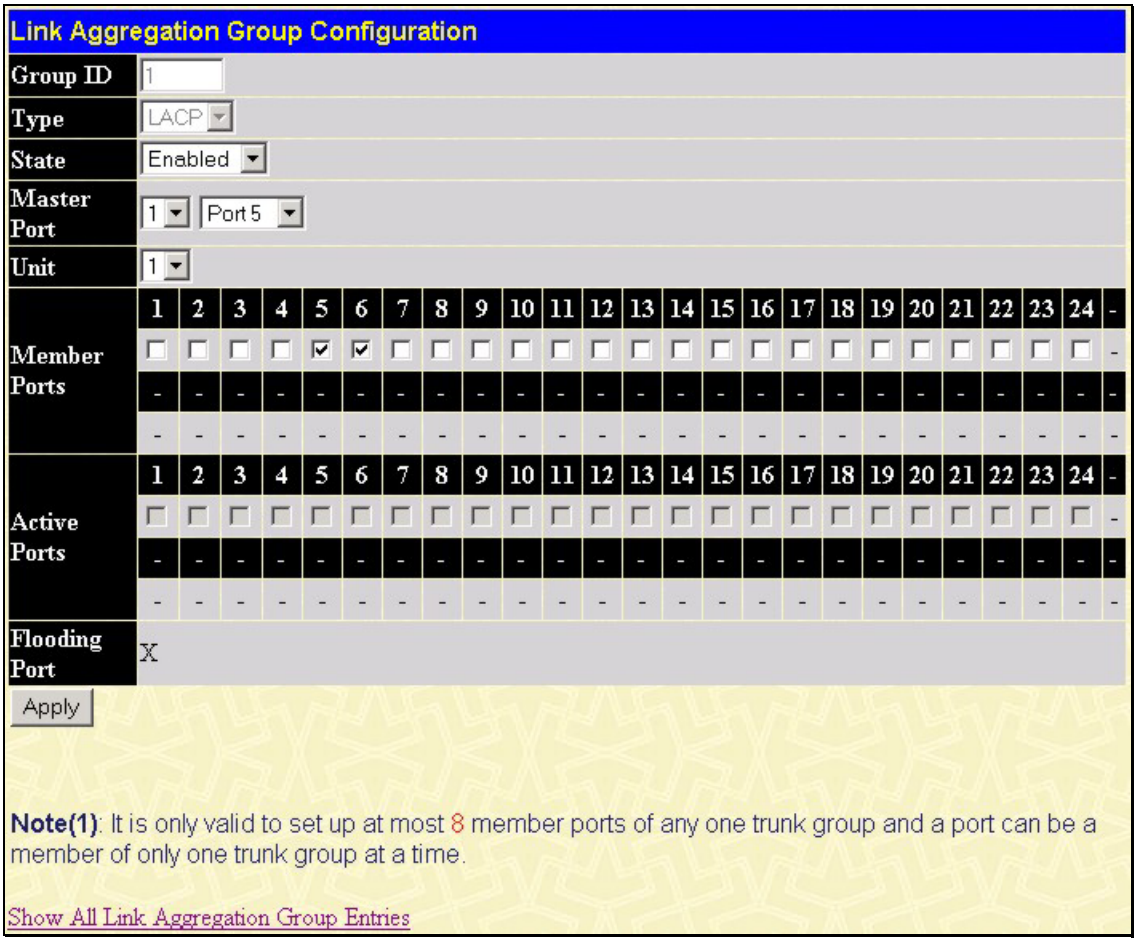


Figure 7- 17. Link Aggregation Settings window - Modify

The user-changeable parameters are as follows:

Parameter	Description
Group ID	Select an ID number for the group, between *1* and 32.
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.
Master Port	Choose the Master Port for the trunk group using the pull-down menu.
Unit	Select the switch in the switch stack to be modified.
Member Ports	Choose the members of a trunked group. Up to eight ports per group can be assigned to a group.
Flooding Port	A trunking group must designate one port to allow transmission of broadcasts, multicasts and unknown unicasts.
Active Port	Shows the port that is currently forwarding packets.
Type	This pull-down menu allows users to select between *Static* and *LACP* (Link Aggregation Control Protocol). LACP allows for the automatic detection of links in a Port Trunking Group.

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

NOTE: To configure the Algorithm for Link Aggregation, please refer back to the DGS-3400 Web Management Tool and select the Link Aggregation Algorithm located on that web page. The description for this function may be found in the explanation for the Device Information window located earlier in this manual.

LACP Port Settings

The **LACP Port Settings** 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.

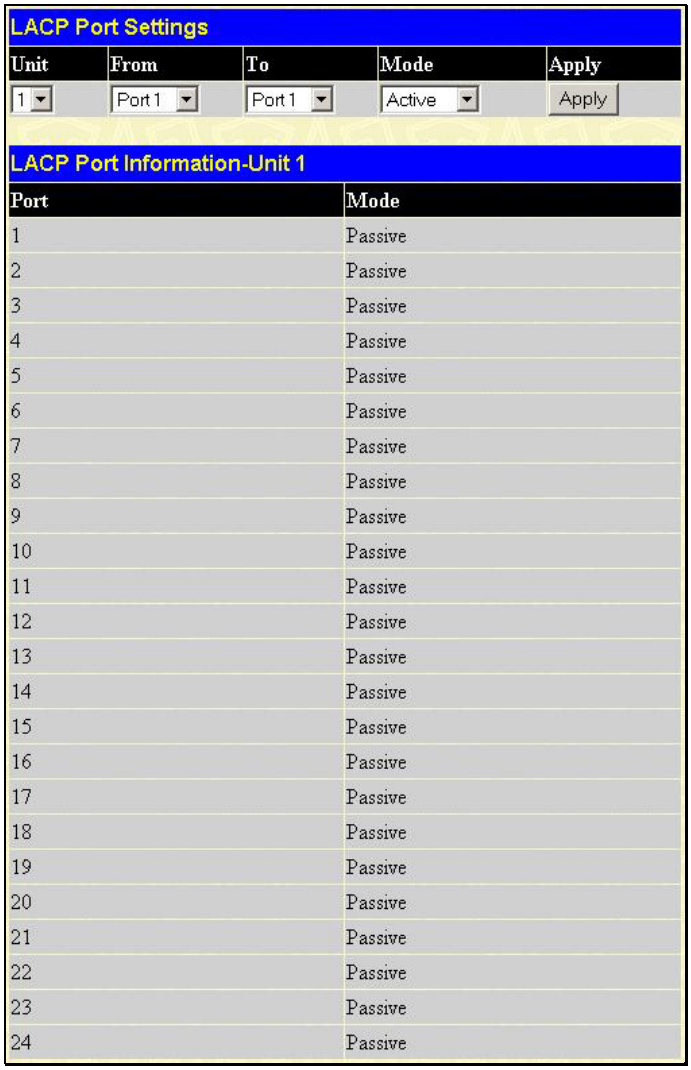


Figure 7- 18. LACP Port Settings window

The user may set the following parameters:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
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.

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 **Device Information**). You may then fine-tune the settings for each VLAN using the **IGMP Snooping Settings** link in the **L2 Features** 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

To view the IGMP Snooping Settings window, Open the **IGMP Snooping** folder and click the **IGMP Snooping Settings** link. To modify the settings, click the **Modify** button of the VLAN ID you want to change.

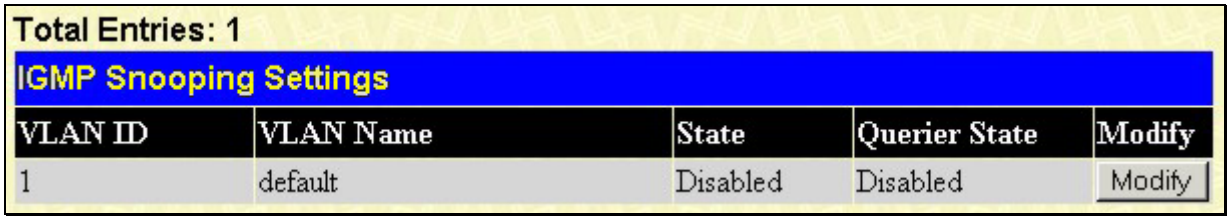


Figure 7- 19. IGMP Snooping Settings window

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

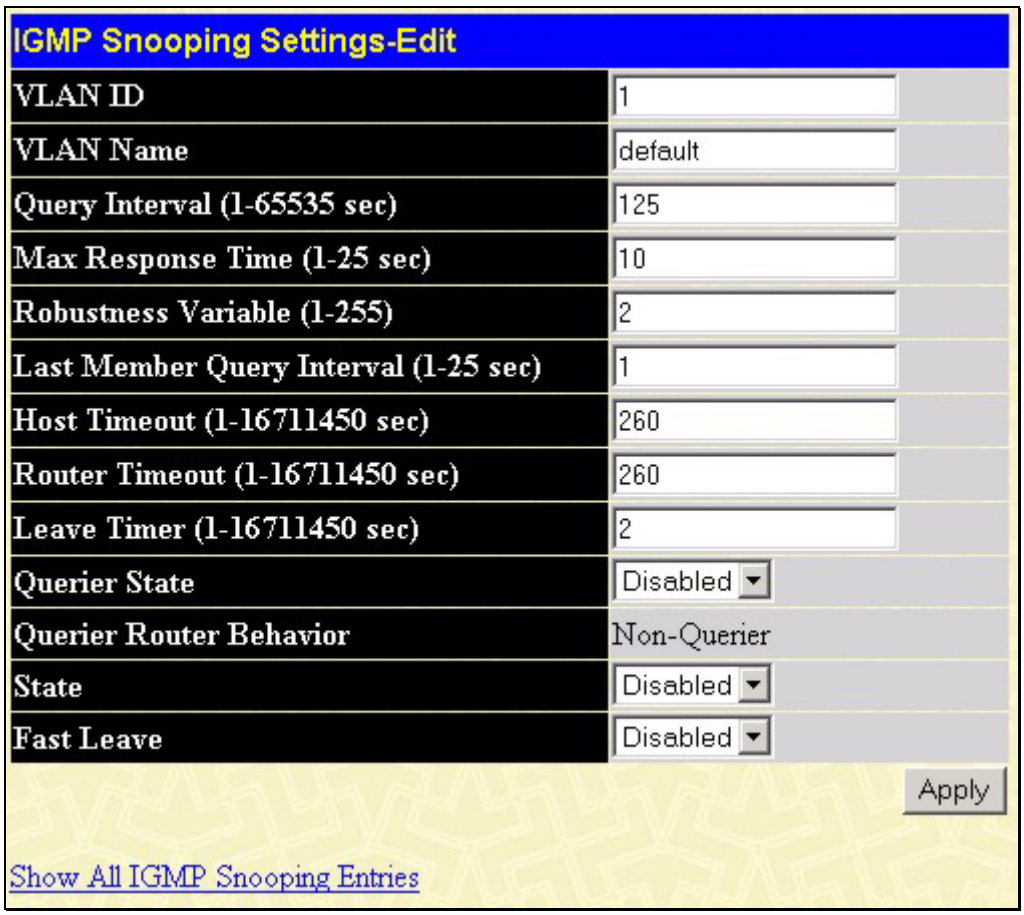


Figure 7- 20. IGMP Snooping Settings –Edit window

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	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	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 Variable	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of *1* to *255*. Default = *2*.
Last Member Query Interval	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	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*.
Route Timeout	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	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. The default setting is 2 seconds.
Querier State	Choose *Enabled* to enable transmitting IGMP Query packets or *Disabled* to disable. The default is *Disabled*.
State	Select *Enabled* to implement IGMP Snooping. This field is *Disabled* by default.
Fast Leave	The Fast Leave option may be enabled or disabled (default). This allows an interface to be pruned without sending group-specific queries.

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

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 **Router Port Settings** link to open the **Router Port Settings** page, as shown below.

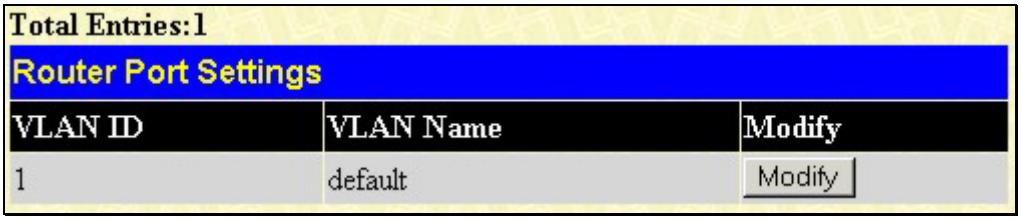


Figure 7- 21. Router Port Settings window

The **Router Ports Settings** window 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 **Router Port** window, as shown below.

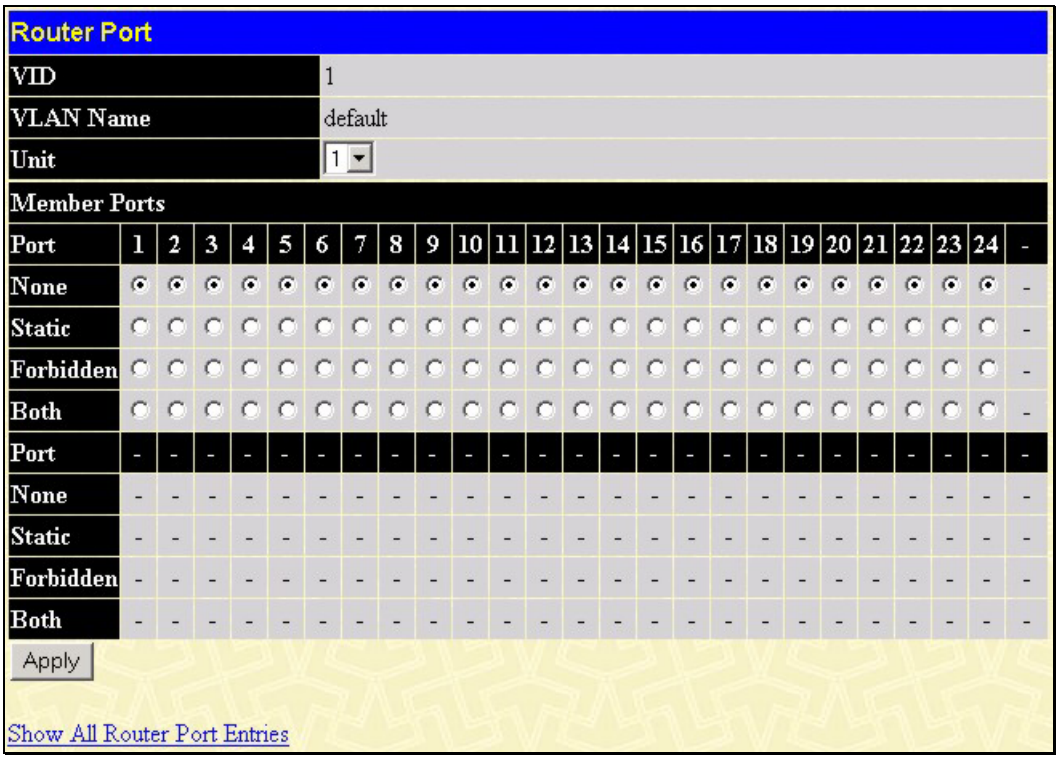


Figure 7- 22. Router Port window

The following parameters can be set:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
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.
Member Ports	Ports on the Switch that will have a multicast router attached to them. There are three options for which to configure these ports: *None* – Click this option to not set these ports as router ports *Static* – Click this option to designate a range of ports as being connected to a multicast-enabled router. This command will ensure that all packets with this router as its destination will reach the multicast-enabled router. *Forbidden* – Click this option to designate a port or range of ports as being forbidden from being connected to multicast enabled routers. This ensures that these configured forbidden ports will not send out routing packets

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

ISM VLAN

In a switching environment, multiple VLANs may exist. Every time a multicast query passes through the Switch, the switch must forward separate different copies of the data to each VLAN on the system, which, in turn, increases data traffic and may clog up the traffic path. To lighten the traffic load, multicast VLANs may be incorporated. These multicast VLANs will allow the Switch to forward this multicast traffic as one copy to recipients of the multicast VLAN, instead of multiple copies.

Regardless of other normal VLANs that are incorporated on the Switch, users may add any ports to the multicast VLAN where they wish multicast traffic to be sent. Users are to set up a source port, where the multicast traffic is entering the switch, and then set the ports where the incoming multicast traffic is to be sent. The source port cannot be a recipient port and if configured to do so, will cause error messages to be produced by the switch. Once properly configured, the stream of multicast data will be relayed to the receiver ports in a much more timely and reliable fashion.

Restrictions and Provisos

The Multicast VLAN feature of this switch does have some restrictions and limitations, such as:

1. Multicast VLANs can only be implemented on edge switches.
2. Member ports and source ports can be used in multiple ISM VLANs. But member ports and source ports cannot be the same port in a specific ISM VLAN.
3. The Multicast VLAN is exclusive with normal 802.1q VLANs, which means that VLAN IDs (VIDs) and VLAN Names of 802.1q VLANs and ISM VLANs cannot be the same. Once a VID or VLAN Name is chosen for any VLAN, it cannot be used for any other VLAN.
4. The normal display of configured VLANs will not display configured Multicast VLANs.
5. Once an ISM VLAN is enabled, the corresponding IGMP snooping state of this VLAN will also be enabled. Users cannot disable the IGMP feature for an enabled ISM VLAN.
6. User can configure 16 ranges of multicast groups, no upper limitation of each range.
7. Router ports cannot be deleted if they are the source ports for ISM VLANs.

To configure the ISM Vlan Settings window, click **L2 Features > IGMP Snooping > ISM VLAN Settings,** which will open the following window:

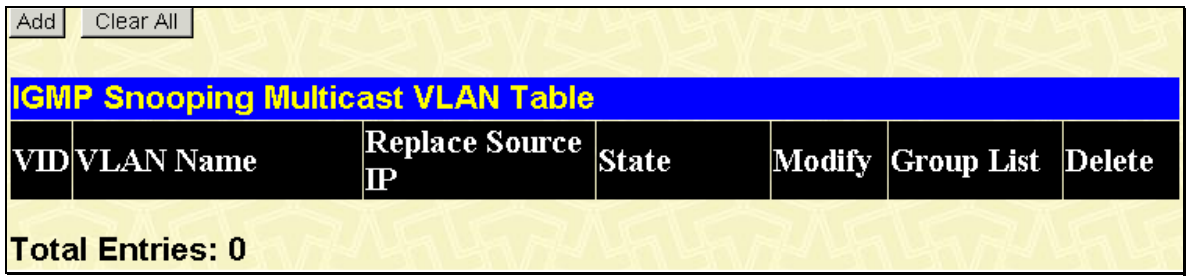


Figure 7- 23. IGMP Snooping Multicast VLAN Table window

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

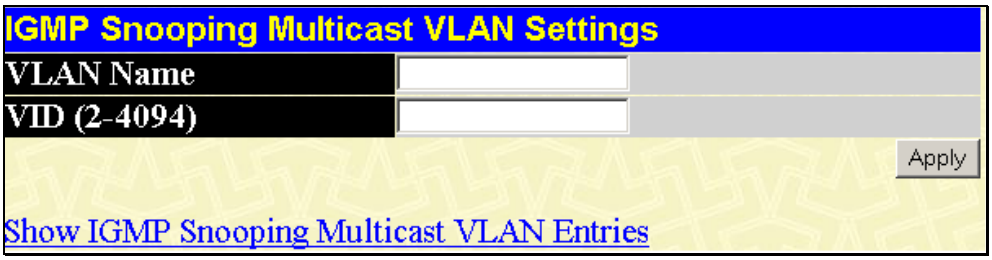


Figure 7- 24. IGMP Snooping Multicast VLAN Settings - Add window

Parameter	Description
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to add.

VID (2-4094)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to add.

To view the settings for all entries, click on the hyperlinked **Show IGMP Multicast VLAN Entries**, which will reveal the following window.

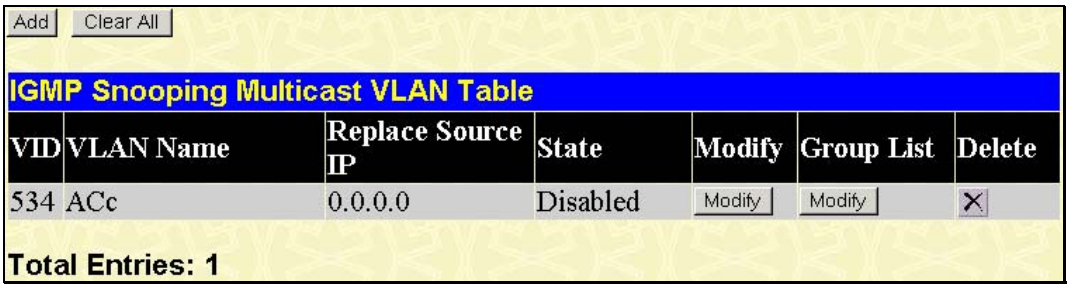


Figure 7- 25. IGMP Snooping Multicast VLAN Entries window

To configure the IGMP Snooping Multicast VLAN settings, click its corresponding Modify button, which will produce the following window for the user to configure.

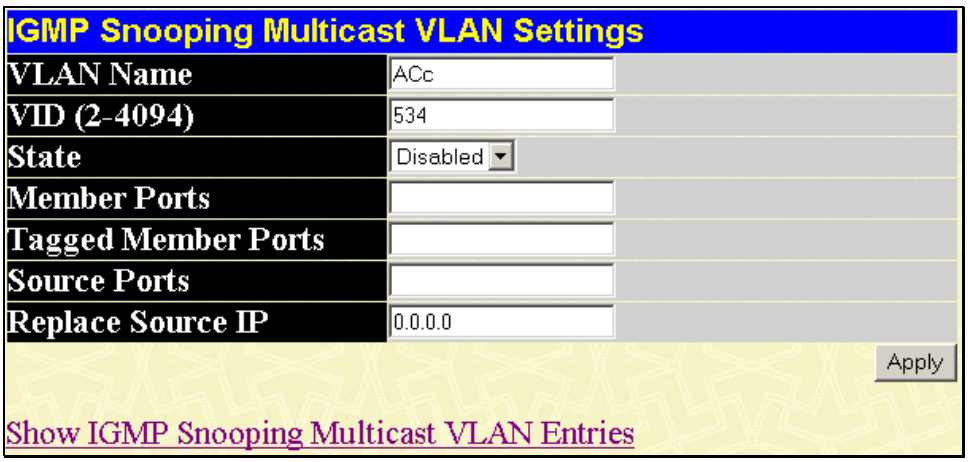


Figure 7- 26. IGMP Snooping Multicast VLAN Settings - Modify window

Parameter	Description
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to modify.
VID (2-4094)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to modify.
State	This parameter specifies the state of the configured ISM VLAN.
Member Ports	This parameter specifies the member ports of the ISM VLAN, which connects with pc users.
Tagged Member Ports	This parameter specifies the tagged member ports of the ISM VLAN, which connects with pc users.
Source Ports	This parameter specifies the source port of the ISM VLAN, which connects with the uplink server.
Replace Source IP	This parameter specifies the replacement for the source port of the ISM VLAN, which connects with the uplink server.

Limited Multicast Address Range

The **Limited Multicast Address Range** window allows the user to specify which multicast address(es) reports are to be received on specified ports on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IP address or range of IP addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports. Click **L2 Features > IGMP Snooping > Limited Multicast Address Range** to open the **Limited Multicast Address Range** window shown adjacent:

To configure Limited IP Multicast Range:

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

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

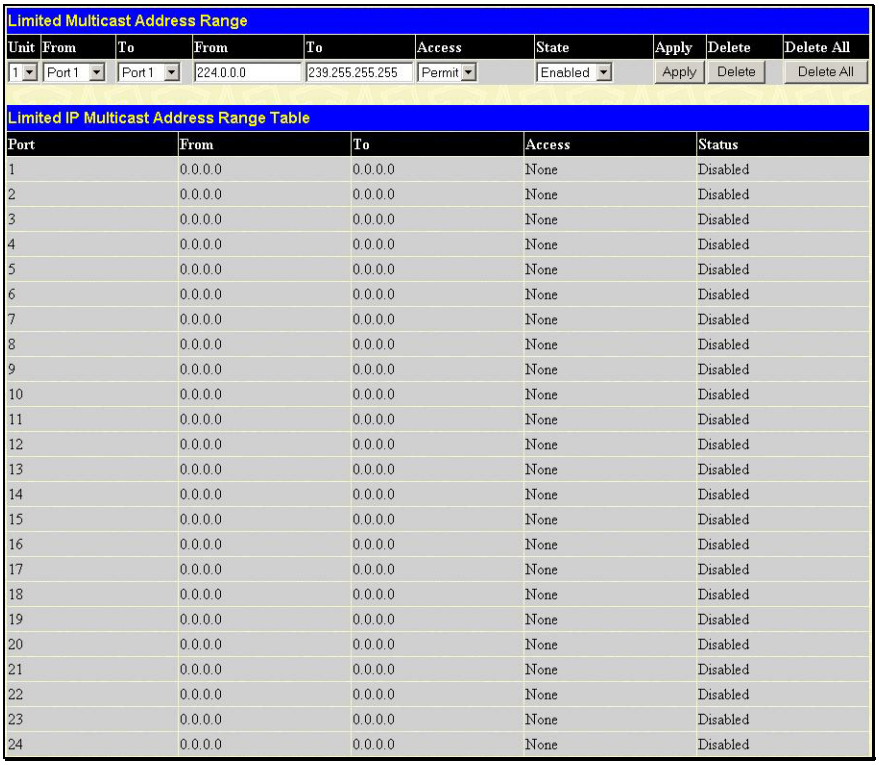


Figure 7- 27. Limited Multicast Address Range

Click **Apply** to implement the new settings on the Switch. Click **Delete** to remove the configured range from the settings. Click **Delete All** to delete all Limited IP Multicast settings.

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
State	Toggle the **State** field to either *Enabled* or *Disabled* for a given port or group of ports where access is to be either permitted or denied.
From	Enter the port for which to begin the Limited IP Multicast Range configuration. Enter the lowest multicast IP address of the range.
To	Enter the port for which to begin the Limited IP Multicast Range configuration. Enter the highest multicast IP address of the range.
Access	Toggle the **Access** field to either *Permit* or *Deny* to limit or grant access to a specified range of Multicast addresses on a particular port or range of ports.
State	Use the pull down menu to enable or disable the state of the Limited Multicast Address Range.

MLD Snooping

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID and the associated multicast IPv6 multicast group address and then considers this port to be a active listening port. The active listening ports are the only ones to receive multicast group data.

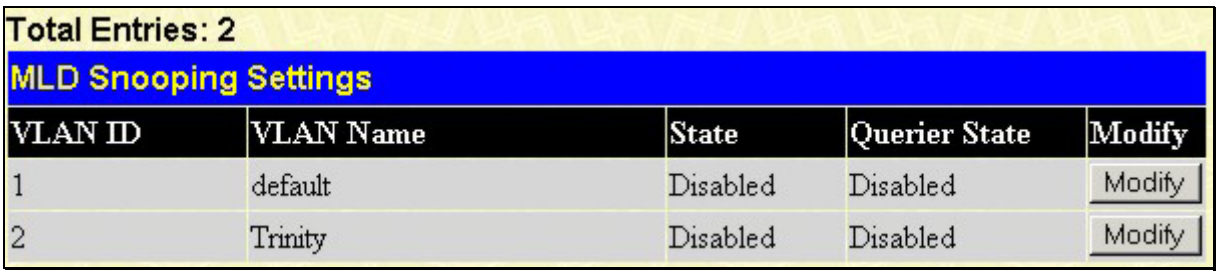
MLD Control Messages

Three types of messages are transferred between devices using MLD snooping. These three messages are all defined by three ICMPv6 packet headers, labeled 130, 131 and 132.

1. **Multicast Listener Query** – Similar to the IGMPv2 Host Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. There are two types of MLD query messages emitted by the router. The General Query is used to advertise all multicast addresses that are ready to send multicast data to all listening ports, and the Multicast Specific query, which advertises a specific multicast address that is also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.
2. **Multicast Listener Report** – Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.
3. **Multicast Listener Done** – Akin to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is "done" with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.

MLD Snooping Settings

To configure the settings for MLD snooping, click **L2 Features > MLD Snooping > MLD Snooping Settings**, which will open the following window.


Total Entries: 2

MLD Snooping Settings

VLAN ID	VLAN Name	State	Querier State	Modify
1	default	Disabled	Disabled	Modify
2	Trinity	Disabled	Disabled	Modify

Figure 7- 28. MLD Snooping Settings window

This window displays the current MLD Snooping settings set on the Switch, defined by VLAN. To configure a specific VLAN for MLD snooping, click the VLAN's corresponding Modify button, which will display the following window for the user to configure.

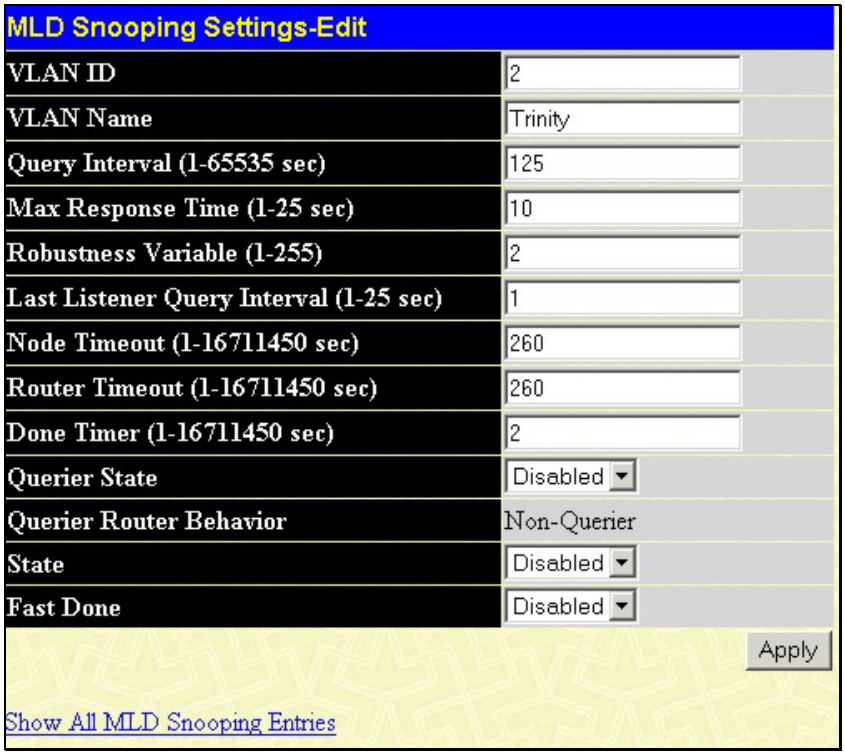


Figure 7- 29. MLD Snooping Settings - Edit window

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 for which to modify the MLD Snooping Settings.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN for which to modify the MLD Snooping Settings.
Query Interval	The Query Interval field is used to set the time (in seconds) between transmitting MLD queries. Entries between *1* and *65535* seconds are allowed. Default = *125*.
Max Response Time	This determines the maximum amount of time in seconds allowed to wait for a response for MLD port listeners. The Max Response Time field allows an entry between *1* and *25* (seconds). Default = *10*.
Robustness Variable	Provides fine-tuning to allow for expected packet loss on a subnet. The user may choose a value between 1 and 255 with a default setting of 2. If a subnet is expected to be lossy, the user may wish to increase this interval.
Last Listener Query Interval	The maximum amount of time to be set between group-specific query messages. This interval may be reduced to lower the amount of time it takes a router to detect the loss of a last listener group. The user may set this interval between 1 and 25 seconds with a default setting of 1 second.
Node Timeout	Specifies the link node timeout, in seconds. After this timer expires, this node will no longer be considered as listening node. The user may specify a time between *1* and *16711450* with a default setting of *260* seconds.
Router Timeout	Specifies the maximum amount of time a router can remain in the Switch's routing table as a listening node of a multicast group without the Switch receiving a node listener report. The user may specify a time between *1* and *16711450* with a default setting of 260 seconds.
Done Timer	Specifies the maximum amount of time a router can remain in the Switch after receiving a done message from the group without receiving a node listener report. The user may specify a time between *1* and *16711450* with a default setting of 2 seconds.

Querier State	Choose *Enabled* to enable transmitting MLD Snooping Query packets or *Disabled* to disable. The default is *Disabled*.
Querier Router Behavior	This read-only field describes the current querier state of the Switch, whether Querier, which will send out Multicast Listener Query Messages to links, or Non-Querier, which will not send out Multicast Listener Query Messages.
State	Used to enable or disable MLD snooping for the specified VLAN. This field is *Disabled* by default.
Fast Done	This parameter allows the user to enable the *fast done* function. Enabled, this function will allow members of a multicast group to leave the group immediately when a *done* message is received by the Switch.

NOTE: The robustness variable of the MLD snooping querier is used in creating the following MLD message intervals:

Group Listener Interval – The amount of time that must pass before a multicast router decides that there are no more listeners present of a group on a network. Calculated as (robustness variable * query interval) + (1 * query interval).

Querier Present Interval – The amount of time that must pass before a multicast router decides that there are no other querier devices present. Calculated as (robustness variable * query interval) + (0.5 * query response interval).

Last Listener Query Count – The amount of group-specific queries sent before the router assumes there are no local listeners in this group. The default value is the value of the robustness variable.

Click **Apply** to implement changes made. Click the Show All MLD Snooping Entries link to return to the MLD Snooping Settings window.

MLD Router Port Settings

The following window is used to designate a port or range of ports as being connected to multicast enabled routers. When IPv6 routing control packets, such as DVMRP, OSPF or RIP, or MLD Query packets are found in an Ethernet port or specified VLAN, the Switch will set these ports as dynamic router ports. Once set, this will ensure that all packets with a multicast router as its destination will arrive at the multicast-enabled router, regardless of protocol. If the Router's Aging Time expires and no routing control packets or query packets are received by the port, that port will be removed from being a router port.

To configure the settings for MLD Router Ports, click **L2 Features > MLD Snooping > MLD Router Port Settings**, which will open the following window.

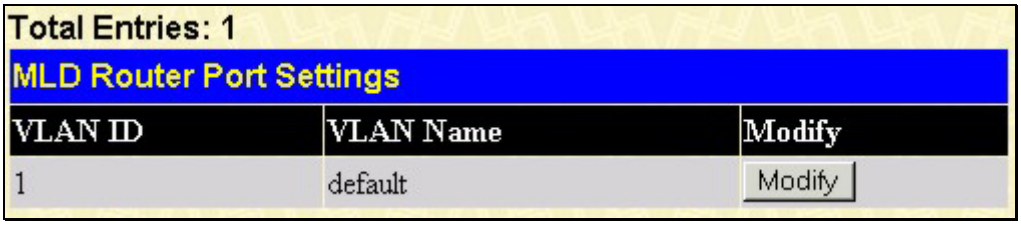


Figure 7- 30. Router Port Settings window for MLD

To configure the router ports settings for a specified VLAN, click its corresponding Modify button, which will produce the following window for the user to configure.

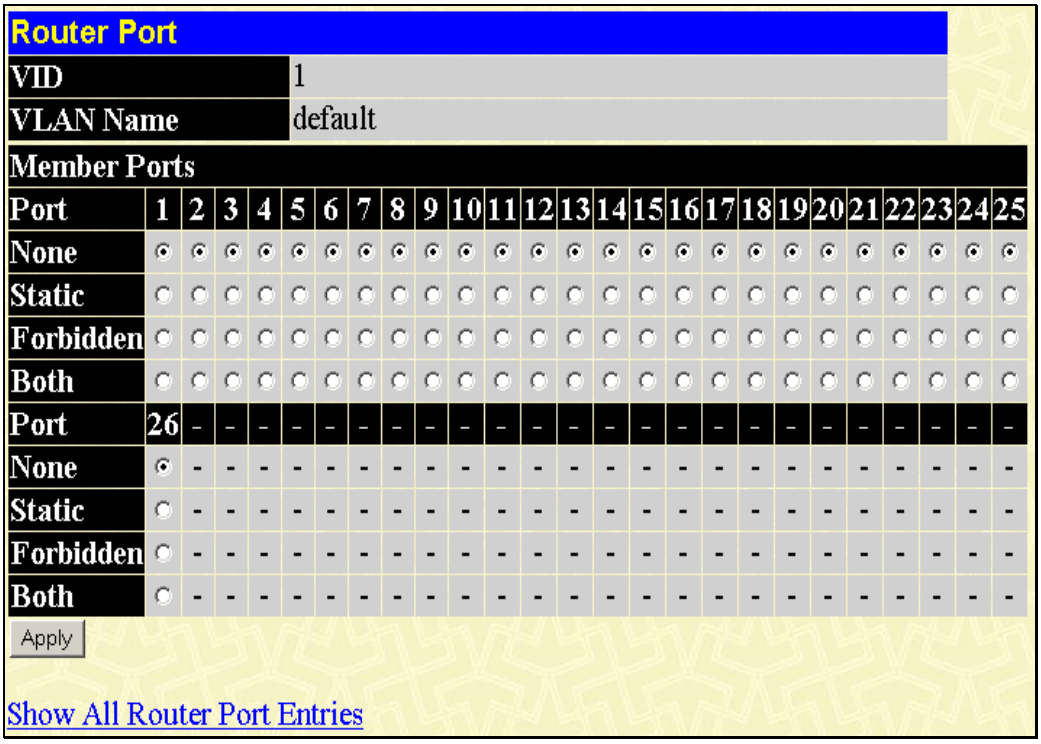


Figure 7- 31. Router Port- modify window

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 MLD multicast router is attached.
VLAN Name	This is the name of the VLAN where the MLD multicast router is attached.
Unit	Select the switch in the switch stack to be modified.
Member Ports	Ports on the Switch that will have a multicast router attached to them. There are four options for which to configure these ports: *None* – Click this option to not set these ports as router ports *Static* – Click this option to designate a range of ports as being connected to a multicast-enabled router. This command will ensure that all packets with this router as its destination will reach the multicast-enabled router. *Forbidden* – Click this option to designate a port or range of ports as being forbidden from being connected to multicast enabled routers. This ensures that these configured forbidden ports will not send out routing packets *Both* –Click this option to designate a port or range of ports as being both forbidden from being connected to multicast enabled routers. This ensures that these configured forbidden ports will not send out routing packets.

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

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 associated with them. An MSTI ID will classify these instances. 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:

2. A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **STP Bridge Global Settings** window in the Configuration Name field).
3. A configuration revision number (named here as a Revision Level and found in the **STP Bridge Global Settings** window) and;
4. A 4096-element table (defined here as a VID List in the **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 **MST Configuration Identification** window 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 **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 7-3 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.

802.1s MSTP	802.1w RSTP	802.1D STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
Discarding	*Discarding*	*Blocking*	No	No
Discarding	*Discarding*	*Listening*	No	No
Learning	*Learning*	*Learning*	No	**Yes**
Forwarding	**Forwarding**	**Forwarding**	**Yes**	**Yes**

Table 7- 3. 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 **Layer 2 Features** menu and click the **STP Bridge Global Settings** link. Use the STP Status pull-down selector to enable or disable STP globally, and choose the STP method used with the STP Version menu.

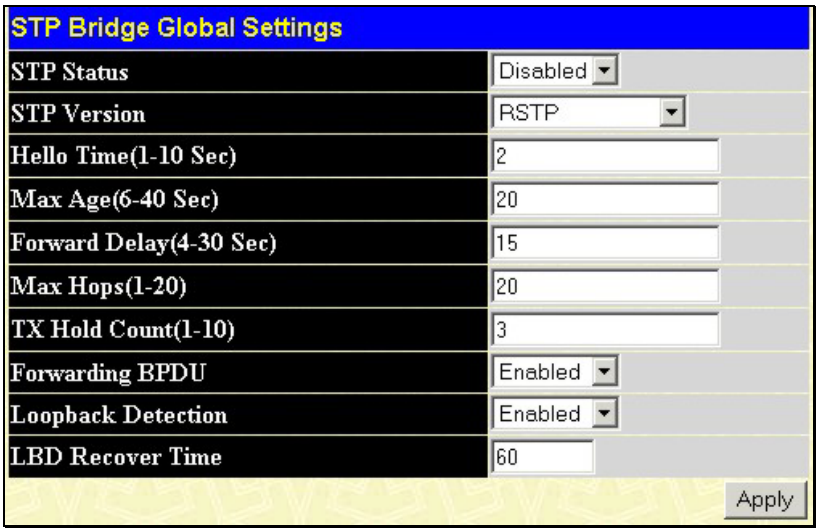


Figure 7- 32. STP Bridge Global Settings window – RSTP (default)

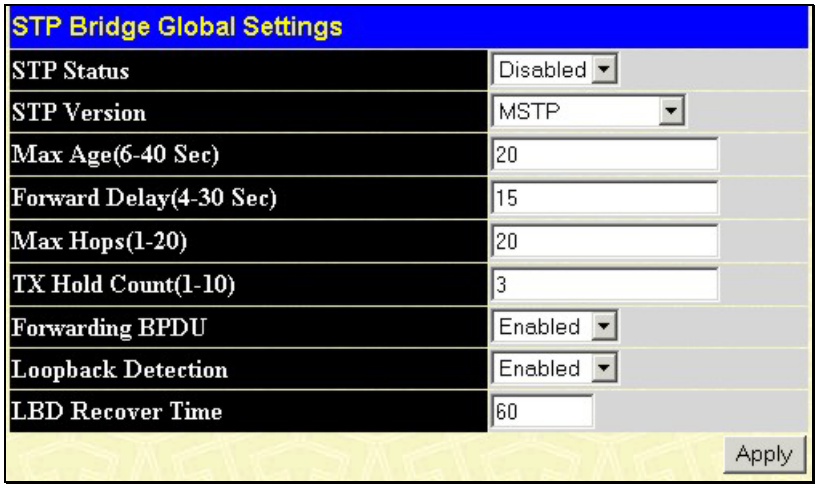


Figure 7- 33. STP Bridge Global Settings window - MSTP

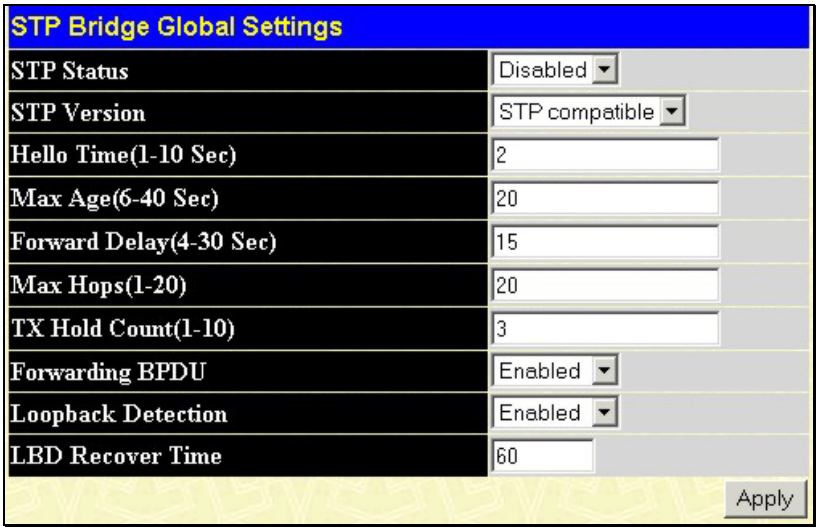


Figure 7- 34. STP Bridge Global Settings – STP Compatible

See the table below for descriptions of the STP versions and corresponding setting options.

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)

Configure the following parameters for STP:

Parameter	Description
STP Status	Use the pull-down menu to globally enable or disable STP.
STP Version	Use the pull-down menu to choose the desired version of STP: *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)	The Hello Time can be set from *1* to *10* seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. 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)	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)	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 forwarding state.
Max Hops (1-20)	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)	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	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*.
Loopback Detection	When enabled, the Switch will temporarily block STP switch-wide when a BDPU packet has looped back. If the Switch detects its own BDPU packet coming back, it signifies a loop on the network – STP is automatically blocked and an alert is sent to the administrator. The default is *Enabled*.
LBD Recover Time	Time allowed (in seconds) for recovery when an STP Loopback is detected. After the timer has expired the Switch checks for an STP loopback, if no loopback detected, STP is resumed. Entering 0 will disable LBD recovery.

Click **Apply** to implement changes made.

MST Configuration Identification

The following screens in the **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 **Layer 2 Features > Spanning Tree > MST Configuration Identification:**

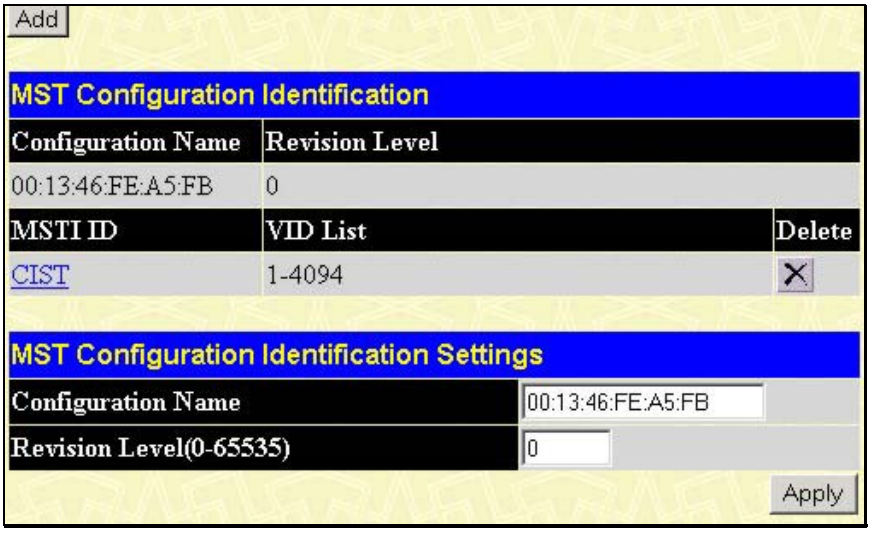


Figure 7- 35. Current MST Configuration Identification menu

The window above contains the following information:

Parameter	Description
Configuration Name	A previously configured name set on the Switch to uniquely identify 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. This field can be set in the STP Bridge Global Settings window.
Revision Level	This value, along with the Configuration Name will identify 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:

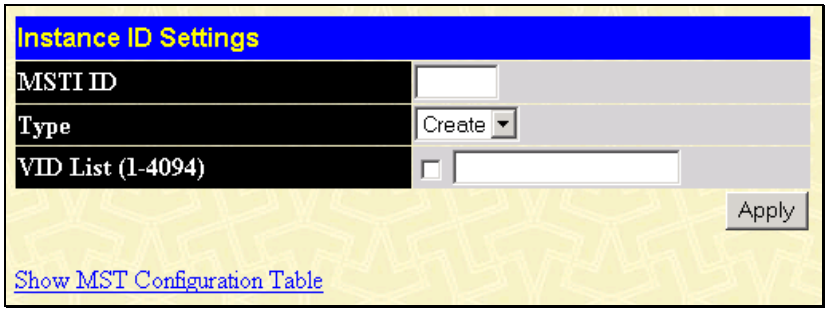


Figure 7- 36. Instance ID Settings window – Add

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:

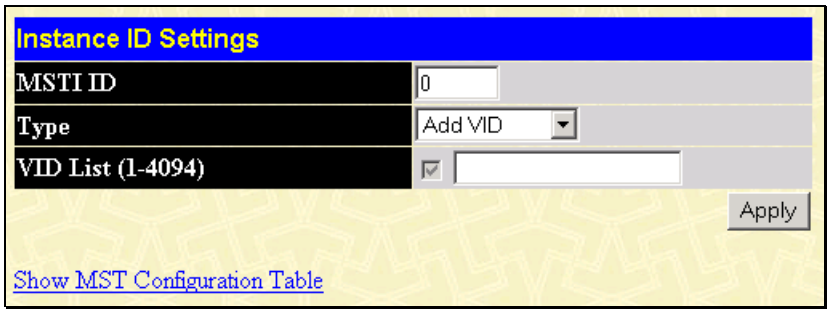


Figure 7- 37. Instance ID Settings window - CIST modify

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	This field allows the user to choose a desired method for altering the MSTI settings. The user has 2 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. 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.

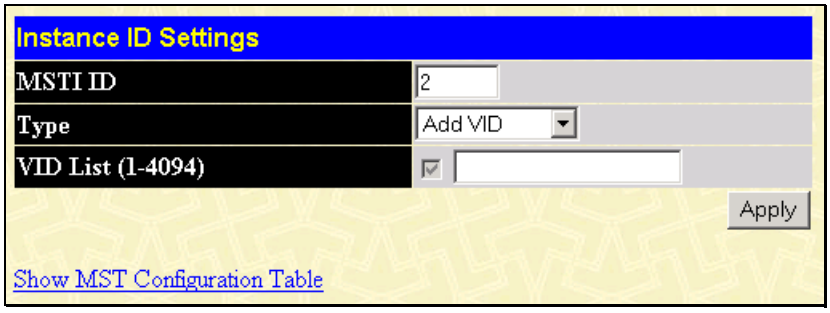


Figure 7- 38. Instance ID Settings window – modify

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 four choices. *Add* - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. *Remove* - 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* or *Remove*.

Click **Apply** to implement changes made.

MSTP Port Information

This window displays the current MSTP Port Information 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 MAC address 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 **Layer 2 Features > Spanning Tree > MSTP Port Information**:

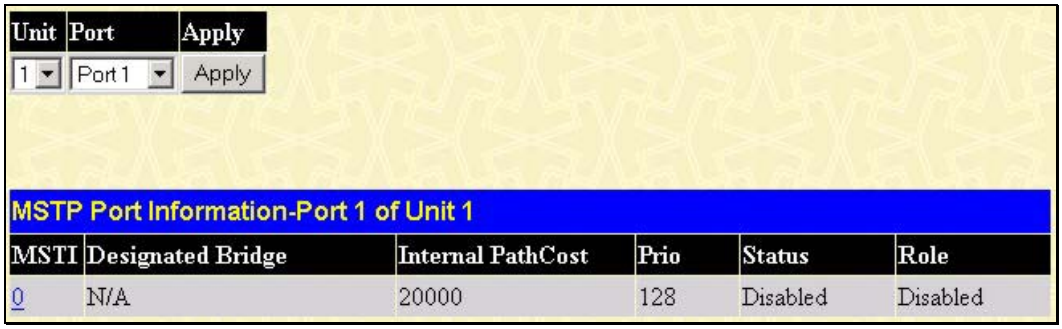


Figure 7- 39. MSTP Port Information

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

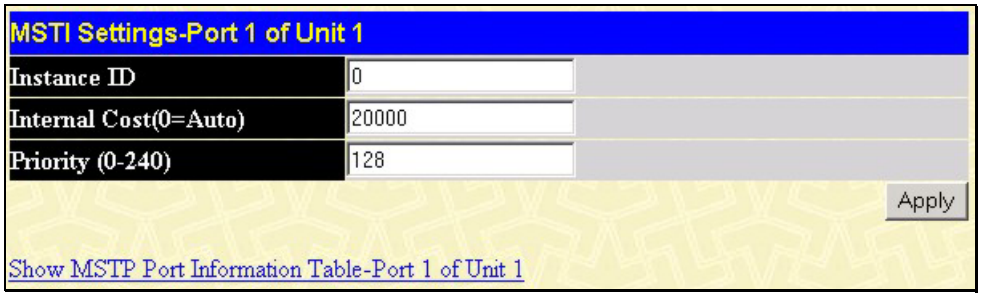


Figure 7- 40. MSTI Settings

The user may configure the following parameters:

Parameter	Description
Instance ID	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)	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 1-200000000* - Selecting this parameter with a value in the range of 1-200000000 will set the quickest route when a loop occurs. A lower Internal cost represents a quicker transmission.
Priority	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 **Layer 2 Features > Spanning Tree > STP Instance Settings**:

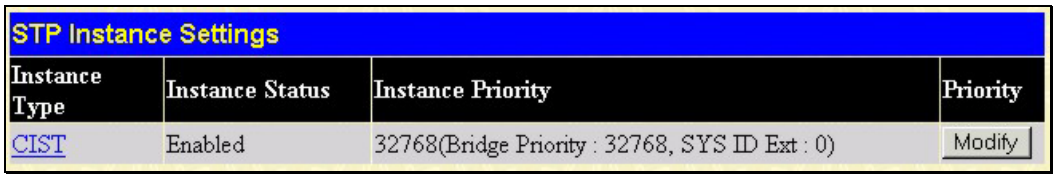


Figure 7- 41. STP Instance Table

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 a 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.

Click the **Modify** button to change the priority of the MSTI. This will open the **Instance ID Settings** window to configure.

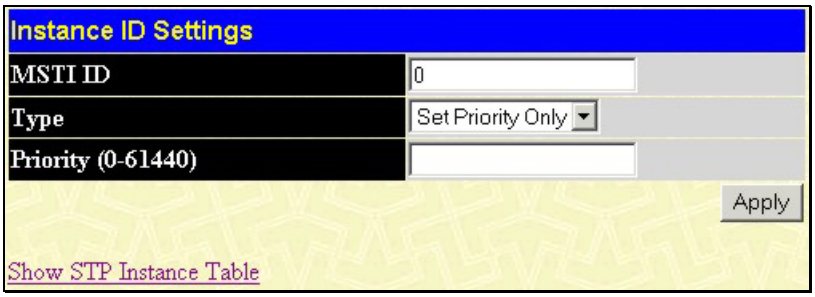


Figure 7- 42. STP Instance Settings Modify

Parameter	Description
MSTI ID	Displays the MSTI ID of the instance being Modified. An entry of 0 in this field denotes the CIST (default MSTI).
Type	The Type field in this window will be permanently set to *Set Priority Only*.
Priority (0-61440)	Enter the new priority in the Priority field

Click **Apply** to implement the new priority setting.

STP Port Settings

STP can be set up on a port per port basis. To view the STP Port Settings window click **Layer 2 Features > Spanning Tree > STP Port Settings**:

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.

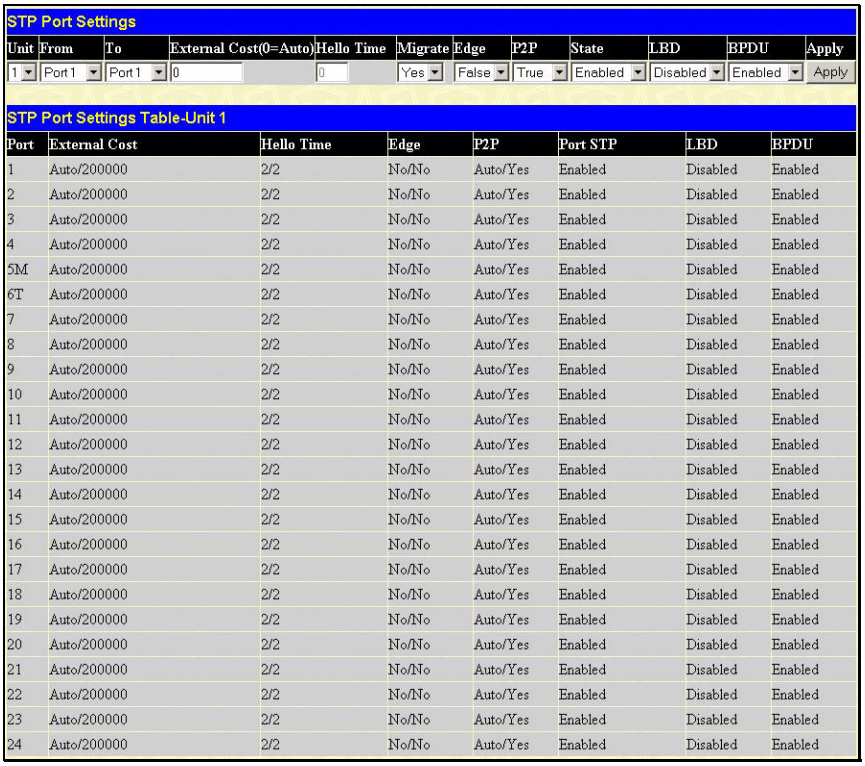


Figure 7- 43. STP Port Settings window

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

The following STP Port Settings fields can be set:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
From/To	A consecutive group of ports may be configured starting with the selected port.
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	The time interval between transmissions of configuration messages by the designated port, to other devices on the bridged LAN. 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	When operating in RSTP mode, selecting yes forces the port that has been selected to transmit RSTP BPDUs.
Edge	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	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	This drop-down menu allows you to enable or disable STP for the selected group of ports. The default is Enabled.
LBD	Use the pull-down menu to enable or disable the loop-back detection function on the switch for the ports configured above.
BPDU	Use the pull-down menu to enable or disable the flooding of BPDU packets when STP is disabled.

Click **Apply** to implement changes made.

Forwarding & Filtering

Unicast Forwarding

Open the **Forwarding & Filtering** folder in the **Layer 2 Features** menu and click on the **Unicast Forwarding** link.

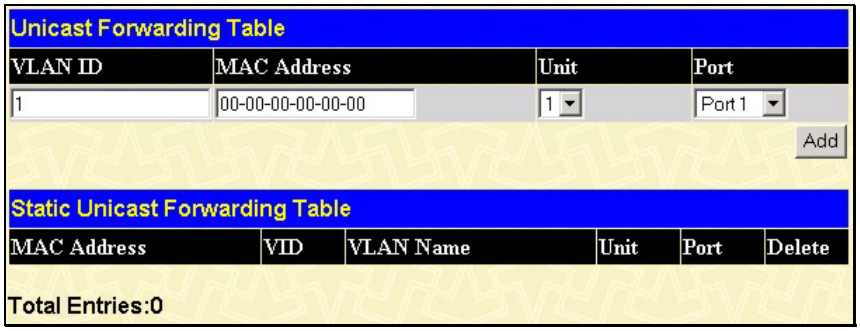


Figure 7- 44. Setup Static Unicast Forwarding Table window

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	Select the switch in the switch stack to be modified.
Port	Allows the selection of the port number on which the MAC address entered above resides.

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

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 screen below:

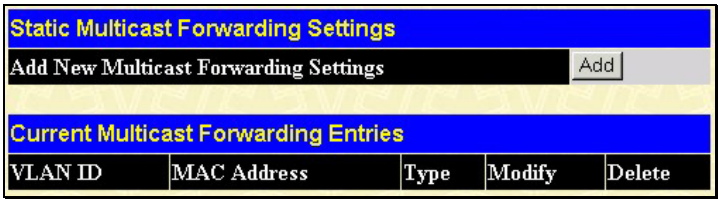


Figure 7- 45. Static Multicast Forwarding Settings window

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

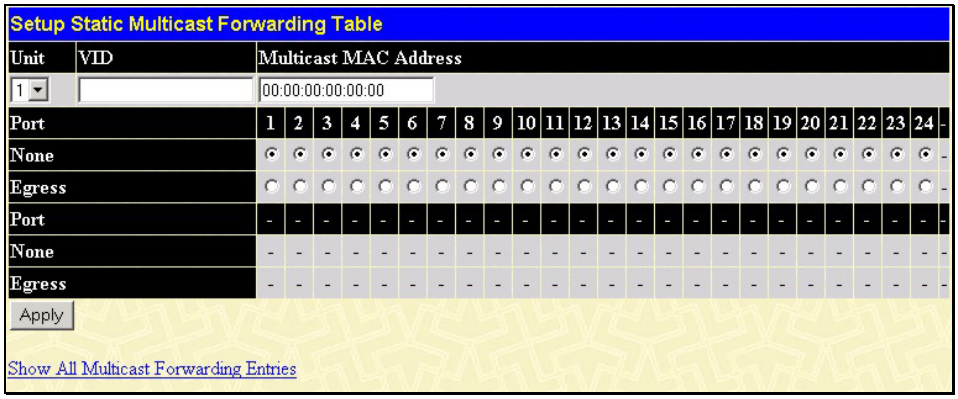


Figure 7- 46. Setup Static Multicast Forwarding Table window

The following parameters can be set:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
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 and ports that are either forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. 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.

Multicast Filtering Mode

Open the **Forwarding & Filtering** folder and click on the **Multicast Filtering Mode** link to see the entry screen below:

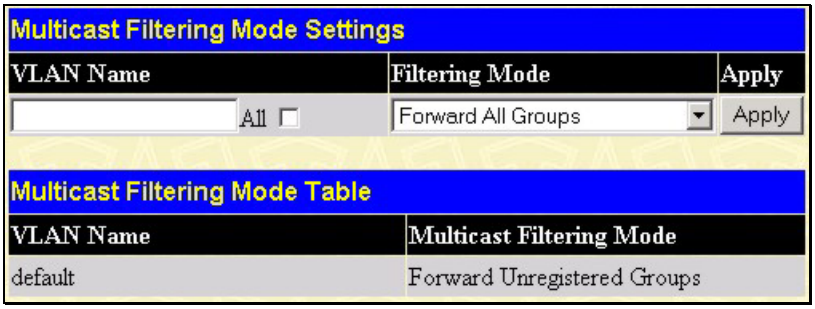


Figure 7- 47. Multicast Filtering Mode

Parameter	Description
VLAN Name	The VLAN to which the specified filtering action applies. Select the **All** option to apply the action to all VLANs on the Switch.
Filtering Mode	This drop-down menu allows you to select the action the Switch will take when it receives a multicast packet that requires forwarding to a port in the specified VLAN. • *Forward All Groups* – This will instruct the Switch to forward a multicast packet to all multicast groups residing within the range of ports specified above. • *Forward Unregistered Groups* – This will instruct the Switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above. • *Filter Unregistered Groups* – This will instruct the Switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above.

Click **Apply** to implement changes made.

QoS

The xStack DGS-3400 switch series 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.

The 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 xStack DGS-3400 switch series implements basic 802.1P priority queuing.

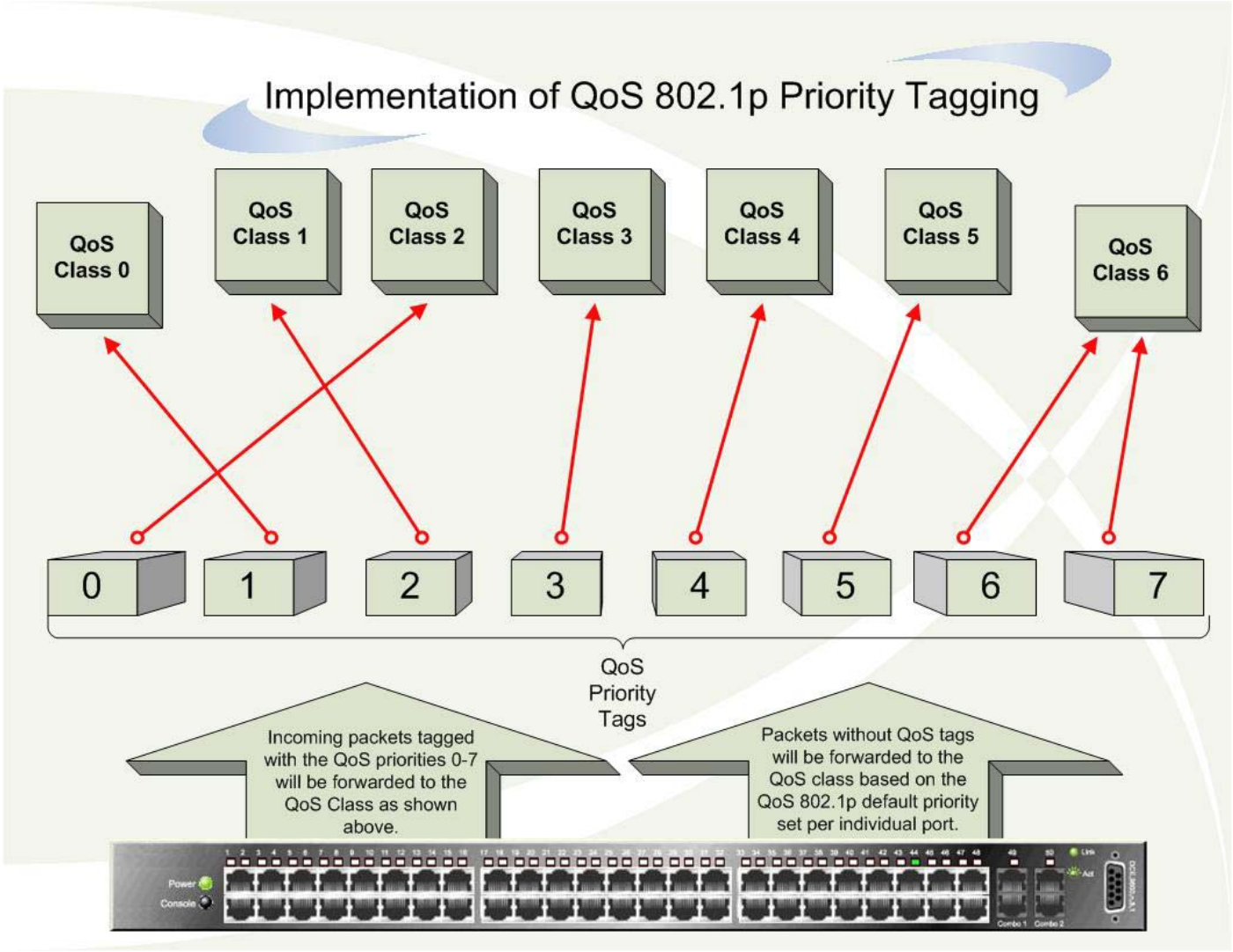


Figure 7- 48. An Example of the Default QoS Mapping on the Switch

The picture above shows the default priority setting for the Switch. Class-6 has the highest priority of the seven priority classes of service 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. Then the user may forward these tagged packets to designated classes of service on the Switch where they will be emptied, based on priority.

For example, let's 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 xStack DGS-3400 Series supports 802.1p priority queuing. The Switch has 8 priority queues. These priority queues are numbered from 6 (Class 6) — the highest priority queue — to 0 (Class 0) — the lowest priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues 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 classes of service are transmitted first. Multiple strict priority classes of service are emptied based on their priority tags. Only when these classes are empty, are packets of lower priority transmitted.

For weighted round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of 8 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 xStack DGS-3400 switch series has 7 configurable priority queues (and seven Classes of Service) for each port on the Switch.

NOTICE: The Switch contains eight classes of service for each port on the Switch. One of these classes is reserved for internal use on the Switch and is therefore not configurable. All references in the following section regarding classes of service will refer to only the seven classes of service that may be used and configured by the administrator.

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 **QoS** folder, click **Bandwidth Control**, to view the screen shown below.

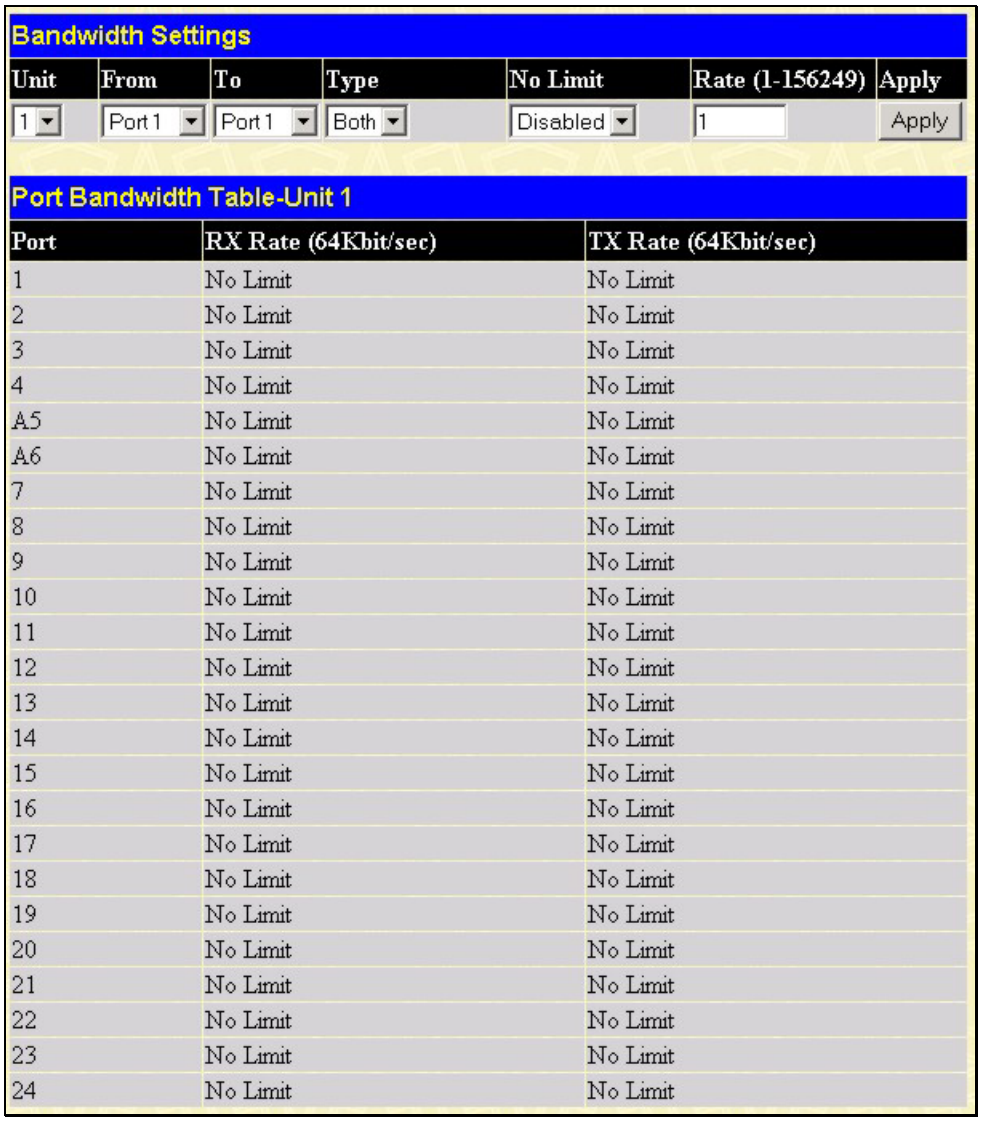


Figure 7- 49. Bandwidth Settings and Port Bandwidth Table window

The following parameters can be set or are displayed:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
From/To	A consecutive group of ports may be configured starting with the selected port.
Type	This drop-down menu allows a selection 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 the user to specify that the selected port will have no bandwidth limit. *Enabled* disables the limit.
Rate	This field allows the input of the data rate that will be the limit for the selected port. The user may choose a rate between 1 and 156249 units, where each unit is defined a 64Kbit/s.

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 a selection between a **Weight Fair** and a **Strict** mechanism for emptying the priority classes. In the **Configuration** menu open the **QoS** folder and click **QoS Scheduling Mechanism**, to view the screen shown below.

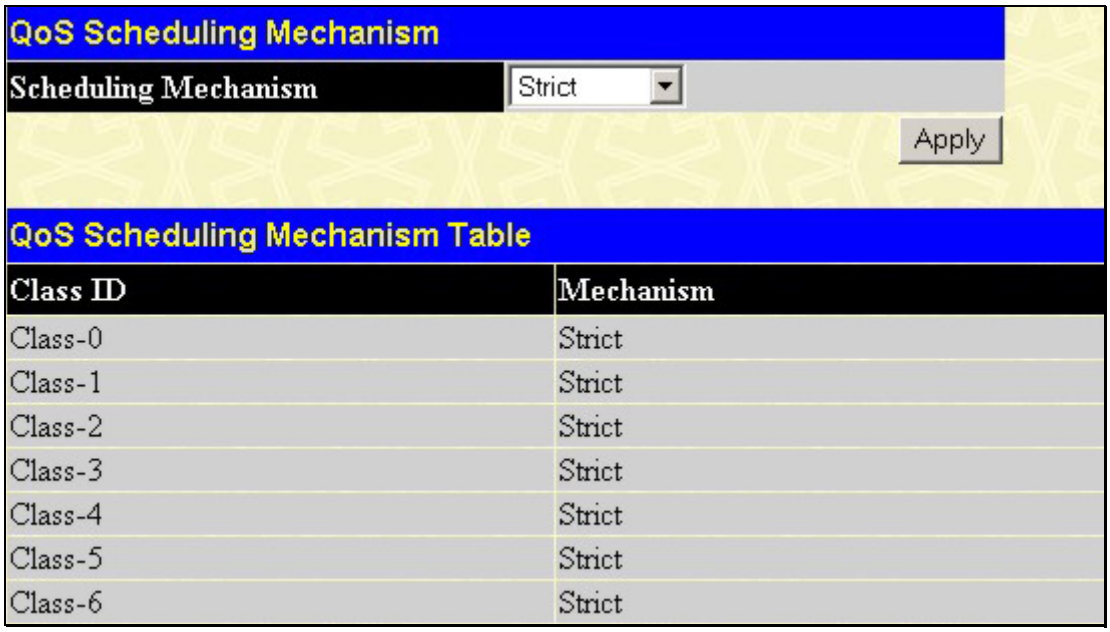


Figure 7- 50. QoS Scheduling Mechanism window

The **Scheduling Mechanism** has the following parameters.

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

Click **Apply** to allow changes to take effect.

QoS Output Scheduling

QoS can be customized by changing the output scheduling used for the hardware classes of service in the Switch. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority classes of service is affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delay. If choosing 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 screen shown below.

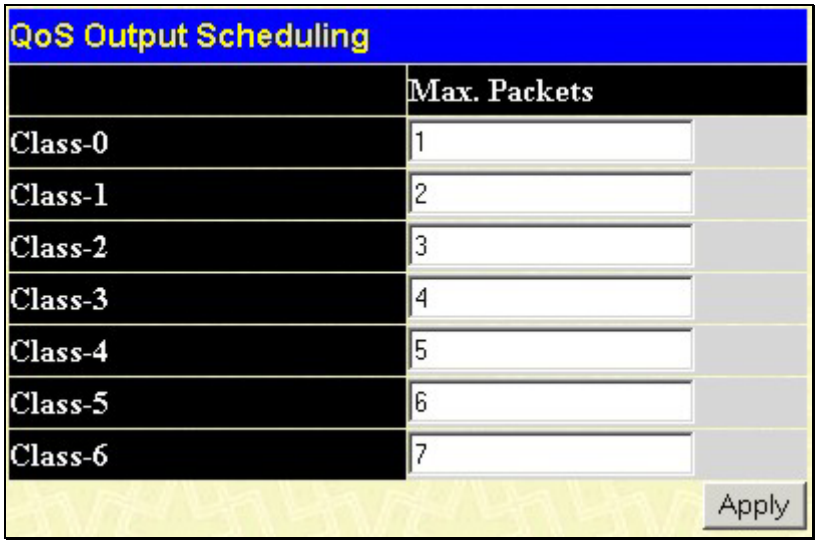


Figure 7- 51. QoS Output Scheduling Configuration window

The following values may be assigned to the QoS classes to set the scheduling.

Parameter	Description
Max. Packets	Specifies the maximum number of packets the above specified hardware priority class of service 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: Entering a 0 for the **Max Packets** field in the **QoS Output 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 xStack DGS-3400 series 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 for emptying given classes of service. To set the combination queue, enter a 0 for the Max Packets entry of the corresponding priority classes of service listed in the window above. Priority classes of service that have a *0* in the **Max Packet** field will forward packets with strict priority scheduling. The remaining classes of service, 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 classes of service with a *0* in their **Max Packet** field are empty. When a packet arrives in a priority class with a *0* in its **Max Packet** field, this class of service will automatically begin forwarding packets until it is empty. Once a priority class of service with a *0* in its **Max Packet** field is empty, the remaining priority classes of service will reset the weighted round-robin (***WRR***) cycle of forwarding packets, starting with the highest available priority class of service. Priority classes of service 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 the maximum number of packets a given priority class of service can transmit per weighted round-robin (***WRR***) scheduling cycle to be selected. This provides for a controllable CoS behavior while allowing other classes to empty as well. A value between 0 and 15 packets can be specified per priority class of service 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 class, while the other classes will follow a weight fair scheduling.

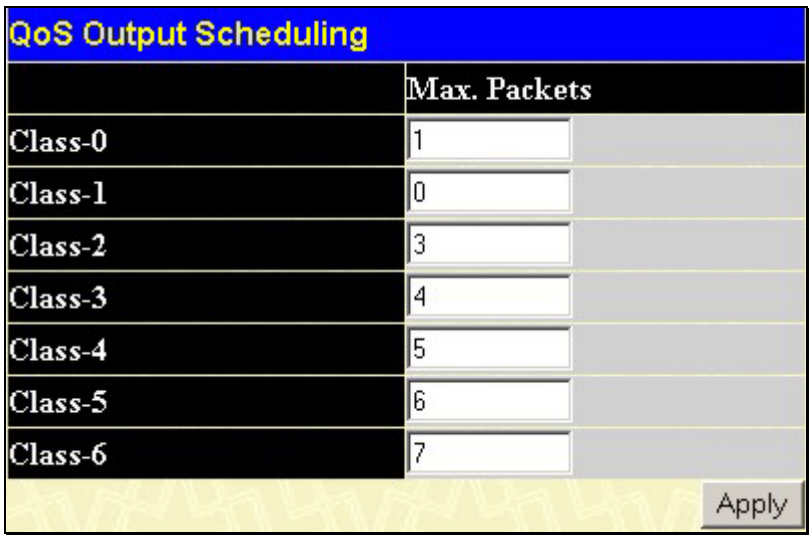


Figure 7- 52. QoS Output Scheduling window – Combination queue example

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 screen shown below.

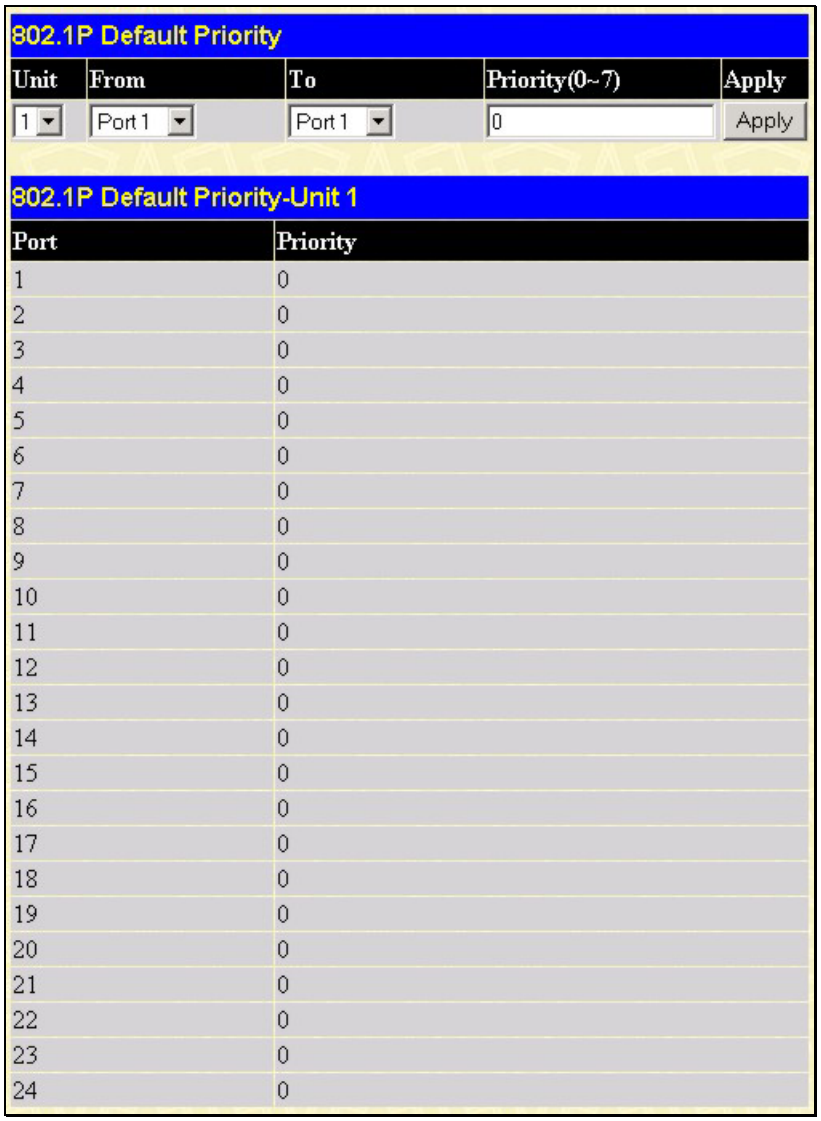


Figure 7- 53. 802.1p Default Priority window

This page allows the user to assign a default 802.1p priority to any given port on the Switch. The priority tags are numbered from 0, the lowest priority, to 7, the highest priority. To implement a new default priority, first choose a switch in the switch stack using the **Unit** pull-down menu, next choose a port range by using the **From** and **To** pull-down menus and then insert a priority value, from 0-7 in the **Priority** field. Click **Apply** to implement settings made.

802.1p User Priority

The xStack DGS-3400 switch series 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.

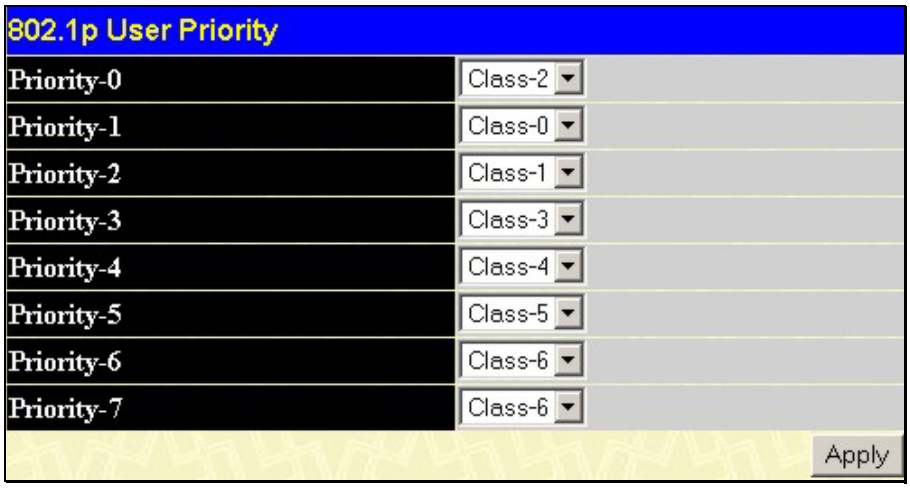


Figure 7- 54. 802.1p User Priority window

Once a priority has been assigned to the port groups on the Switch, then a Class may be assigned to each of the seven levels of 802.1p priorities. Click **Apply** to set the changes made.

Section 8

ACL (Access Control List)

Time Range

Access Profile Table

CPU Interface Filtering

Time Range

The Time Range window is used in conjunction with the Access Profile feature to determine a starting point and an ending point, based on days of the week, when an Access Profile configuration will be enabled on the Switch. Once configured here, the time range settings are to be applied to an access profile rule using the **Access Profile** table. The user may enter up to 64 time range entries on the Switch.

NOTE: The Time Range commands are based on the time settings of the Switch. Make sure to configure the time for the Switch appropriately for these commands using commands listed in the following chapter, **Time and SNTP Commands**.

To open the Time Range window, click **ACL > Time Range**, which will display the following window for the user to configure.

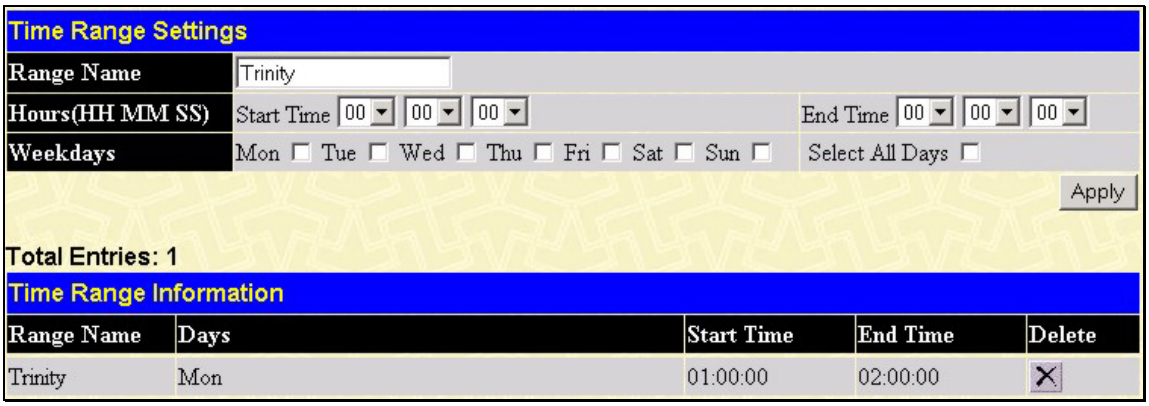


Figure 8- 1. Time Range Settings window

The user may adjust the following parameters to configure a time range on the Switch:

Parameter	Description
Range Name	Enter a name of no more than 32 alphanumeric characters that will be used to identify this time range on the Switch. This range name will be used in the **Access Profile** table to identify the access profile and associated rule to be enabled during this time range.
Hours	This parameter is used to set the time in the day that this time range is to be enabled using the following parameters: • *Start Time* - Use this parameter to identify the starting time of the time range, in hours, minutes and seconds, based on the 24-hour time system. • *End Time* - Use this parameter to identify the ending time of the time range, in hours, minutes and seconds, based on the 24-hour time system.
Weekdays	Use the check boxes to select the corresponding days of the week that this time range is to be enabled. Click the **Select All Days** check box to configure this time range for every day of the week.

Click **Apply** to implement changes made. Currently configured entries will be displayed in the **Time Range Information** table in the bottom half of the window shown above.

Access Profile Table

Access profiles allow you to establish criteria to determine whether 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 **ACL** folder and click on the **Access Profile Table** link. This will open the **Access Profile Table** page, as shown below.

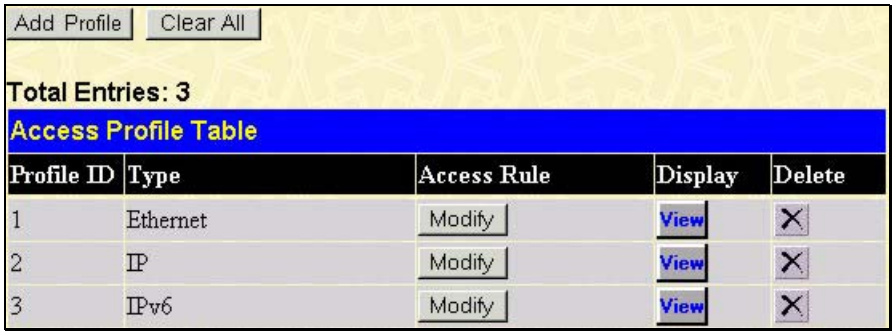


Figure 8- 2. Access Profile Table

To add an entry to the **Access Profile Table**, click the **Add Profile** button. This will open the **Access Profile Configuration** page, as shown below. There are three **Access Profile Configuration** pages; one for **Ethernet** (or MAC address-based) profile configuration, one for **IP** address-based profile configuration and one **IPv6**. You can switch between the three **Access Profile Configuration** pages by using the **Type** drop-down menu. The page shown below is the **Ethernet Access Profile Configuration** page. To remove all access profiles from this table, click **Clear All**.

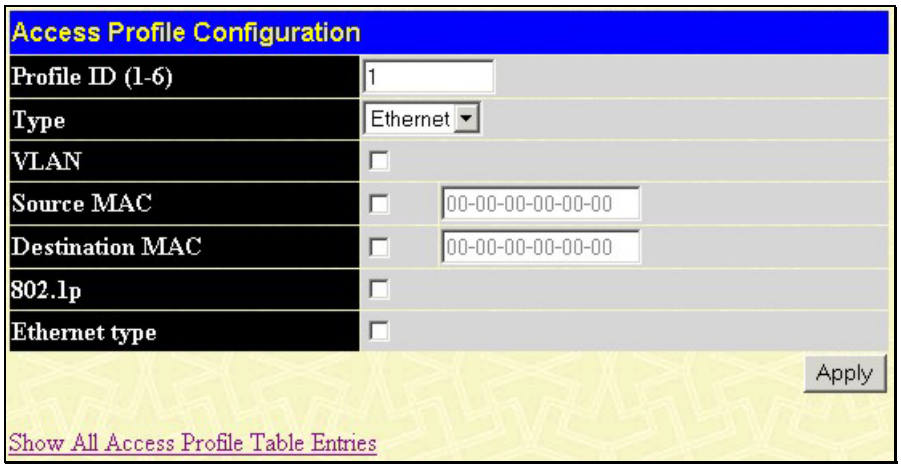


Figure 8- 3. Access Profile Configuration (Ethernet)

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

Parameter	Description
Profile ID (1-6)	Type in a unique identifier number for this profile set. This value can be set from 1 - 6.
Type	Select profile based on Ethernet (MAC Address), IP or IPv6 address. This will change the menu 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 *IPv6* to instruct the Switch to examine the IPv6 address in each frame's 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.

To view the settings for a created profile, click its corresponding View button in the Access Profile table, revealing the following window.

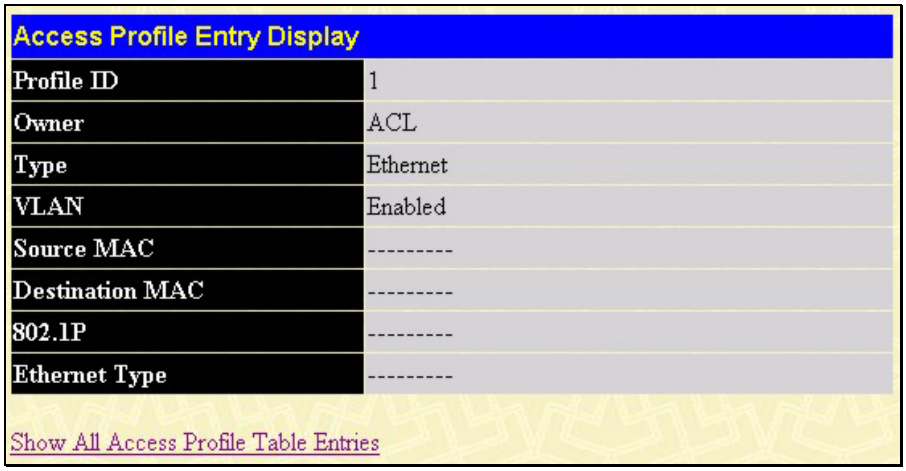


Figure 8- 4. Access Profile Entry Display for Ethernet

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

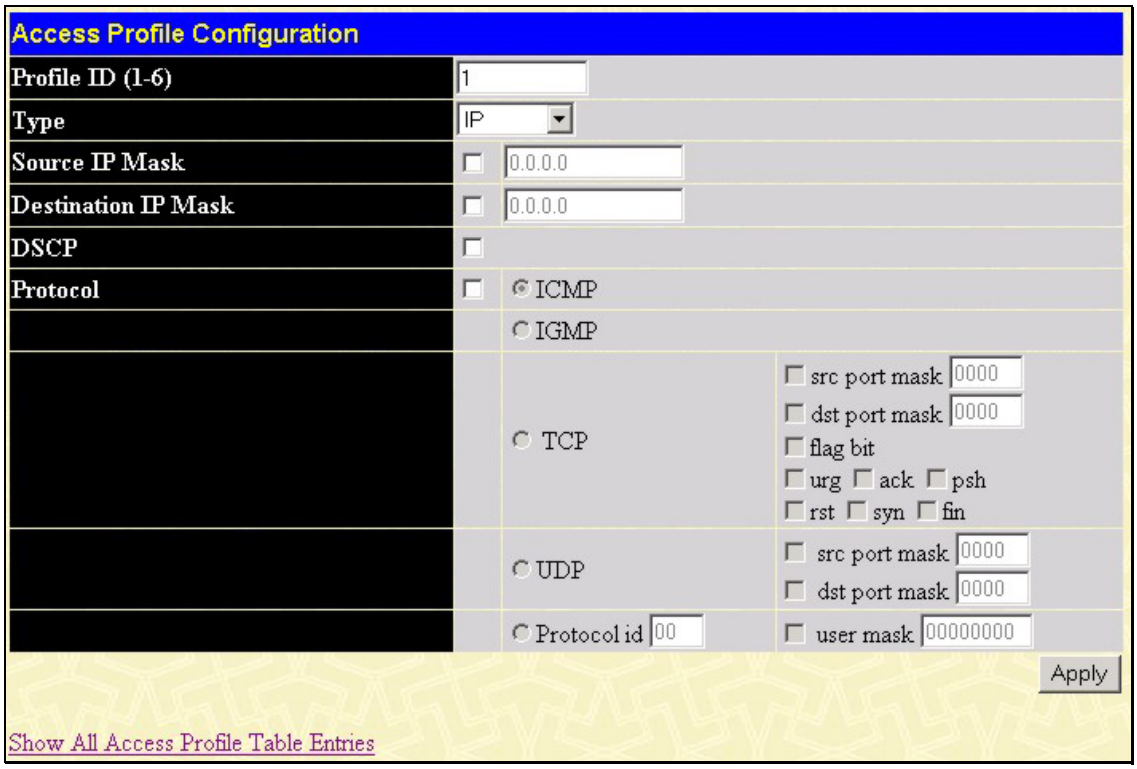


Figure 8- 5. Access Profile Configuration (IP)

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

Parameter	Description
Profile ID (1-6)	Type in a unique identifier number for this profile set. This value can be set from 1 -6.
Type	Select profile based on Ethernet (MAC Address), IP or IPv6 address. This will change the menu 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 *IPv6* to instruct the Switch to examine the IPv6 address in each frame's header.
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. Then the user must 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 *IGMP* to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. 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. • *src port mask* - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. • *dst port mask* - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. • *flag bit* - 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). 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 UDP port mask for the source port in hex form (hex 0x0-0xffff). • *dst port mask* - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). *protocol id* - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff).

To view the settings for a created profile, click its corresponding View button in the Access Profile table, revealing the following window.

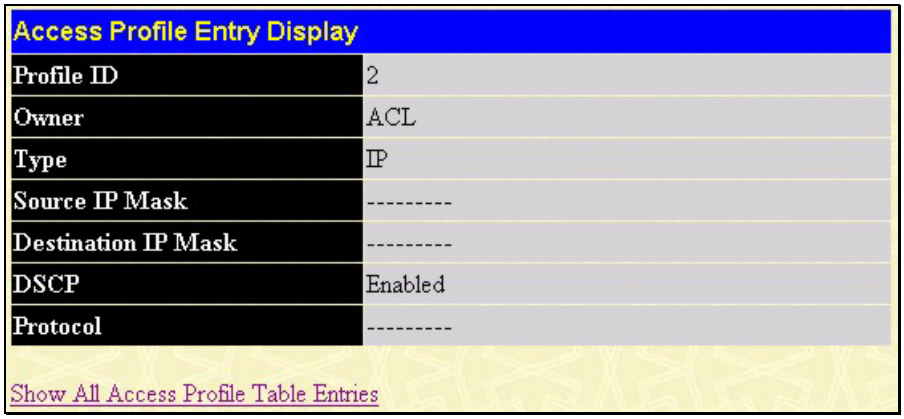


Figure 8- 6. Access Profile Entry Display for IP

The page shown below is the **IPv6** configuration window.

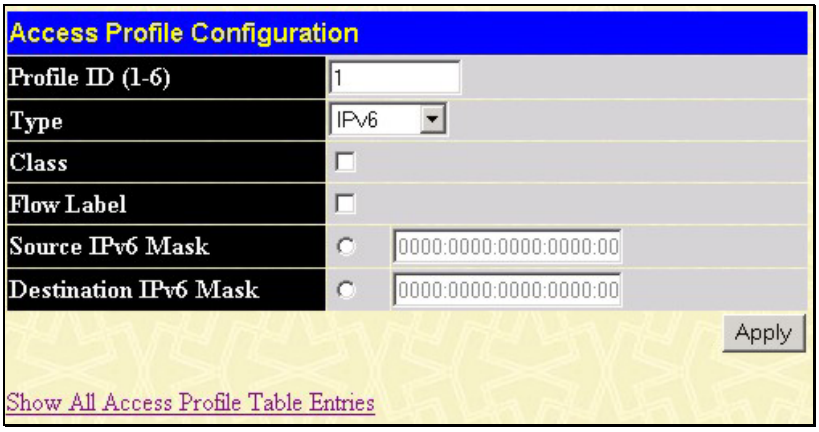


Figure 8- 7. Access Profile Configuration window (IPv6)

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

Parameter	Description
Profile ID (1-6)	Type in a unique identifier number for this profile set. This value can be set from 1 - 6.
Type	Select profile based on Ethernet (MAC Address), IP or IPv6 address. This will change the menu 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 *IPv6* to instruct the Switch to examine the IPv6 address in each frame's header.
Class	Checking this field will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
Flow Label	Checking this field will instruct the Switch to examine the *flow label* field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Source IPv6 Mask	The user may specify an IP address mask for the source IPv6 address by checking the corresponding box and entering the IP address mask.
Destination IPv6 Mask	The user may specify an IP address mask for the destination IPv6 address by checking the corresponding box and entering the IP address mask.

Click **Apply** to implement changes made.

To view the settings for a created profile, click its corresponding View button in the Access Profile table, revealing the following window.

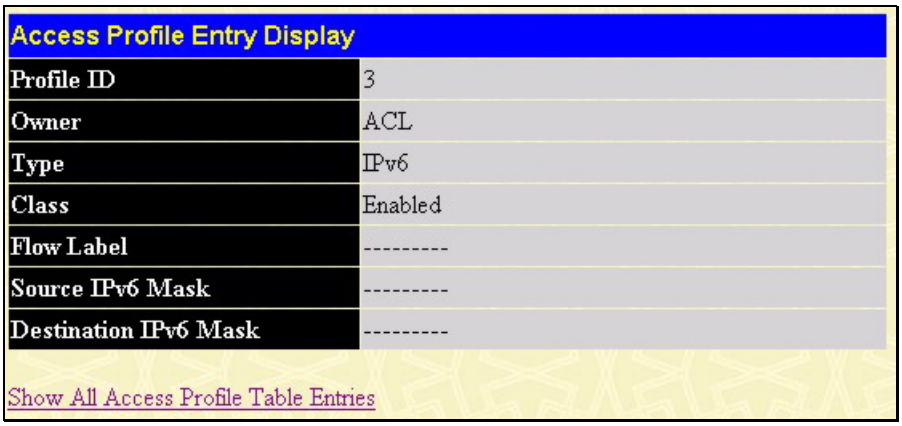


Figure 8- 8. Access Profile Entry Display for IPv6

To establish the rule for a previously created Access Profile:

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

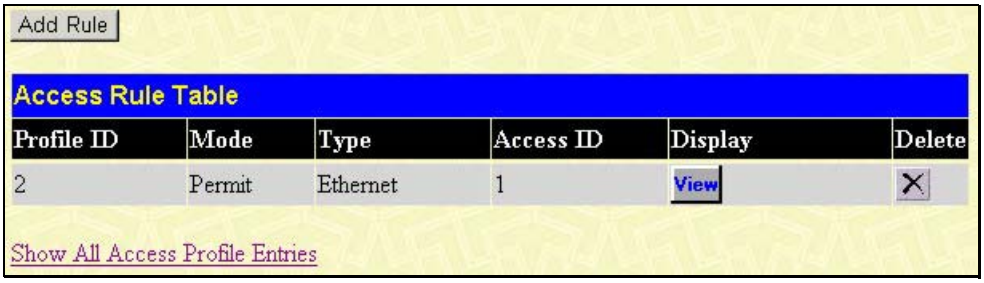


Figure 8- 9. Access Rule Table

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

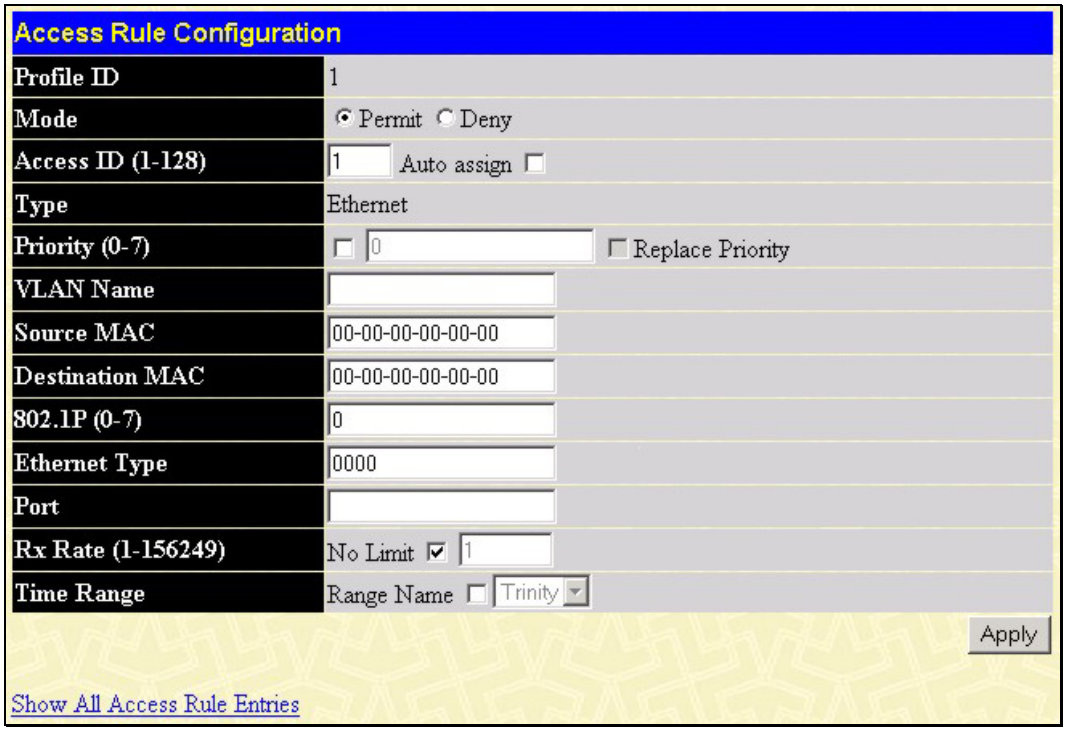


Figure 8- 10. Access Rule Configuration window - Ethernet

To set the Access Rule for Ethernet, 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 - 128. **Auto Assign** – Checking this field will instruct the Switch to automatically assign an Access ID for the rule being created.
Type	Selected profile based on Ethernet (MAC Address), IP address or IPv6 address *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. *IPv6* instructs the Switch to examine the IPv6 address in each frame's header.
Priority (0-7)	This parameter is to be specified 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* – 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 command, before forwarding it on to the specified CoS queue. 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.
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 0-7 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 0-9.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the switch in the switch stack into this field. When a range of ports is to be configured, the **Auto Assign** check box MUST be clicked in the **Access ID** field of this window. If not, the user will be presented with an error message and the access rule will not be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3 - 2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Entering *all* will denote all ports on the Switch.
Rx Rate	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an Rx rate of 10 then the ingress rate is 640kbit/sec.) The user many select a value between *1-156249* or *No Limit*. The default setting is No Limit.
Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range** window. This will set specific times when this access rule will be implemented on the Switch.

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

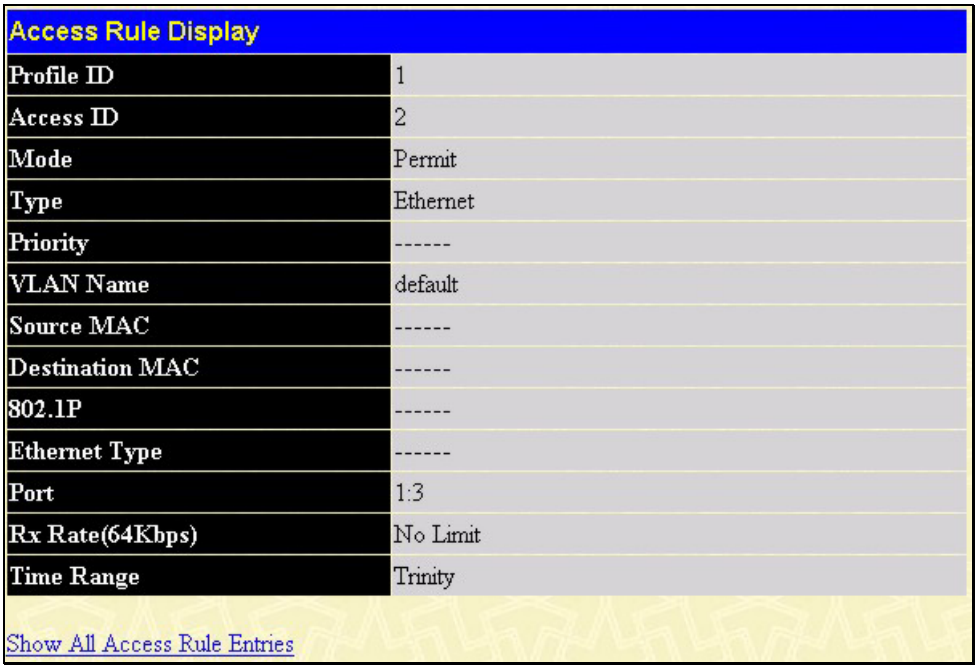


Figure 8- 11. Access Rule Display window (Ethernet)

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

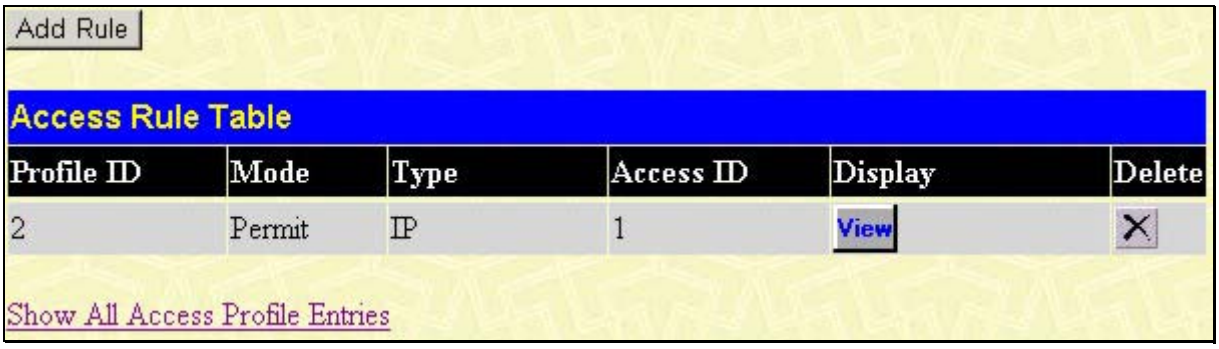


Figure 8- 12. Access Rule Table window – IP

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

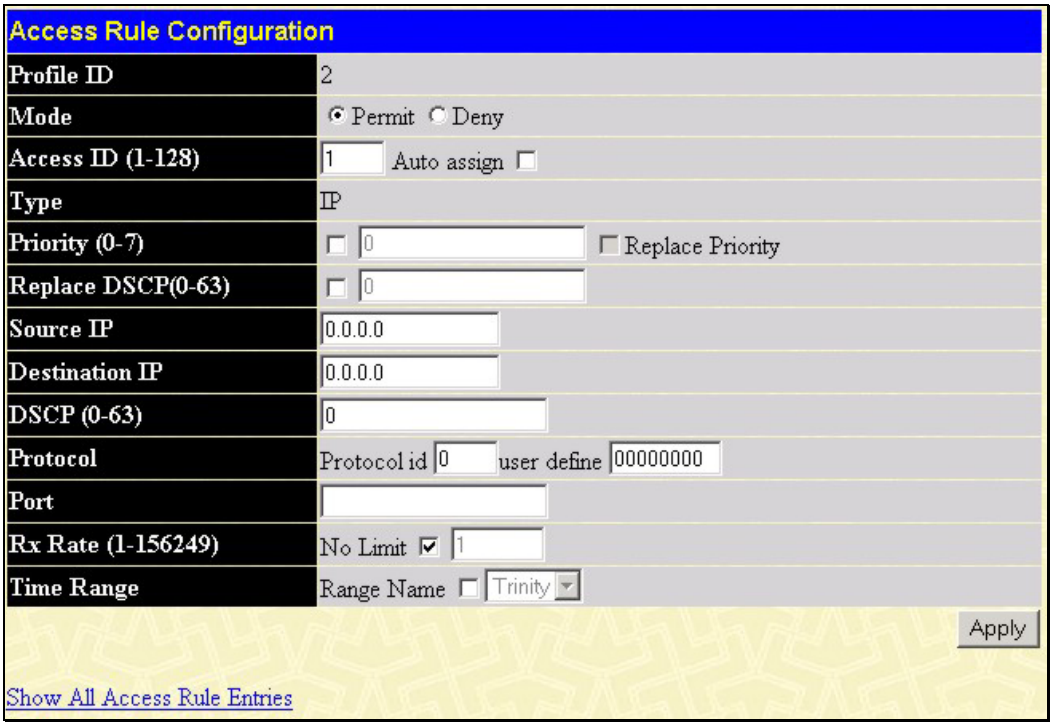


Figure 8- 13. Access Rule Configuration window (IP)

Configure the following **Access Rule Configuration** settings for IP:

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 - 128. **Auto Assign** – Checking this field will instruct the Switch to automatically assign an Access ID for the rule being created.
Type	Selected profile based on Ethernet (MAC Address), IP address or IPv6 address. *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. *IPv6* instructs the Switch to examine the IPv6 address in each frame's 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. 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 command, before forwarding it on to the specified CoS queue. 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.
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	Specifies that the Switch will examine the Protocol field in each packet and if this field contains the value entered here, apply the appropriate rules. • *user define* – Enter a hexadecimal value in the form *0x0-0xffffffff* that will identify the protocol to be discovered in the packet header.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the switch in the switch stack into this field. When a range of ports is to be configured, the **Auto Assign** check box MUST be clicked in the **Access ID** field of this window. If not, the user will be presented with an error message and the access rule will not be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3 - 2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Entering *all* will denote all ports on the Switch.
Rx Rate	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an Rx rate of 10 then the ingress rate is 640kbit/sec.) The user many select a value between 1- 156249 or *No Limit*. The default setting is No Limit.
Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range** window. This will set specific times when this access rule will be implemented on the Switch.

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

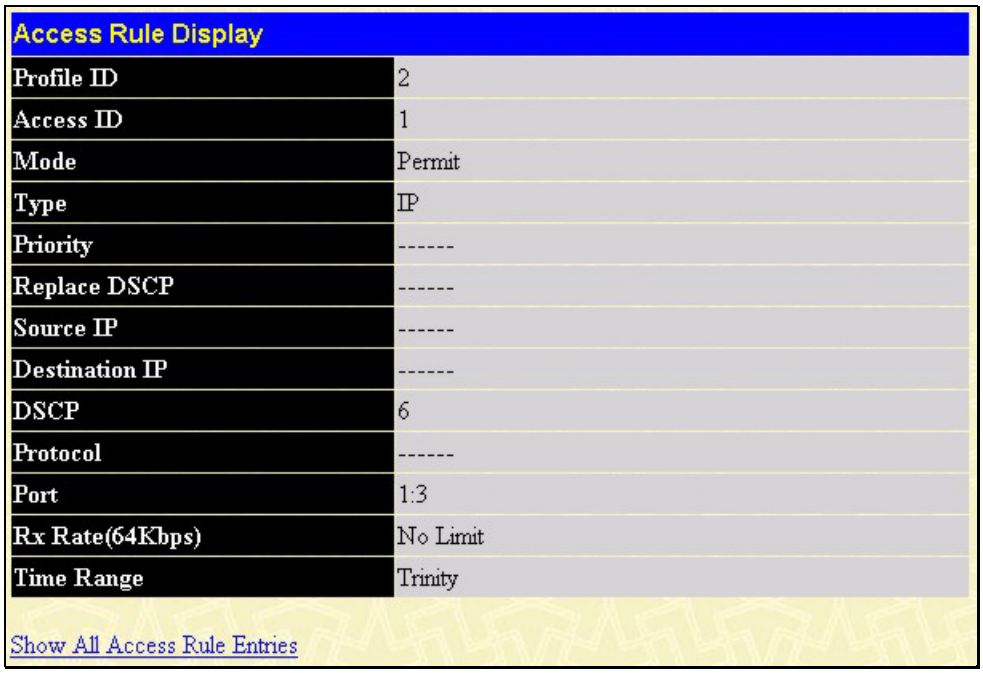


Figure 8- 14. Access Rule Display window (IP)

To configure the Access Rule for **IPv6**, open the **Access Profile Table** and click **Modify** for an **IPv6** entry. This will open the following screen:

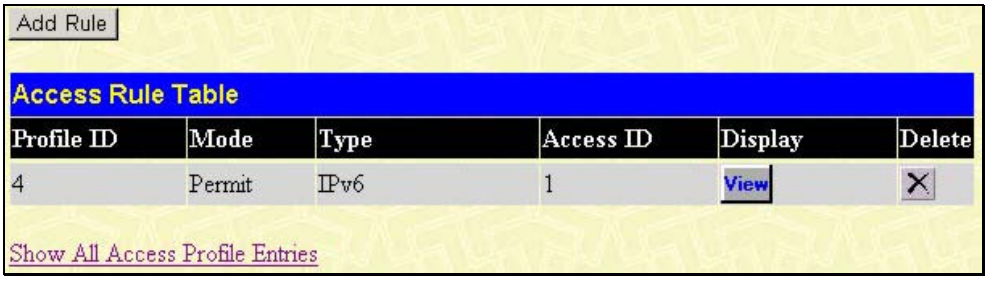


Figure 8- 15. Access Rule Table

Click **Add Rule** to open the next screen to configure the IPv6 entry for an access rule.

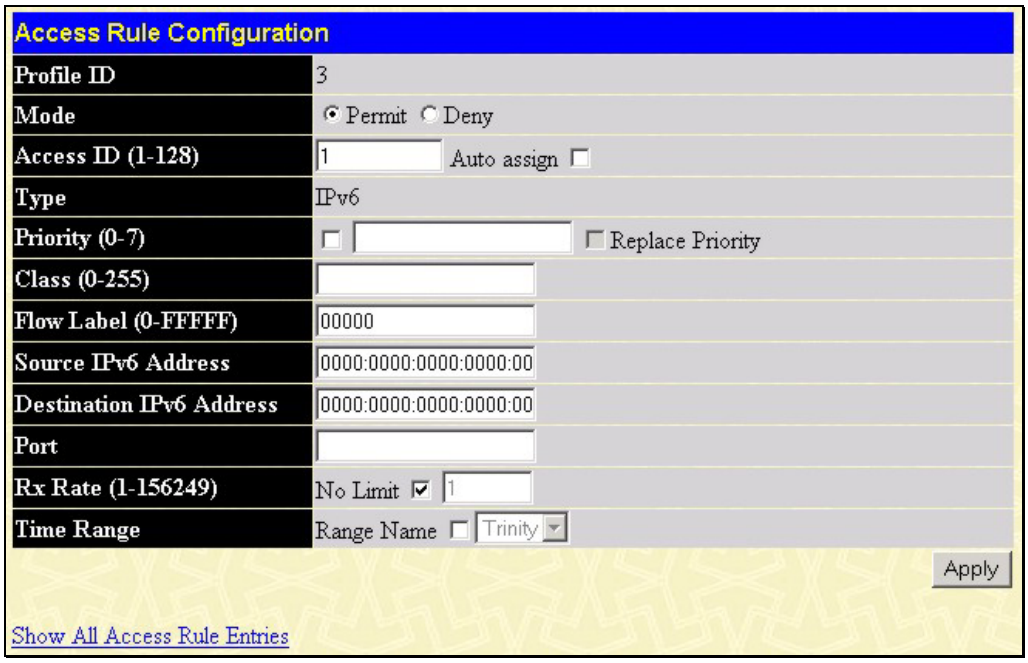


Figure 8- 16. Access Rule Configuration – IPv6

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 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 rule. This value can be set from 1 - 128.
Type	Selected profile based on Ethernet (MAC Address), IP address or IPv6 address *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. *IPv6* instructs the Switch to examine the IPv6 address in each frame's header.
Priority	This parameter is specified 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* – Click the corresponding box 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 command, before forwarding it on to the specified CoS queue. 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.
Class	Entering a value between *0* and *255* will instruct the Switch to examine the class field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field of IPv4.
Flow Label	Configuring this field, in hex form, will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Source IPv6 Address	The user may specify an IP address mask for the source IPv6 address by entering the IP address mask, in hex form.

Destination IPv6 Address	The user may specify an IP address mask for the destination IPv6 address by and entering the IP address mask, in hex form.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the switch in the switch stack into this field. When a range of ports is to be configured, the **Auto Assign** check box MUST be clicked in the **Access ID** field of this window. If not, the user will be presented with an error message and the access rule will not be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3 - 2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Entering *all* will denote all ports on the Switch.
Rx Rate	Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an Rx rate of 10 then the ingress rate is 640kbit/sec.) The user many select a value between 1- 156249 or *No Limit*. The default setting is No Limit.
Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range** window. This will set specific times when this access rule will be implemented on the Switch.

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

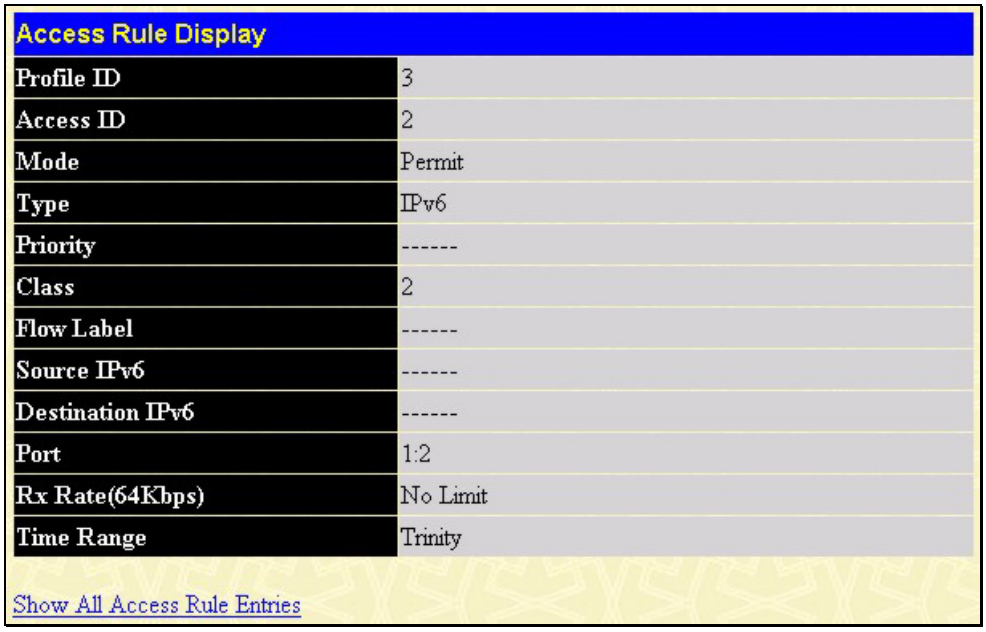


Figure 8- 17. Access Rule Display (IPv6)

CPU Interface Filtering

Due to a chipset limitation and needed extra switch security, the xStack DGS-3400 Series switch incorporates CPU Interface filtering. This added feature increases the running security of the Switch by enabling the user to create a list of access rules for packets destined for the Switch's CPU interface. Employed similarly to the Access Profile feature previously mentioned, CPU interface filtering examines Ethernet, IP and Packet Content Mask packet headers destined for the CPU and will either forward them or filter them, based on the user's implementation. As an added feature for the CPU Filtering, the xStack DGS-3400 Series switch allows the CPU filtering mechanism to be enabled or disabled globally, permitting the user to create various lists of rules without immediately enabling them.

Creating an access profile for the CPU 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.

CPU Interface Filtering State Settings

In the following window, the user may globally enable or disable the CPU Interface Filtering mechanism by using the pull-down menu to change the running state. To access this window, click **ACL > CPU Interface Filtering > CPU Interface Filtering State**. Choose **Enabled** to enable CPU packets to be scrutinized by the Switch and **Disabled** to disallow this scrutiny.

Figure 8- 18. CPU Interface Filtering State Settings window

CPU Interface Filtering Table

The **CPU Interface Filtering Table** displays the CPU Access Profile Table entries created on the Switch. To view the configurations for an entry, click the hyperlinked **Profile ID** number.

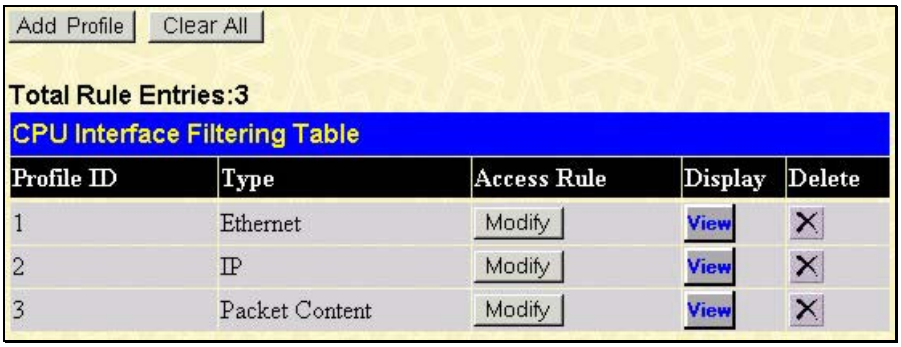


Figure 8- 19. CPU Interface Filtering Table

To add an entry to the **CPU Interface Filtering Table**, click the **Add Profile** button. This will open the **CPU Interface Filtering Configuration** page, as shown below. To remove all CPU Interface Filtering Table entries, click the **Clear All** button. There are three **Access Profile Configuration** pages; 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 between the three **Access Profile Configuration** pages by using the **Type** drop-down menu. The page shown below is the **Ethernet CPU Interface Filtering Configuration** page.

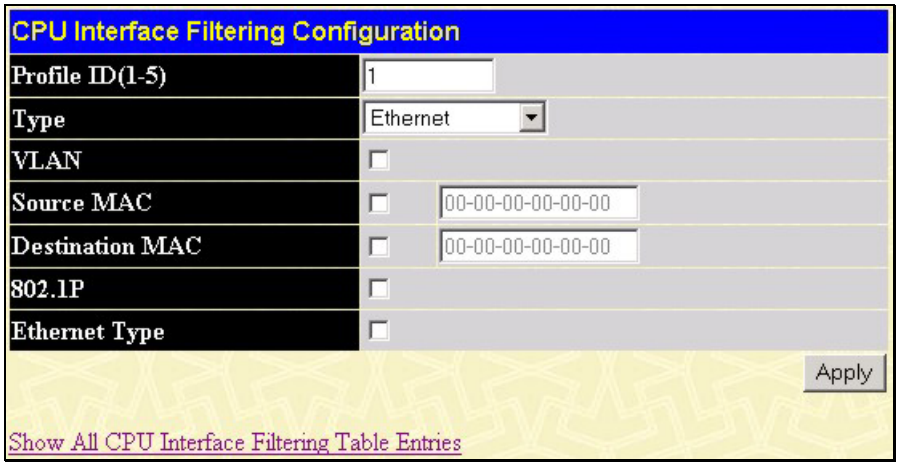


Figure 8- 20. CPU Interface Filtering Configuration window – Ethernet

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from 1 - 5.
Type	Select profile based on Ethernet (MAC Address), IP address or packet content mask. This will change the menu according to the requirements for the type of profile. Select *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	Enter a value from 0-7 to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click **Apply** to set this entry in the Switch's memory.

To view the settings of a previously correctly created profile, click View in the **Access Profile Table** to view the following screen:

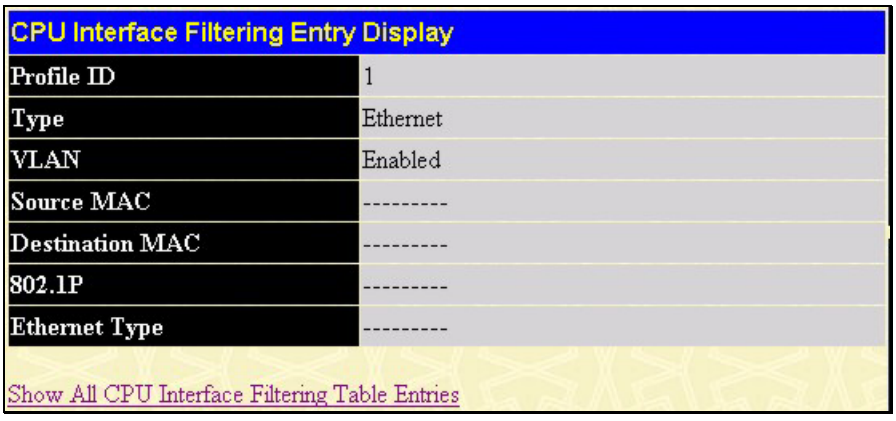


Figure 8- 21. CPU Interface Filtering Entry Display for Ethernet

The page shown below is the **CPU Interface Filtering Profile Configuration** for **IP** page.

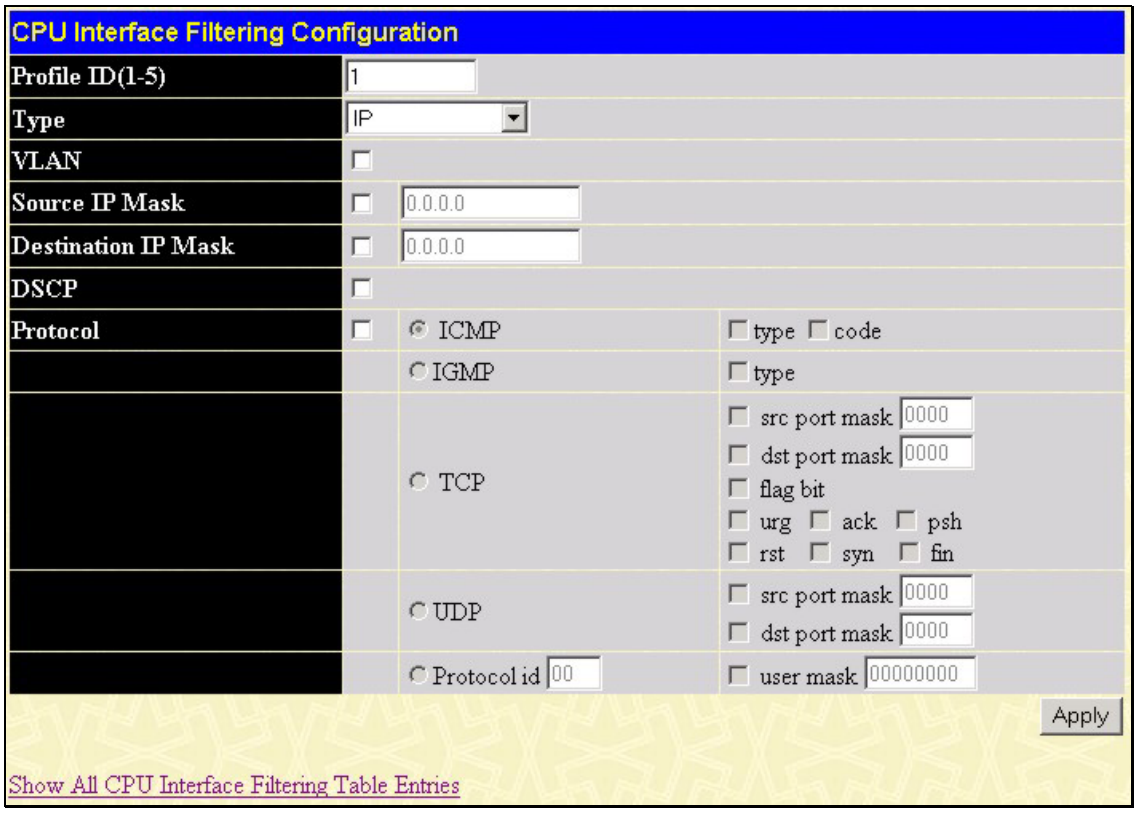


Figure 8- 22. CPU Interface Filtering Configuration window- IP

The following parameters may be configured for the IP CPU filter.

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from 1 - 5.
Type	Select profile based on Ethernet (MAC Address), IP address or Packet Content Mask. This will change the menu according to the requirements for the type of profile. Select *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 a source port mask and/or a destination port mask is to be

	specified. 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 filter. • *dst port mask* - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. 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 UDP port mask for the source port in hex form (hex 0x0-0xffff). • *dst port mask* - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). *Protocol id* - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff).

Click **Apply** to set this entry in the Switch's memory.

To view the settings of a previously correctly created profile, click View in the **Access Profile Table** to view the following screen:

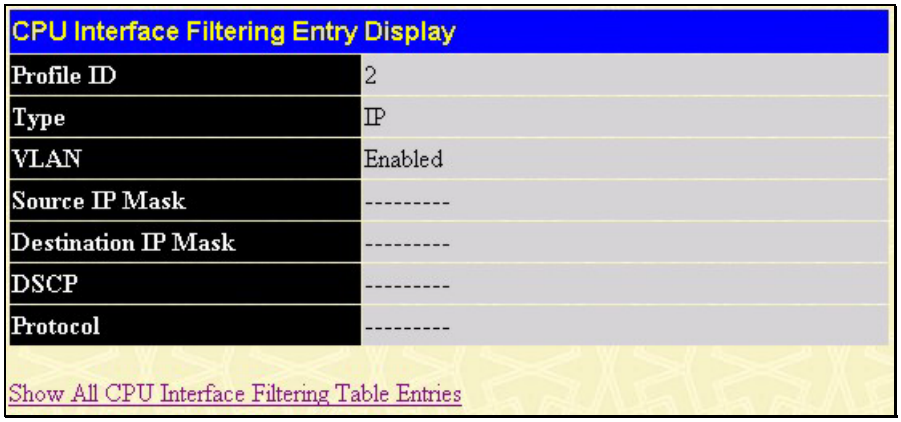


Figure 8- 23.CPU Interface Filtering Entry Display for IP

The page shown below is the **Packet Content Mask** configuration window.

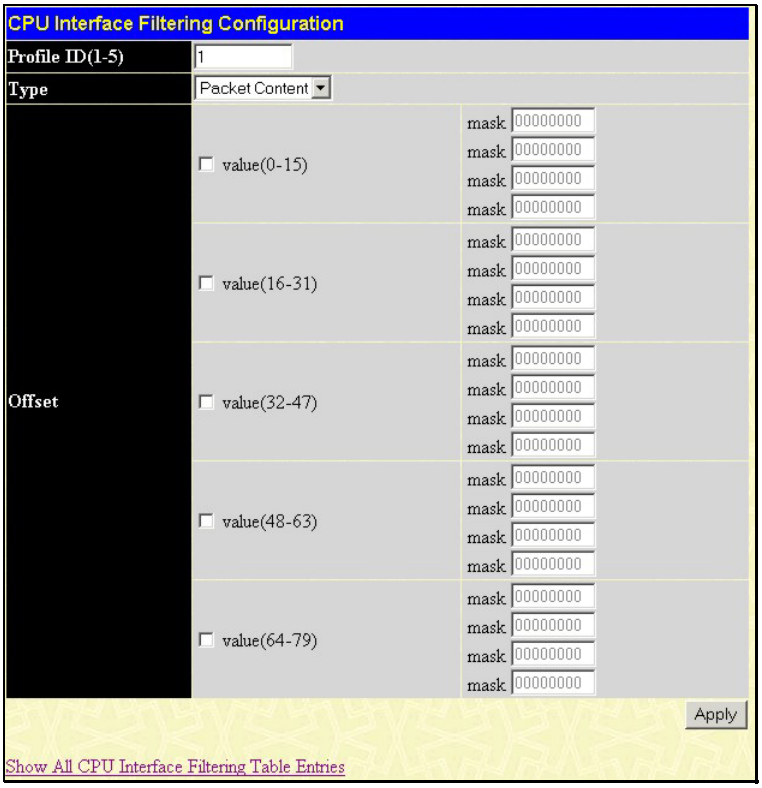


Figure 8- 24. CPU Interface Filtering Configuration window- Packet Content

This screen 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 (1-5)	Type in a unique identifier number for this profile set. This value can be set from 1 - 5.
Type	Select profile based on Ethernet (MAC Address), IP address or packet content mask. This will change the menu according to the requirements for the type of profile. Select *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.

Click **Apply** to implement changes made.

To view the settings of a previously correctly created profile, click View in the **Access Profile Table** to view the following screen:

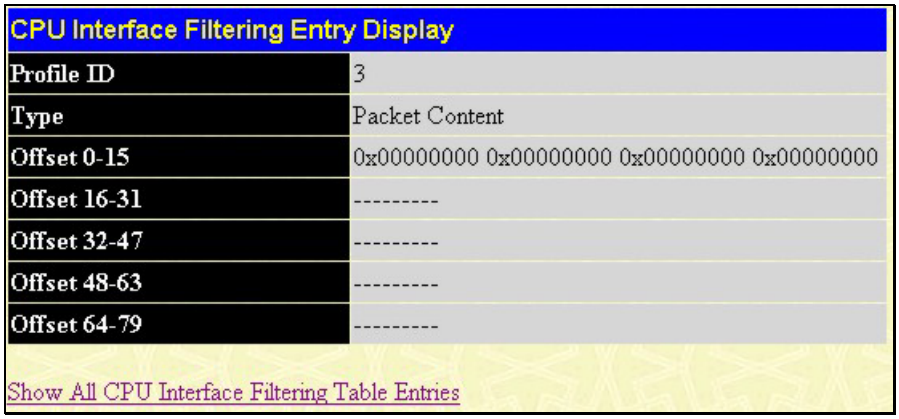


Figure 7- 55. CPU Interface Filtering Display for Packet Content

To establish the rule for a previously created CPU Access Profile:

In the **ACL** folder, click the **CPU Interface Filtering > CPU Interface Filtering Table** to open the **CPU Interface Filtering Table**.

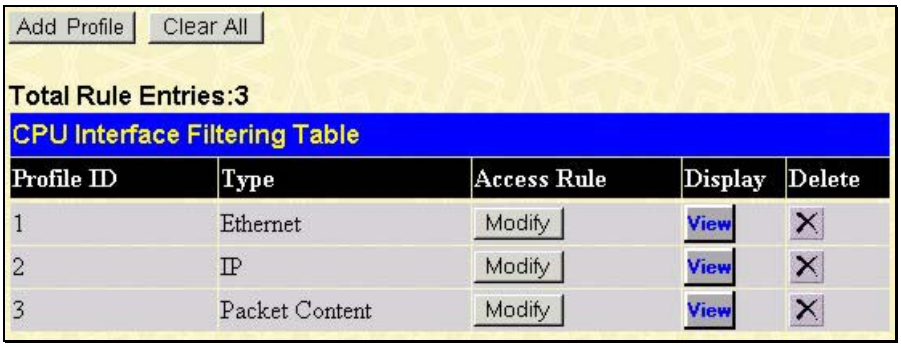


Figure 8- 25. CPU Interface Filtering Table

In this window, the user may add a rule to a previously created CPU access profile by clicking the corresponding Modify button of the entry to configure, **Ethernet, IP** or **Packet Content**. Each entry will open a new and unique window, as shown in the examples below.

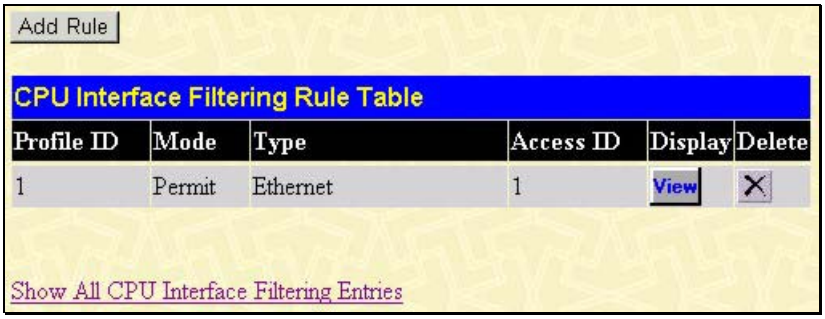


Figure 8- 26. CPU Interface Filtering Table – Ethernet

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

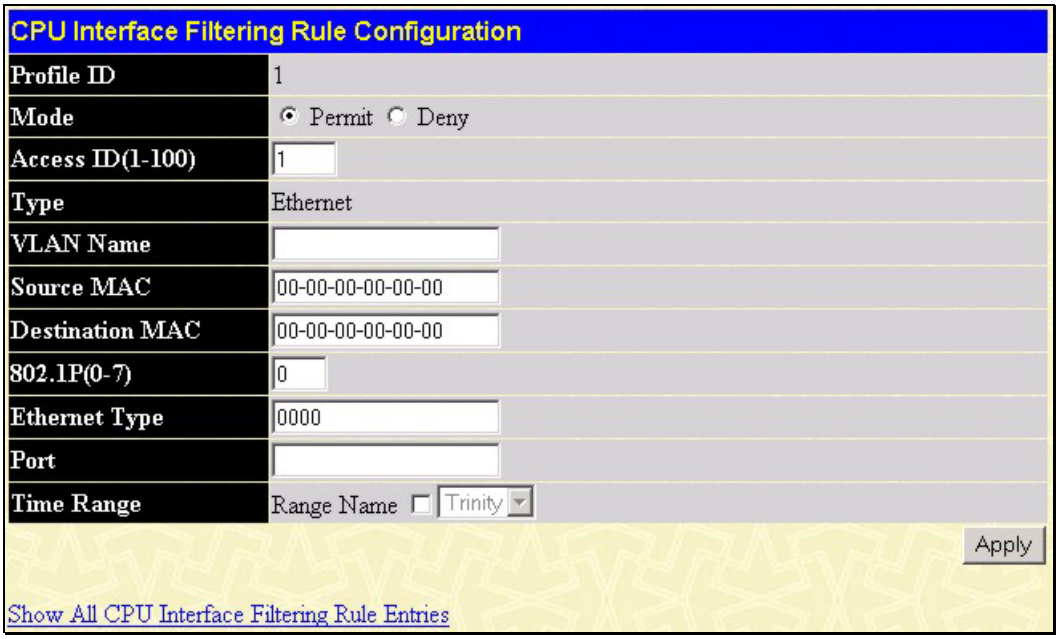


Figure 8- 27. CPU Interface Filtering Rule Configuration – Ethernet

To set the CPU Interface Filtering Rule for Ethernet, 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 and priority. This value can be set from 1 - 100.
Type	Selected profile based on Ethernet (MAC Address), IP address or Packet Content. *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.
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)	Specify the rule be based on 802.1p priority.
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 a combination of letters and numbers ranging from a-f and from 0-9.
Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range** window. This will set specific times when this access rule will be implemented on the Switch.

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

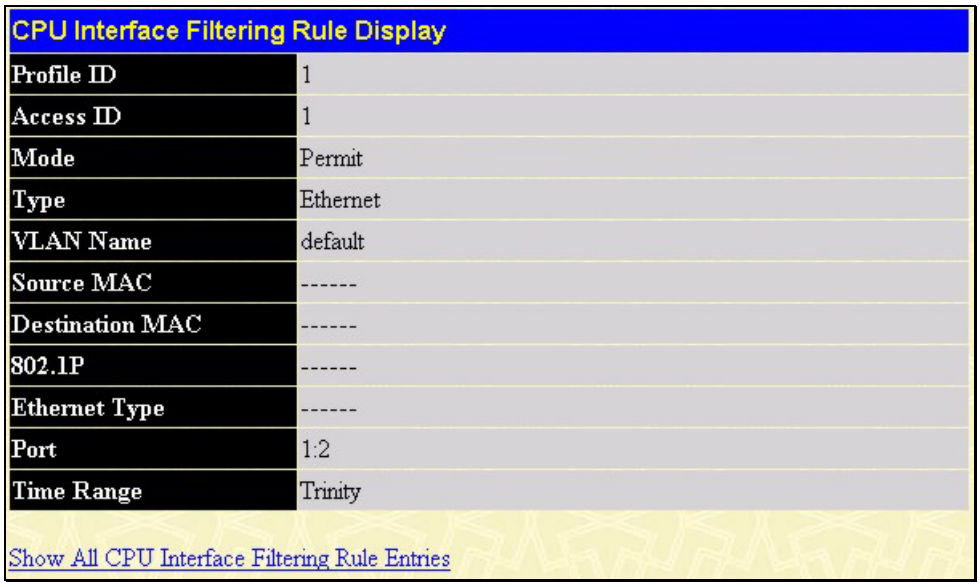


Figure 8- 28. CPU Interface Filtering Rule Display – Ethernet

The following window is the **CPU Interface Filtering Rule Table** for IP.

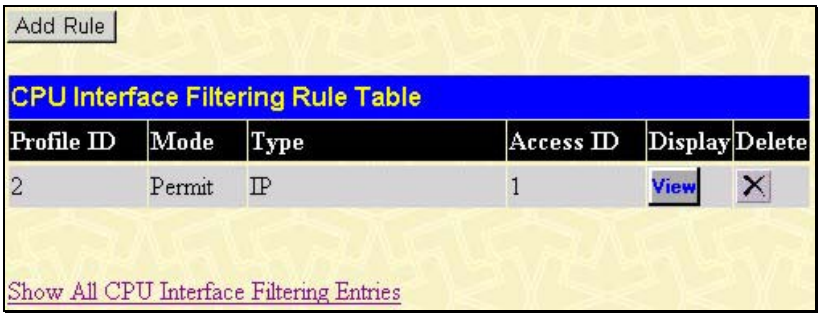


Figure 8- 29. CPU Interface Filtering Rule Table – IP

To create a new rule set for an access profile click the **Add Rule** button. A new window is displayed. To remove a previously created rule, click the corresponding button. The following window is used for the IP Rule configuration.

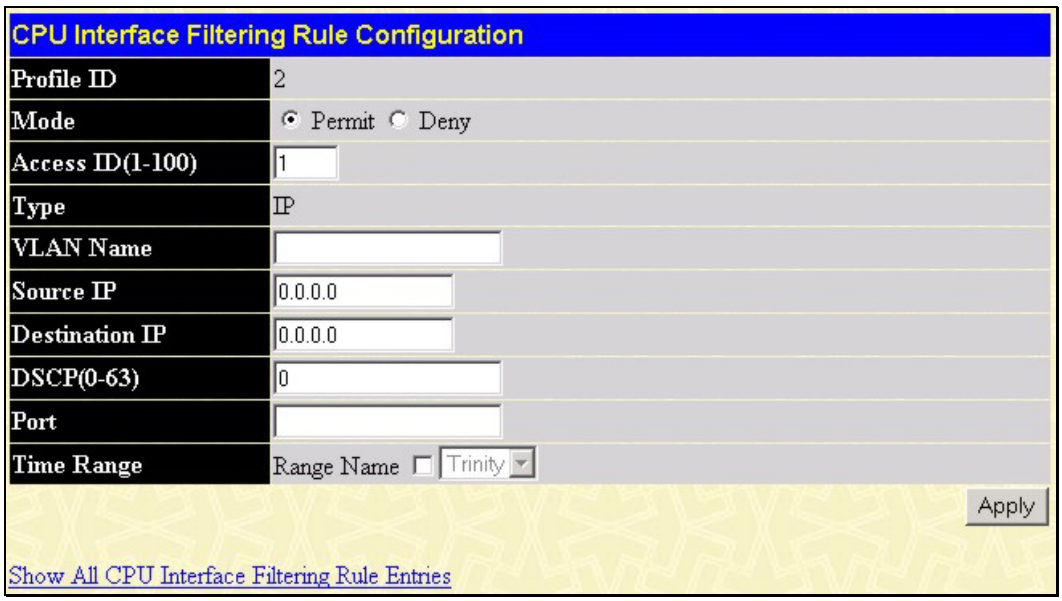


Figure 8- 30. CPU Interface Filtering Rule Configuration – IP

Configure the following **Access Rule Configuration** settings for IP:

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 - 100.
Type	Selected profile based on Ethernet (MAC Address), IP address or Packet Content. *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.
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.
Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range** window. This will set specific times when this access rule will be implemented on the Switch.

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

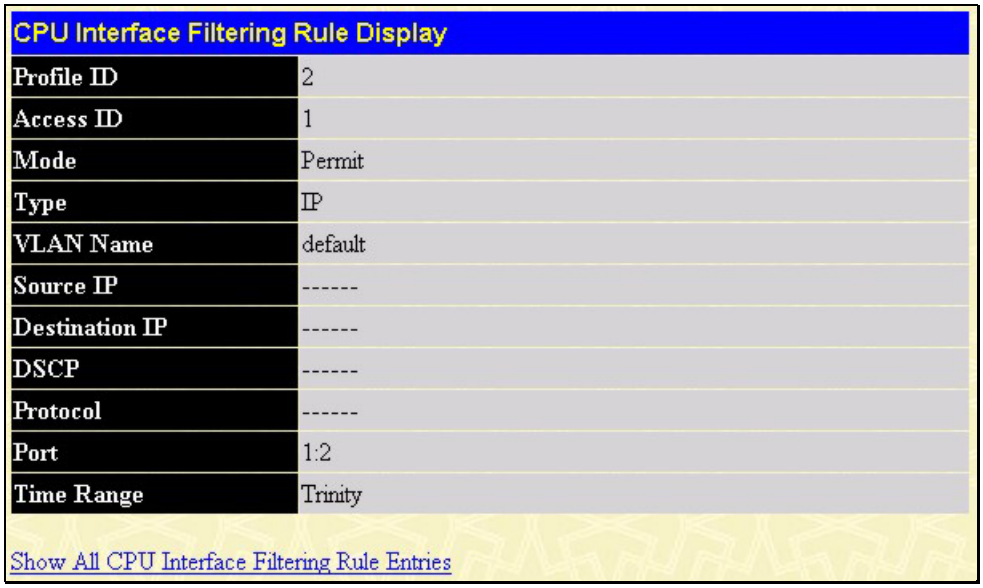


Figure 8- 31. CPU Interface Filtering Rule Display - IP

The following window is the **CPU Interface Filtering Rule Table** for Packet Content.

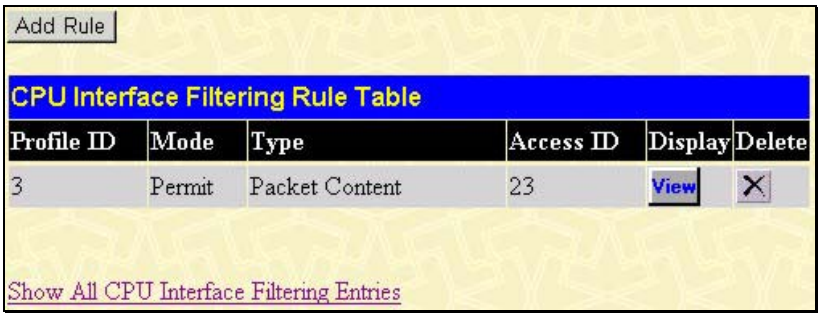


Figure 8- 32. CPU Interface Filtering Rule Table – Packet Content

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

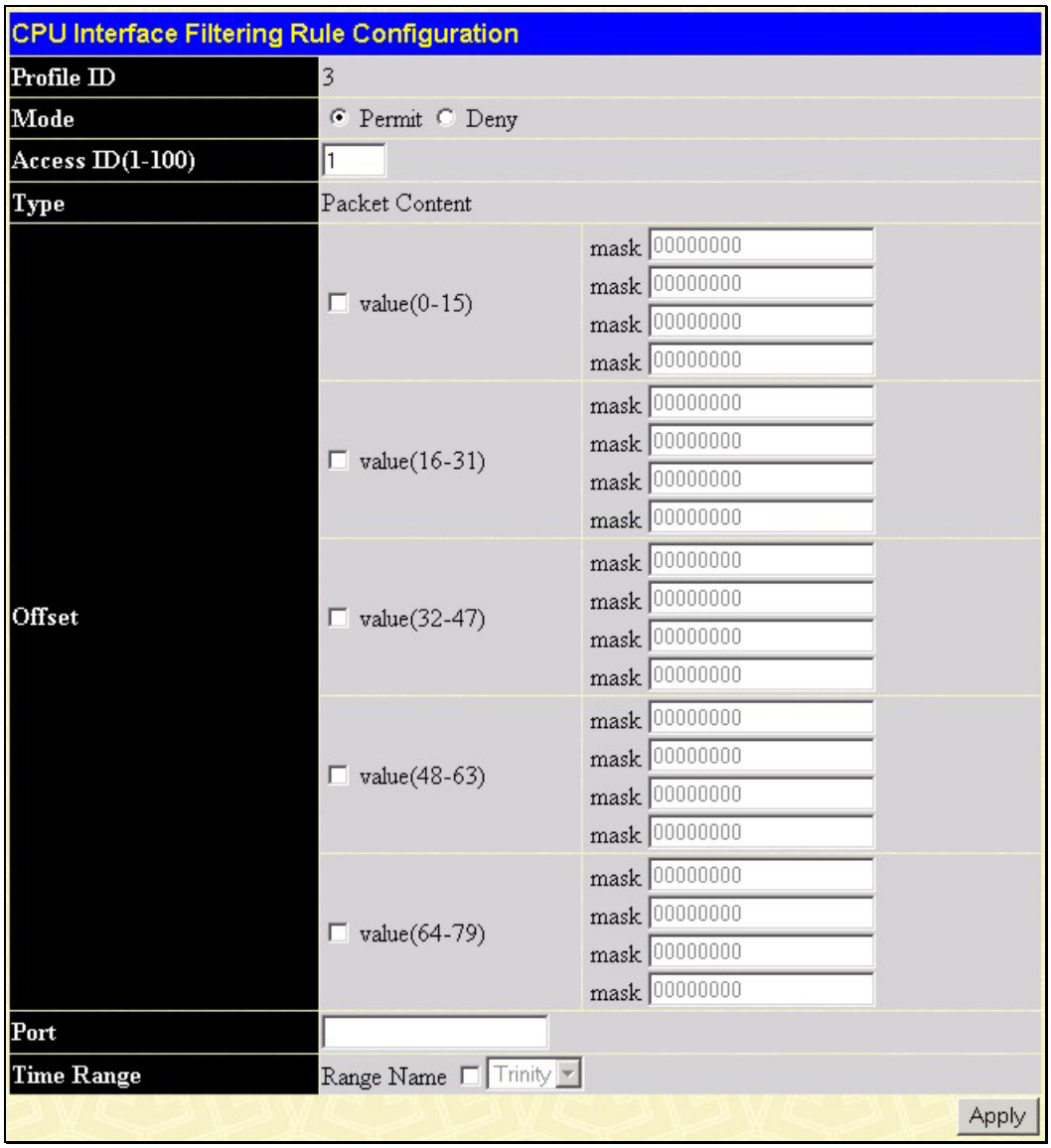


Figure 8- 33. CPU Interface Filtering Rule Configuration - Packet Content

To set the Access Rule for Packet Content, 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 - 100.
Type	Selected profile based on Ethernet (MAC Address), IP address or Packet Content. *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.
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	Type in the port or range of ports that will be affected.
Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range** window. This will set specific times when this access rule will be implemented on the Switch.

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

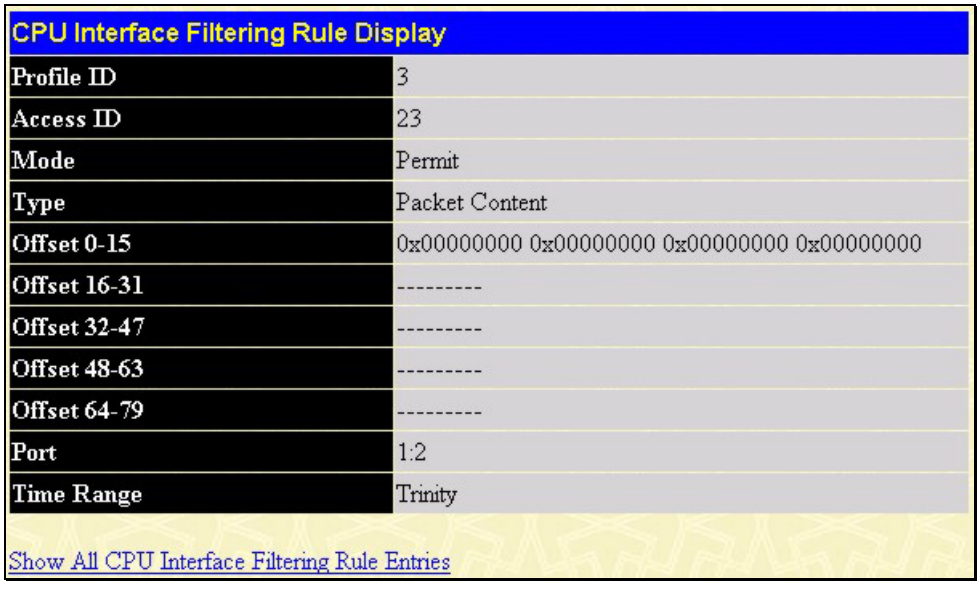


Figure 8- 34. CPU Interface Filtering Rule Display – Packet Content

Section 9

Security

Traffic Control

Port Security

802.1X

Trust Host

Access Authentication Control

Traffic Segmentation

SSL

SSH

JWAC

Traffic Control

On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase do to a malicious endstation on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the **Drop** option of the **Action** field in the window below.

The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the Countdown field.

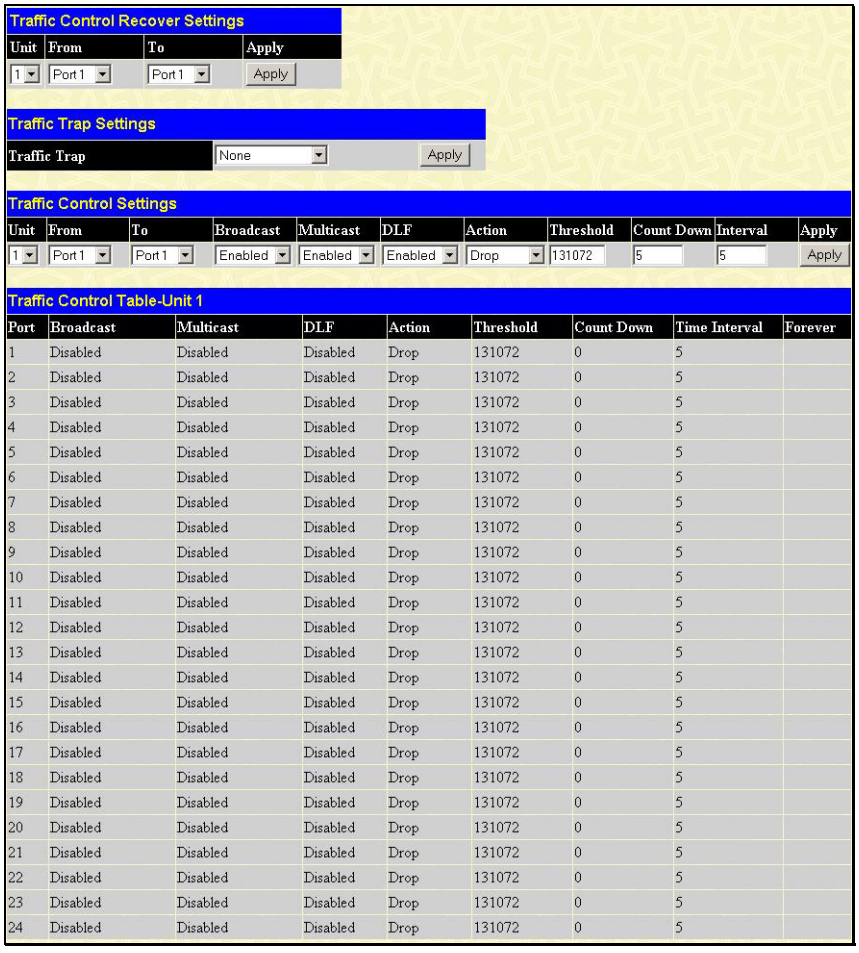


Figure 9- 1. Traffic Control Settings window

If this field times out and the packet storm continues, the port will be placed in a Shutdown Forever mode which will produce a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, the only method of recovering this port is to manually recoup it using the **Port Configuration** window in the **Administration** folder and selecting the disabled port and returning it to an Enabled status. To utilize this method of Storm Control, choose the **Shutdown** option of the **Action** field in the window below.

Use the **Traffic Control** menu to enable or disable storm control and adjust the threshold for multicast and broadcast storms, as well as DLF (Destination Look Up Failure). To view the following window, click **Security > Traffic Control**:

To configure **Traffic Control**, enable or disable the **Broadcast Storm**, **Multicast Storm** and **DLF** using their corresponding pull-down menus. Click **Apply** to implement changes made.

Parameter	Description
Traffic Control Recover	
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.
From… To	Select the ports to be shutdown.
Traffic Trap Configuration	
Traffic Trap	Enable sending of Storm Trap messages when the type of action taken by the Traffic Control function in handling a Traffic Storm is one of the following: • *None* – Will send no Storm trap warning messages regardless of action taken by the Traffic Control mechanism. • *Storm Occurred* – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only. • *Storm Cleared* – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only. • *Both* – Will send Storm Trap messages when a Traffic Storm has been both detected and cleared by the Switch. This function cannot be implemented in the Hardware mode. (When Drop is chosen in the Action field.
Traffic Control Settings	
From…To	Select the ports of this Switch to configure for Storm Control.
Broadcast	Enables or disable Broadcast Storm Control.
Multicast	Enables or disables Multicast Storm Control.
DLF	Enables or disables Destination Lookup Failure (DLF) storm control. (Not available for Software based Traffic Control {Shutdown}).
Action	Select the method of traffic Control from the pull down menu. The choices are: *Drop* – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved. *Shutdown* – Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the Countdown timer has expired and yet the Packet Storm continues, the port will be placed in Shutdown Forever mode and is no longer operational until the user manually resets the port using the Storm Control Recover setting at the top of this window. Choosing this option obligates the user to configure the Interval setting as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring.
Threshold	Specifies the maximum number of packets per second that will trigger the Traffic Control function to commence. The configurable threshold range is from 0-255000 with a default setting of 131072.
Count Down	The Count Down timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. This parameter is only useful for ports configured as Shutdown in their Action field and therefore will not operate for Hardware based Traffic Control implementations. The possible time settings for this field are 0, 5-30 minutes. 0 is the default setting for this field and 0 will denote that the port will never shutdown.
Interval	The Interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value. The Interval may be set between 5 and 30 seconds with the default setting of 5 seconds.

Click **Apply** to implement the settings of each field.

NOTE: Traffic Control cannot be implemented on ports that are set for Link Aggregation (Port Trunking).

NOTE: Ports that are in the Shutdown (Forever) mode will be seen as Discarding in Spanning Tree windows and implementations though these ports will still be forwarding BPDUs to the Switch's CPU.

NOTE: Ports that are in Shutdown (Forever) mode will be seen as link down in all windows and screens until the user recovers these ports.

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. To view the following window, click **Security > Port Security**.

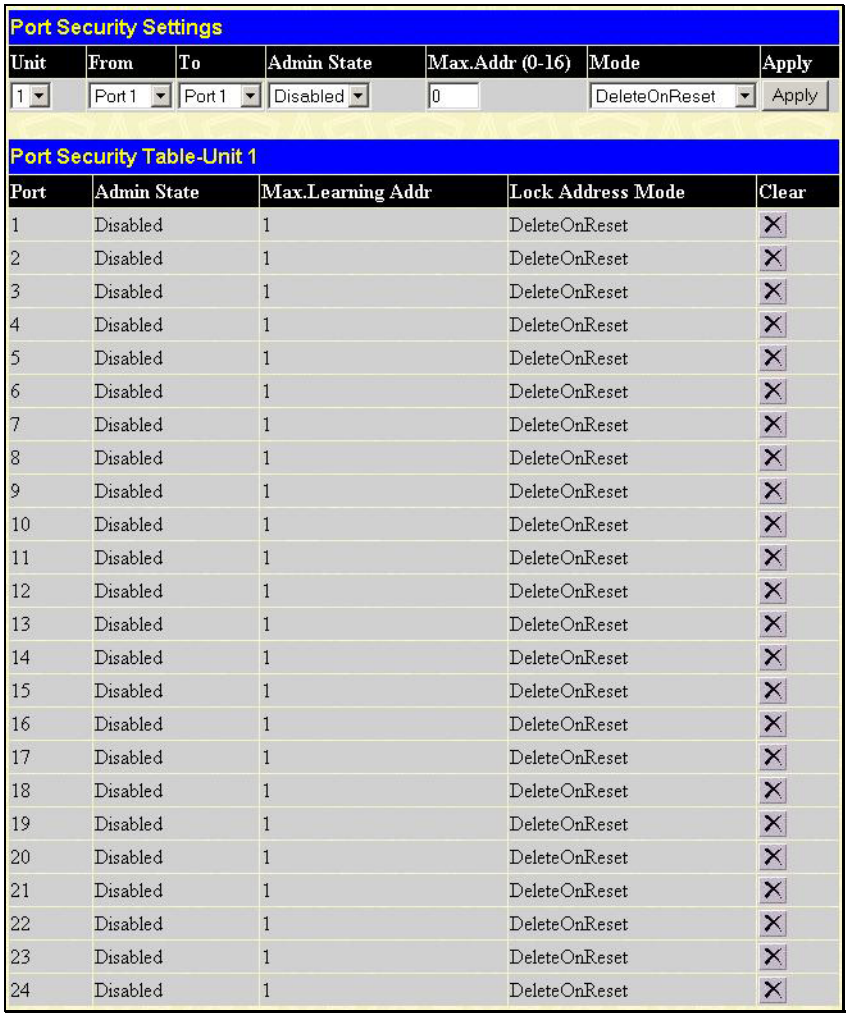


Figure 9- 2. Port Security Settings and Table

The following parameters can be set:

Parameter	Description
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.
From/To	A consecutive group of ports may be configured starting with the selected port.
Admin State	This pull-down menu allows the user to enable or disable Port Security (locked MAC address table for the selected ports).
Max. Learning Addr. (0-16)	The number of MAC addresses that will be in the MAC address forwarding table for the selected switch and group of ports.
Mode	This pull-down menu allows the option of 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 only age out after the Switch has been reset. *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 or rebooted.
Clear	Click the ✕ to clear MAC address entries which were learned by the Switch by a specified port. This only relates to the port security function. This command will only take effect if the Mode is set as *Permanent* or *DeleteonReset*.

Click **Apply** to implement changes made.

Port Security Entries

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

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 statically 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.

Figure 9- 3. Port Lock Entries Table

This window displays the following information:

Parameter	Description
VID	The VLAN ID of the entry in the forwarding database table that has been permanently learned by the Switch.
VLAN Name	The VLAN Name of the entry in the forwarding database table that has been permanently learned by the Switch.
MAC Address	The MAC address of the entry in the forwarding database table that has been permanently learned by the Switch.
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 Permanent or Delete on Reset can be deleted.
Delete	Click the ☒ in this field to delete the corresponding MAC address that was permanently learned by the Switch.

802.1X

Guest VLANs

On 802.1X security enabled networks, there is a need for non 802.1X supported devices to gain limited access to the network, due to the lack of the proper 802.1X software or incompatible devices, such as computers running Windows 98 or lower operating systems, or the need for guests to gain access to the network without full authorization or local authentication on the Switch. To supplement these circumstances, this switch now implements Guest 802.1X VLANs. These VLANs should have limited access rights and features separate from other VLANs on the network.

To implement Guest 802.1X VLANs, the user must first create a VLAN on the network with limited rights and then enable it as an 802.1X guest VLAN. Then the administrator must configure the guest accounts accessing the Switch to be placed in a Guest VLAN when trying to access the Switch. Upon initial entry to the Switch, the client wishing services on the Switch will need to be authenticated by a remote RADIUS Server or local authentication on the Switch to be placed in a fully operational VLAN. If authenticated and the authenticator posseses the VLAN placement information, that client will be accepted into the fully operational target VLAN and normal switch functions will be open to the client. If the authenticator does not have target VLAN placement information, the client will be returned to its originating VLAN. Yet, if the client is denied authentication by the authenticator, it will be placed in the Guest VLAN where it has limited rights and access. The adjacent figure should give the user a better understanding of the Guest VLAN process.

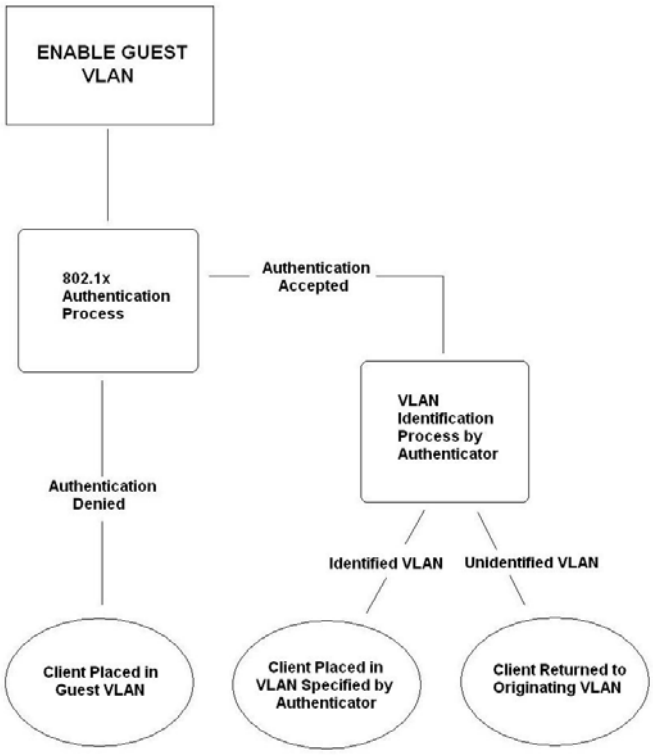


Figure 9- 4. Guest VLAN Authentication Process

Limitations Using the Guest VLAN

1. Ports supporting Guest VLANs cannot be GVRP enabled and vice versa.
2. A port cannot be a member of a Guest VLAN and a static VLAN simultaneously.
3. Once a client has been accepted into the target VLAN, it can no longer access the Guest VLAN.
4. If a port is a member of multiple VLANs, it cannot become a member of the Guest VLAN.

Guest VLAN

In the **Security** menu, open the **802.1X** folder and click **Configure 802.1X Guest VLAN**, which will display the following window for the user to configure. Remember, to set a Guest 802.1X VLAN, the user must first configure a normal VLAN which can be enabled here for Guest VLAN status.

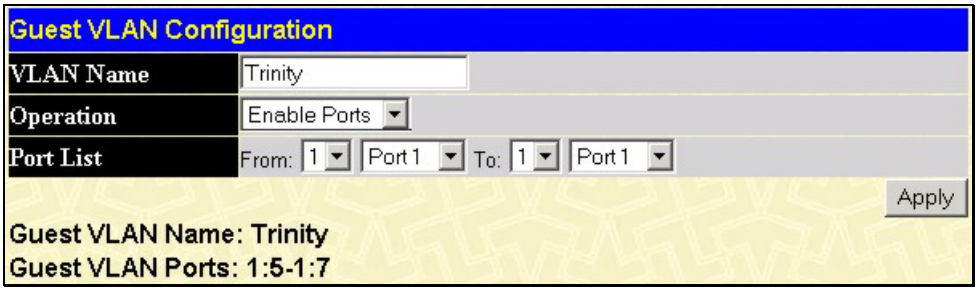


Figure 9- 5. Guest VLAN Configuration window

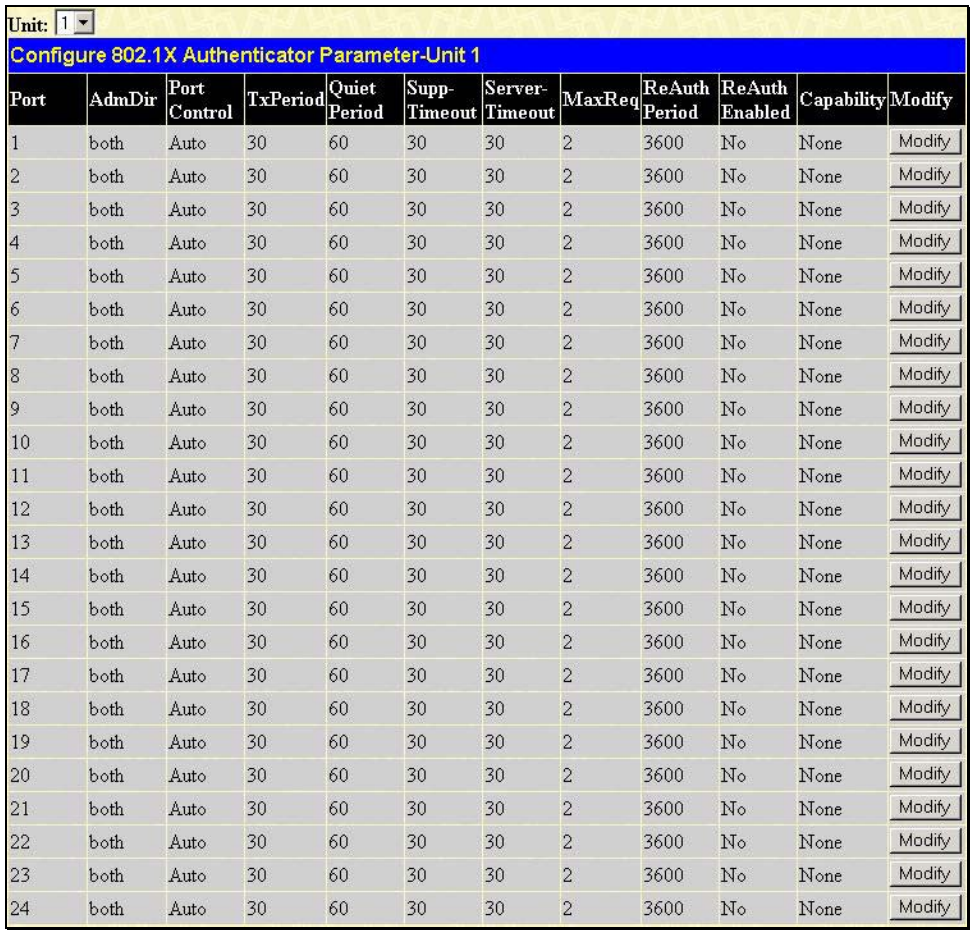
The following fields may be modified to enable the guest 802.1X VLAN:

Parameter	Description
VLAN Name	Enter the pre-configured VLAN name to create as a Guest 802.1X VLAN.
Operation	The user has three choices in configuring the Guest 802.1X VLAN, which are: *Enable Ports* – Selecting this option will enable ports listed in the Port List below, as part of the Guest VLAN. Be sure that these ports are configured for this VLAN or users will be prompted with an error message. *Disable Ports* - Selecting this option will disable ports listed in the Port List below, as part of the Guest VLAN. Be sure that these ports are configured for this VLAN or users will be prompted with an error message. *Delete* – Selecting this option will delete the VLAN entered in the VLAN Name window above.
Port List	Set the port list of ports of switches in the switch stack to be enabled for the Guest 802.1X VLAN using the pull down menus.

Click **Apply** to implement the guest 802.1X VLAN settings entered. Only one VLAN may be assigned as the 802.1X Guest VLAN.

Configure 802.1X Authenticator

To configure the 802.1X authenticator settings, click **Security > 802.1X** > **Configure 802.1X Authenticator Parameter**. The user may toggle between switches in the switch stack by using the **Unit** pull-down menu.



Unit: 1

Configure 802.1X Authenticator Parameter-Unit 1

Port	AdmDir	Port Control	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled	Capability	Modify
1	both	Auto	30	60	30	30	2	3600	No	None	Modify
2	both	Auto	30	60	30	30	2	3600	No	None	Modify
3	both	Auto	30	60	30	30	2	3600	No	None	Modify
4	both	Auto	30	60	30	30	2	3600	No	None	Modify
5	both	Auto	30	60	30	30	2	3600	No	None	Modify
6	both	Auto	30	60	30	30	2	3600	No	None	Modify
7	both	Auto	30	60	30	30	2	3600	No	None	Modify
8	both	Auto	30	60	30	30	2	3600	No	None	Modify
9	both	Auto	30	60	30	30	2	3600	No	None	Modify
10	both	Auto	30	60	30	30	2	3600	No	None	Modify
11	both	Auto	30	60	30	30	2	3600	No	None	Modify
12	both	Auto	30	60	30	30	2	3600	No	None	Modify
13	both	Auto	30	60	30	30	2	3600	No	None	Modify
14	both	Auto	30	60	30	30	2	3600	No	None	Modify
15	both	Auto	30	60	30	30	2	3600	No	None	Modify
16	both	Auto	30	60	30	30	2	3600	No	None	Modify
17	both	Auto	30	60	30	30	2	3600	No	None	Modify
18	both	Auto	30	60	30	30	2	3600	No	None	Modify
19	both	Auto	30	60	30	30	2	3600	No	None	Modify
20	both	Auto	30	60	30	30	2	3600	No	None	Modify
21	both	Auto	30	60	30	30	2	3600	No	None	Modify
22	both	Auto	30	60	30	30	2	3600	No	None	Modify
23	both	Auto	30	60	30	30	2	3600	No	None	Modify
24	both	Auto	30	60	30	30	2	3600	No	None	Modify

Figure 9- 6. Configure 802.1X Authenticator Parameter window

To configure the settings by port, click on its corresponding **Modify** button, which will display the following table to configure:

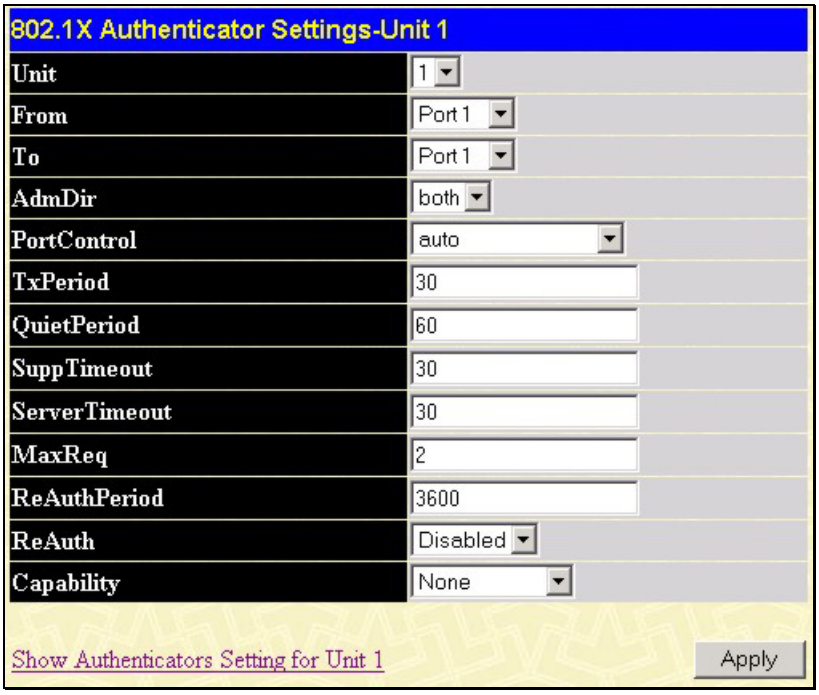


Figure 9- 7. 802.1X Authenticator Settings of Unit 1 – Modify

This screen allows setting of the following features:

Parameter	Description
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.
From [ ] To [ ]	Enter the port or ports to be set.
AdmCtrlDir	Sets the administrative-controlled direction to either *in* or *both*. If *in* is selected, control is only exerted over incoming traffic through the port 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	This allows the user 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	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	This allows the user 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	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is 30 seconds.
ServerTimeout	This value determines timeout conditions in the exchanges between the Authenticator and the

	authentication server. The default setting is 30 seconds.
MaxReq	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	A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is 3600 seconds.
ReAuth	Determines whether regular reauthentication will take place on this port. The default setting is *Disabled*.
Capability	This allows the 802.1X Authenticator settings to be applied on a per-port basis. Select *Authenticator* to apply the settings to the port. When the setting is activated, a user must pass the authentication process to gain access to the network. Select *None* disable 802.1X functions on the port.

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.

Configure 802.1x Guest VLAN

In the **Security** menu, open the **802.1x** folder and click **Configure 802.1x Guest VLAN**, which will display the following window for the user to configure. Remember, to set a Guest 802.1x VLAN, the user must first configure a normal VLAN which can be enabled here for Guest VLAN status.

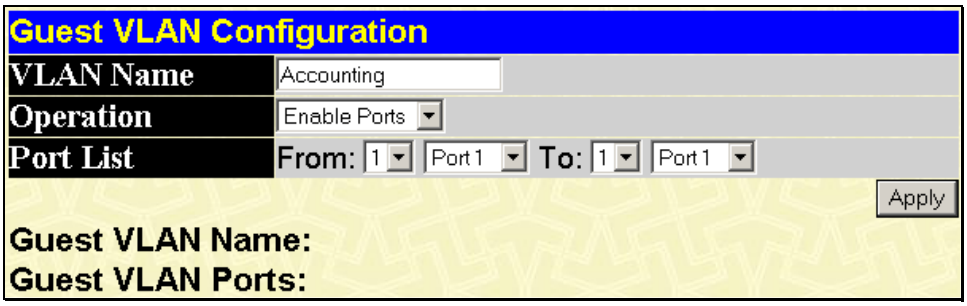


Figure 9- 8 Configure 802.1x Guest VLAN window

The following fields may be modified to enable the guest 802.1x VLAN:

Parameter	Description
VLAN Name	Enter the pre-configured VLAN name to create as a Guest 802.1x VLAN.
Operation	The user has two choices in configuring the Guest 802.1X VLAN, which are: *Enabled* – Selecting this option will enable ports listed in the Port List below, as part of the Guest VLAN. Be sure that these ports are configured for this VLAN or users will be prompted with an error message. *Disabled* - Selecting this option will disable ports listed in the Port List below, as part of the Guest VLAN. Be sure that these ports are configured for this VLAN or users will be prompted with an error message.
Port List	Set the port list of ports to be enabled for the Guest 802.1x VLAN using the pull-down menus.

Click **Apply** to implement the guest 802.1x VLAN settings entered. Only one VLAN may be assigned as the 802.1X Guest VLAN.

Authentic RADIUS Server

The RADIUS feature of the Switch allows the user to facilitate centralized user administration as well as providing protection against a sniffing, active hacker. The Web Manager offers three windows.

Click **Security > 802.1X > Authentic RADIUS Server** to open the **Authentic RADIUS Server Setting** window shown below:

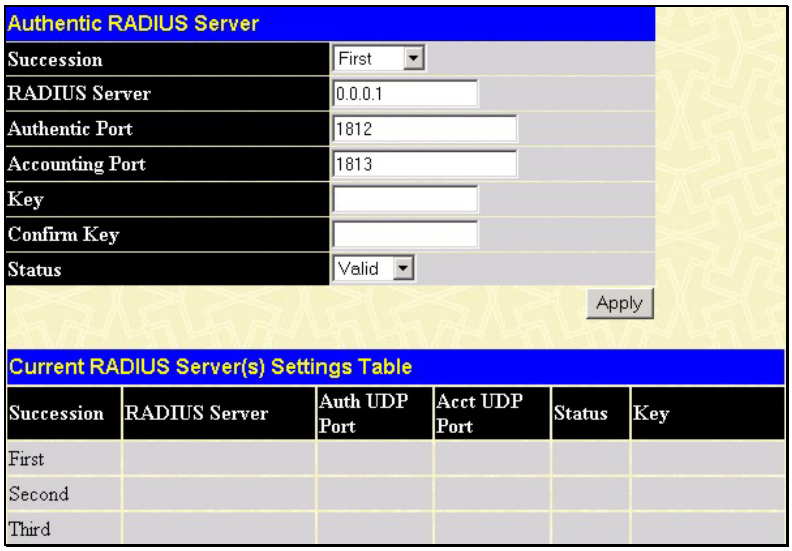


Figure 9- 9. Authentic RADIUS Server and Current RADIUS Server Settings Table window

This window displays the following information:

Parameter	Description
Succession	Choose the desired RADIUS server to configure: *First, Second* or *Third*.
RADIUS Server	Set the RADIUS server IP.
Authentic Port	Set the RADIUS authentic server(s) UDP port. The default port is 1812.
Accounting Port	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 the user to set the RADIUS Server as *Valid* (Enabled) or *Invalid* (Disabled).

Trust Host

Up to four trusted-host secure IP addresses may be configured and used for remote Switch management. It should be noted that if one or more trusted hosts are enabled, the Switch will immediately accept remote instructions from only the specified IP address or addresses. If you enable this feature, be sure to first enter the IP address of the station you are currently using.

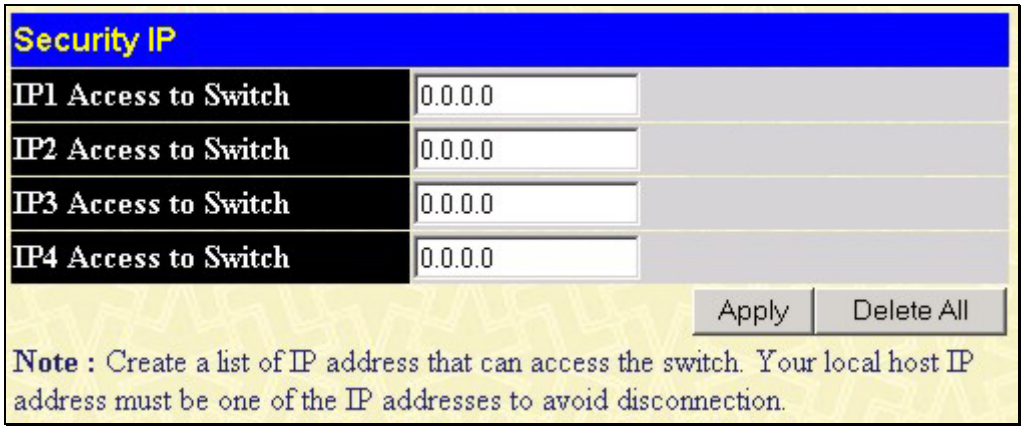


Figure 9- 10. Security IP menu for Trusted Host configuration

To configure secure IP addresses for trusted host management of the Switch, type the IP address of the station you are currently using in the first field as well as up to three additional IP addresses of trusted hosts. Click the **Apply** button to assign trusted host status to the IP addresses. This goes into effect immediately. Click **Delete All** to remove all configured trusted hosts from this switch.

Access Authentication Control

The TACACS / XTACACS / TACACS+ / RADIUS commands allow users to 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.)

Authentication Policy & Parameters

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

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

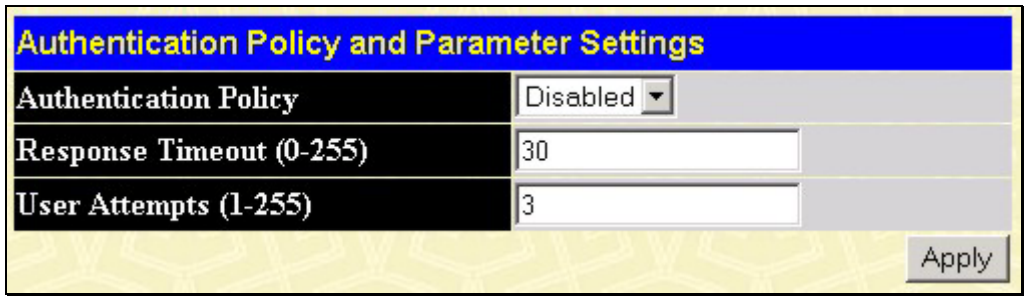


Figure 9- 11. Authentication Policy and Parameter Settings window

The following parameters can be set:

Parameter	Description
Authentication Policy	Use the pull down menu to enable or disable the Authentication Policy on the Switch.
Response Timeout (1-255)	This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between 1 and 255 seconds. The default setting is 30 seconds.
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's 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 > Access Authentication Control > Application Authentication Settings:**

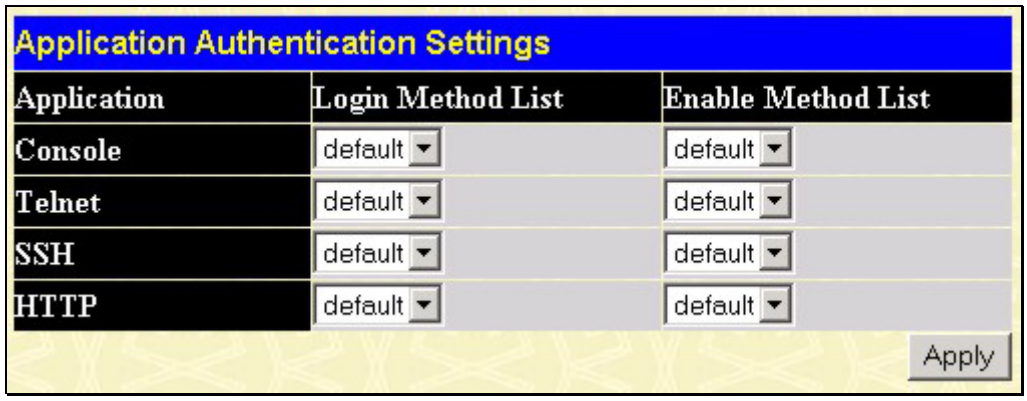


Figure 9- 12. Application's Authentication Settings window

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 three built-in Authentication Server Groups that cannot be removed but can be modified. Up to eight authentication server hosts may be added to any particular group.

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

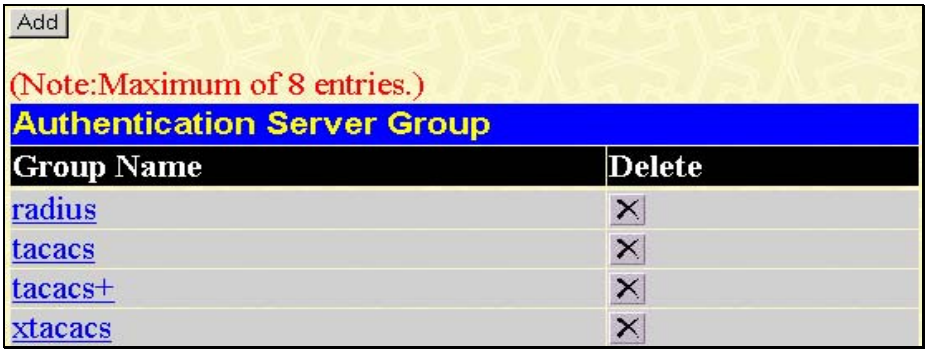


Figure 9- 13. Authentication Server Group window

This screen 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.

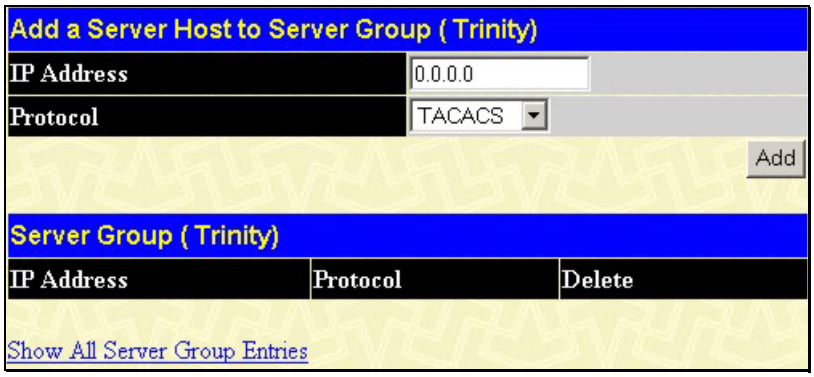


Figure 9- 14. Add a Server Host to Server Group (XTACACS) window.

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 add this Authentication Server Host to the group.

To add a server group other than the ones listed, click the add button, revealing the following window to configure.

Figure 9- 15. 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: The 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 > Access Authentication Control > Authentication Server Host**:

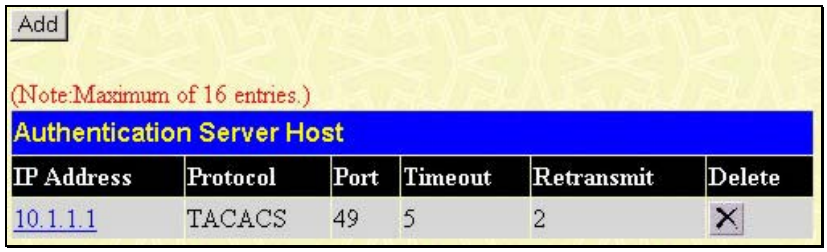


Figure 9- 16. Authentication Server Host window

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

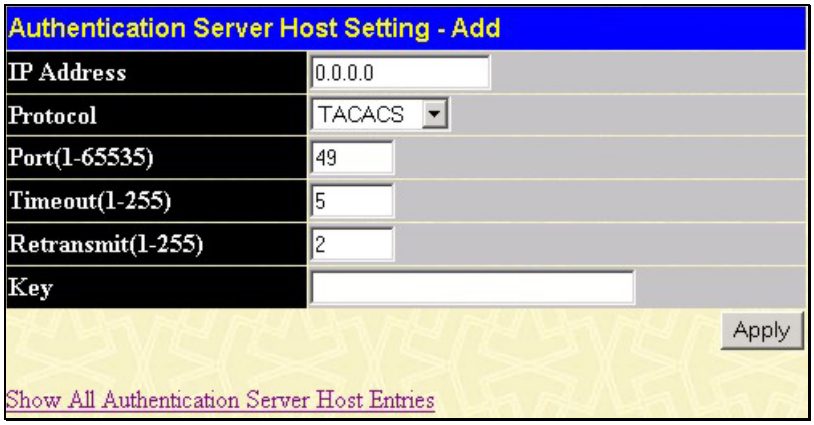


Figure 9- 17. Authentication Server Host Setting - Add window

Configure the following parameters to add an Authentication Server Host:

Parameter	Description
IP Address	The IP address of the remote server host 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 screen click **Security Management > Access Authentication Control > Login Method Lists**:

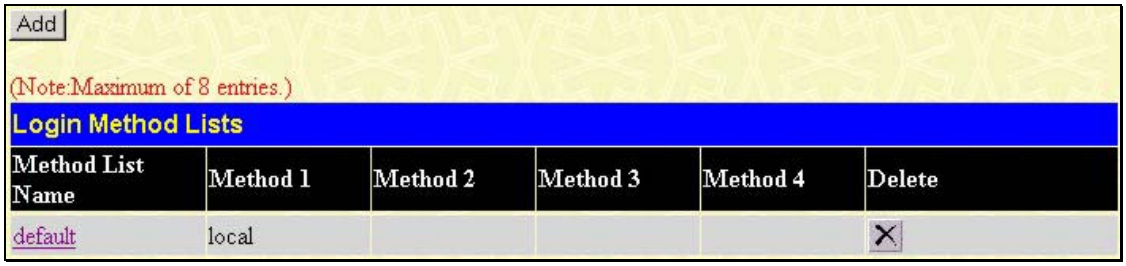


Figure 9- 18. Login Method List Settings window

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

Both actions will result in the same screen to configure:

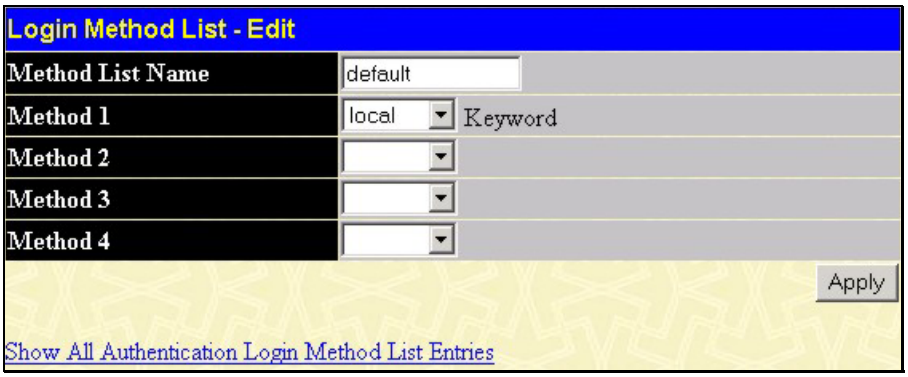


Figure 9- 19. Login Method List - Edit window (default)

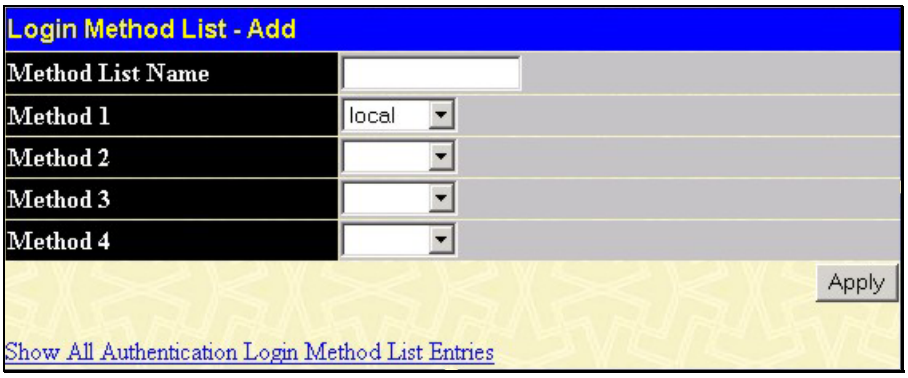


Figure 9- 20. Login Method List – Add window

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 (4) 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 Lists*** 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 (8) Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

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

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

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

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

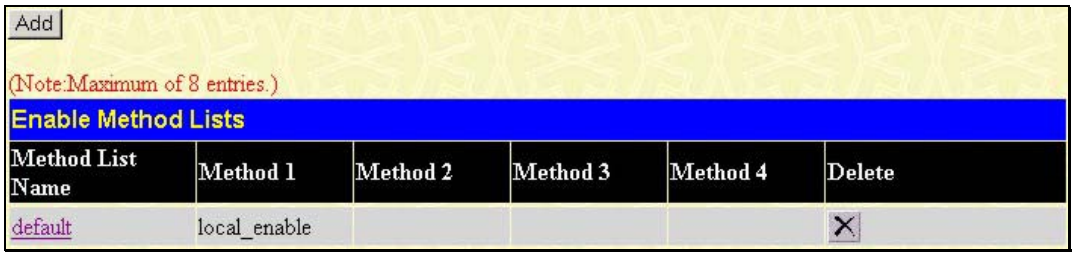


Figure 9- 21. Enable Method List Settings window

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

Both actions will result in the same screen to configure:

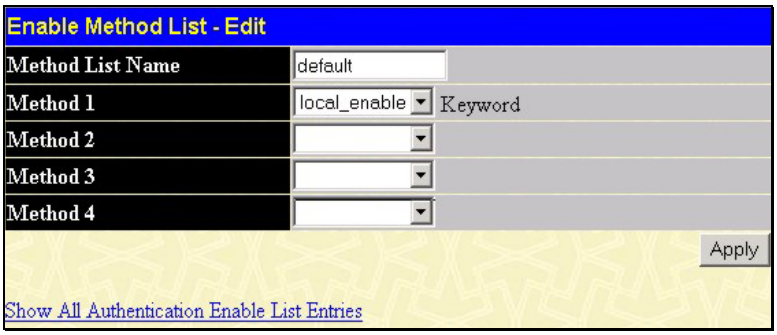


Figure 9- 22. Enable Method List - Edit window

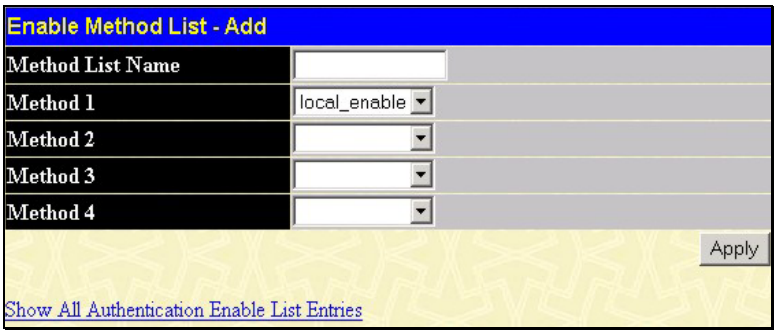


Figure 9- 23. Enable Method List - Add window

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 (4) 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.

Configure 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 > Access Authentication Control > Local Enable Password**:

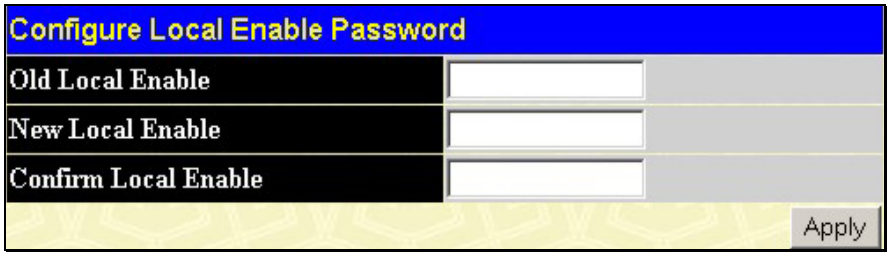


Figure 9- 24. Configure Local Enable Password window

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

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

Click **Apply** to implement changes made.

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 > Access Authentication Control > Enable Admin**:

Figure 8- 35. Enable Admin Screen

When this screen appears, click the **Enable Admin** button revealing a window 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.

Traffic Segmentation

Traffic segmentation is used to limit traffic flow from a single port to a group of ports. 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.

Open the **Security** folder and click **Traffic Segmentation**, to view the screen shown below.

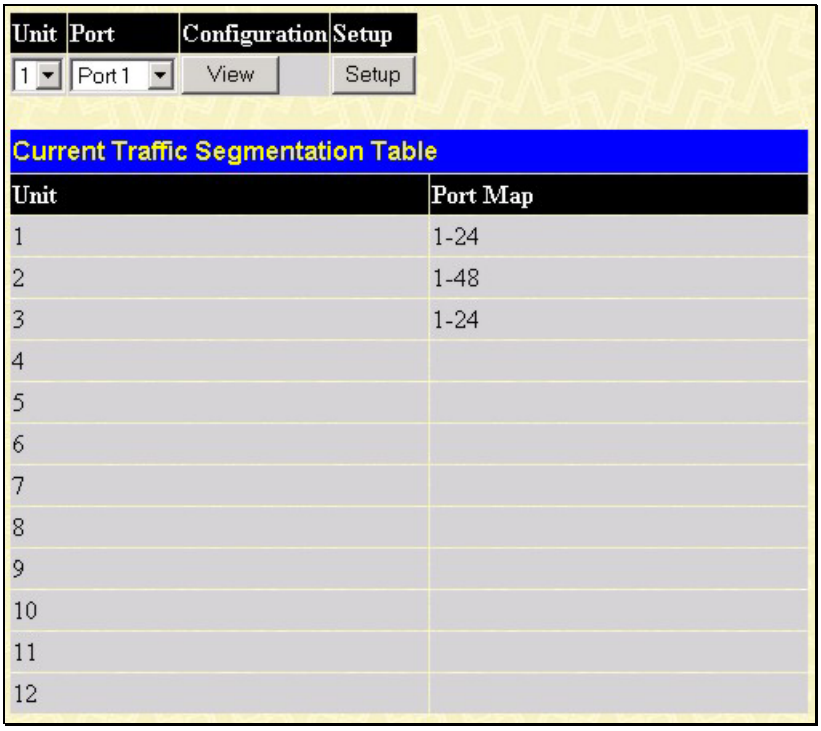


Figure 9- 25. Current Traffic Segmentation Table

Click on the **Setup** button to open the **Setup Forwarding ports** menu, as shown below.

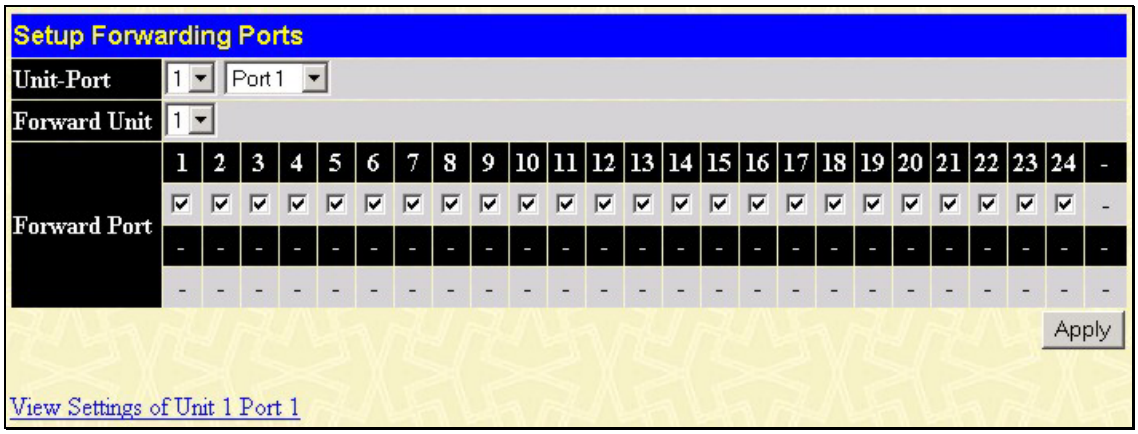


Figure 9- 26. Setup Forwarding Ports

Configuring traffic segmentation on the xStack DGS-3400 switch series is accomplished in two parts. First, select a switch in the switch stack by using the **Unit** pull-down menu, and then specify a port from the switch, using the **Port** pull-down menu. Next, specify which ports on the switch that are able to receive packets from the switch and port 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.

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.

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. 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. Currently, all xStack DGS-3400 Series switch come with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

To view the following window, click **Security > SSL** at the top of the window:

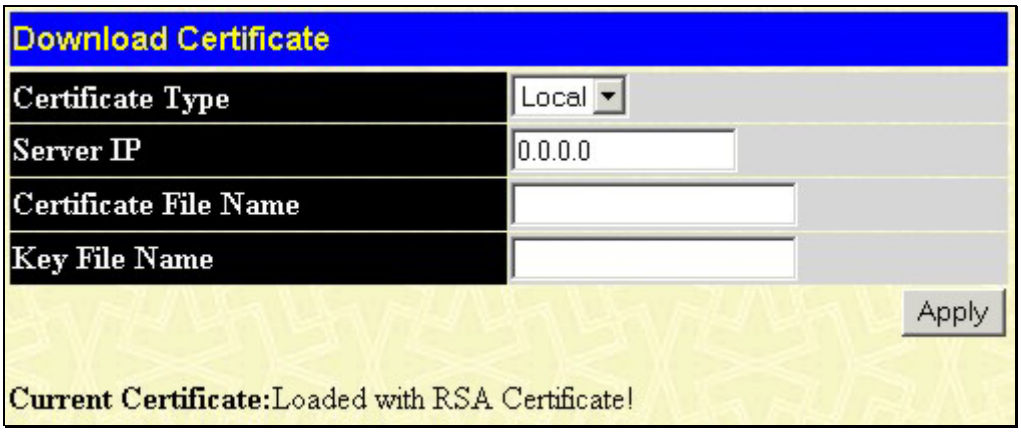


Figure 9- 27. Download Certificate menu

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

Parameter	Description
Certificate Type	Select Local to specify certificate type.
Server IP	Enter the IPv4 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)

Click **Apply** to implement changes made.

SSL Configuration

This screen 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://xx.xx.xx.xx) 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 > SSL**:

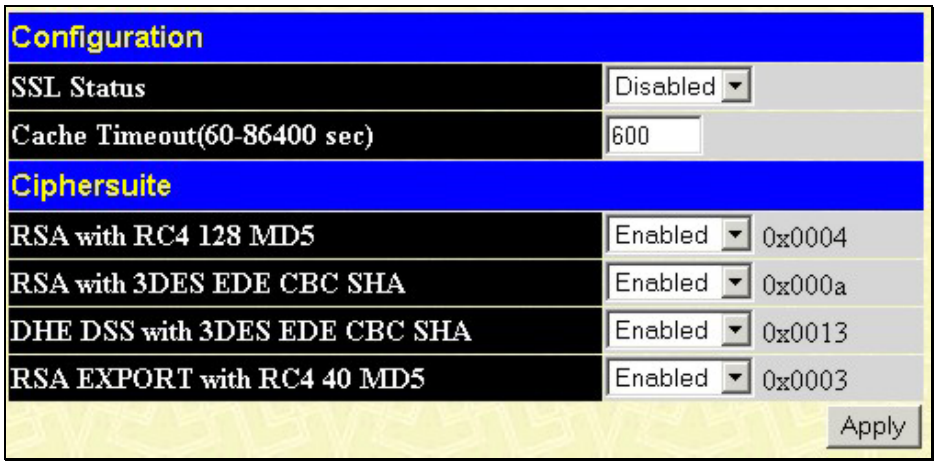


Figure 9- 28. SSL Configuration and Ciphersuite menu

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 (60-86400)	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.
SSL 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.

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

Secure Shell (SSH)

SSH is 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 **SSH User Authentication** window. There are three choices as to the method SSH will use to authorize the user, which are **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 **SSH Configuration** 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 > SSH > SSH Configuration**:

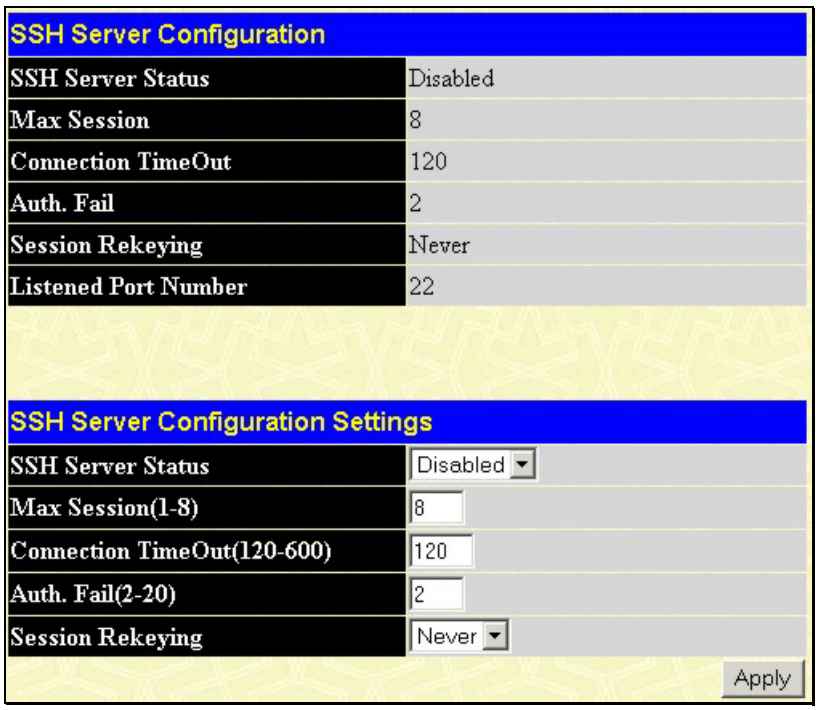


Figure 9- 29. Current SSH Configuration and SSH Server Configuration Settings menu

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 (1-8)	Enter a value between 1 and 8 to set the number of users that may simultaneously access the Switch. The default setting is 8.

Connection TimeOut (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 120 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*.
Port	Enter the virtual port number to be used with this feature. The common port number for SSH is 22.

SSH Authentication Mode

The SSH Authentication 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 > SSH > SSH Authentication Mode and Algorithm Settings:**

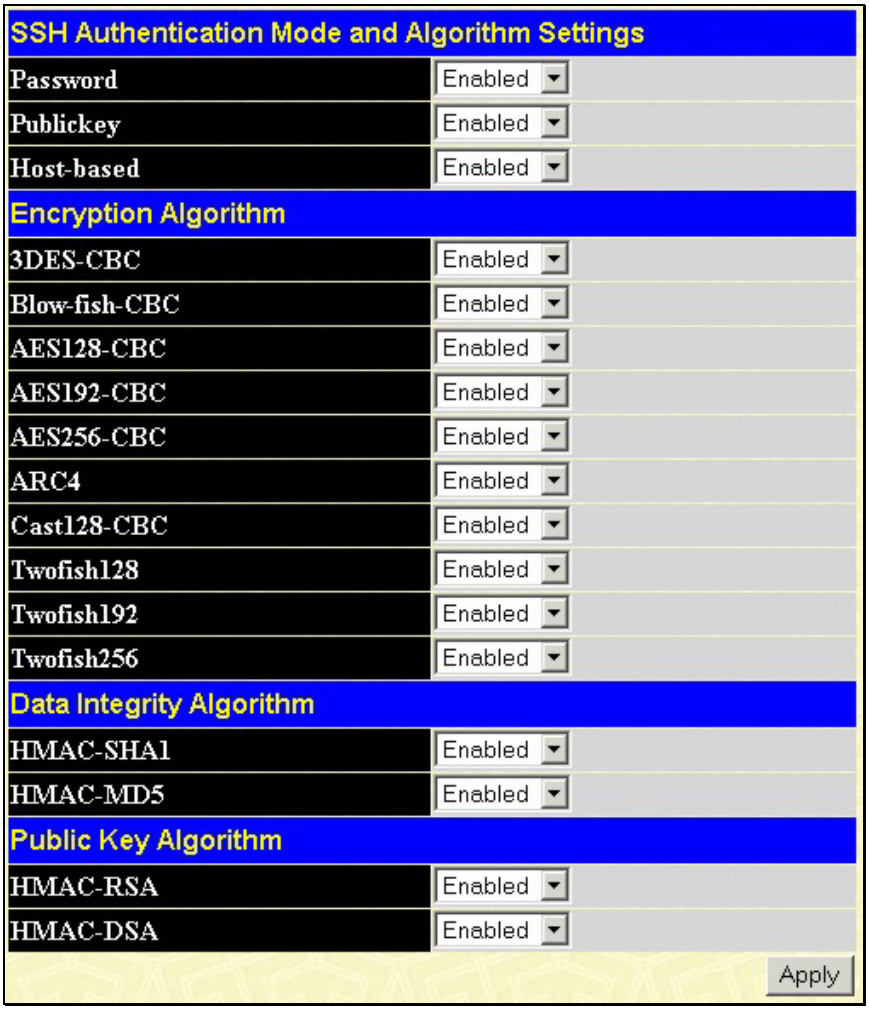


Figure 9- 30. SSH Algorithms window

The following algorithms may be set:

Parameter	Description
Authentication Algorithm	
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 (DSA) encryption. The default is *Enabled*.

Click **Apply** to implement changes made.

SSH User Authentication Mode

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

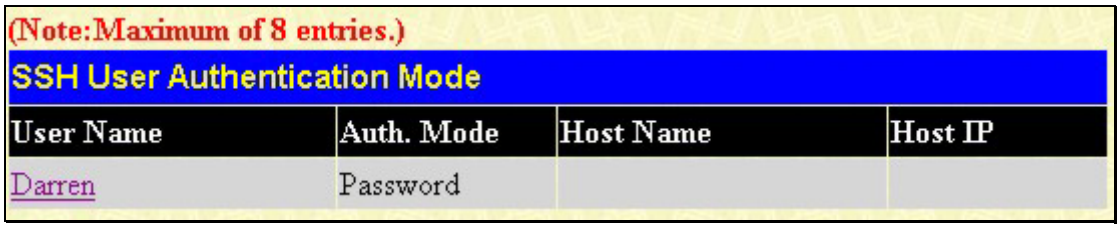
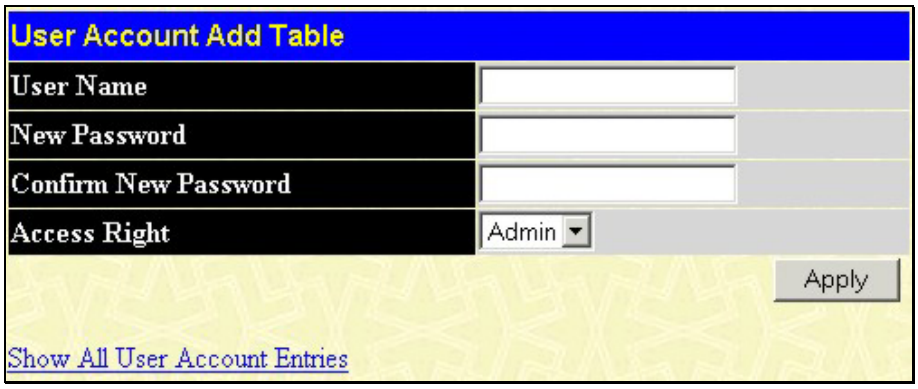


Figure 9- 31. Current Accounts window

In the example screen above, the User Account "Darren" has been previously set using the User Accounts window in the **Security** 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.



NOTE: To set the **SSH User Authentication** parameters on the Switch, a User Account must be previously configured.

Figure 9- 32. SSH User menu

Once a User Account has been configured, return to the SSH User Authentication window, which now displays the newly created account, as shown here.

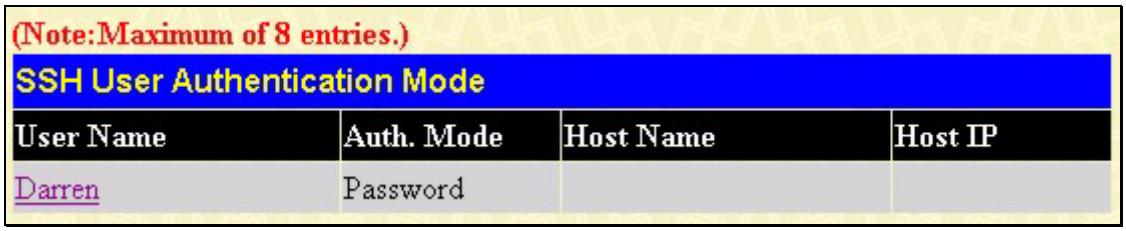


Figure 9- 33. SSH User Authentication Mode window

To configure the SSH settings for this user, click its hyperlinked User Name which will display the following window to configure:

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.

JWAC (Japanese Web-based Access Control)

The **JWAC** folder contains four windows: **JWAC Global Configuration**, **JWAC Port Settings**, **JWAC User Account** and **JWAC Host Information**.

JWAC Global Configuration

Use this window to enable and configure Japanese Web-based Access Control on the Switch. Please note that JWAC and Web Authentication are mutually exclusive functions. That is, they cannot be enabled at the same time. To use the JWAC feature, computer users need to pass through two stages of authentication. The first stage is to do the authentication with the quarantine server and the second stage is the authentication with the Switch. For the second stage, the authentication is similar to Web Authentication, except that there is no port VLAN membership change by JWAC after a host passes authentication. The RADIUS server will share the server configuration defined by the 802.1X command set.

To configure JWAC global settings for the Switch, go to the **Security** folder, open **JWAC**, and click **JWAC Global Configuration**, which will open the following window:

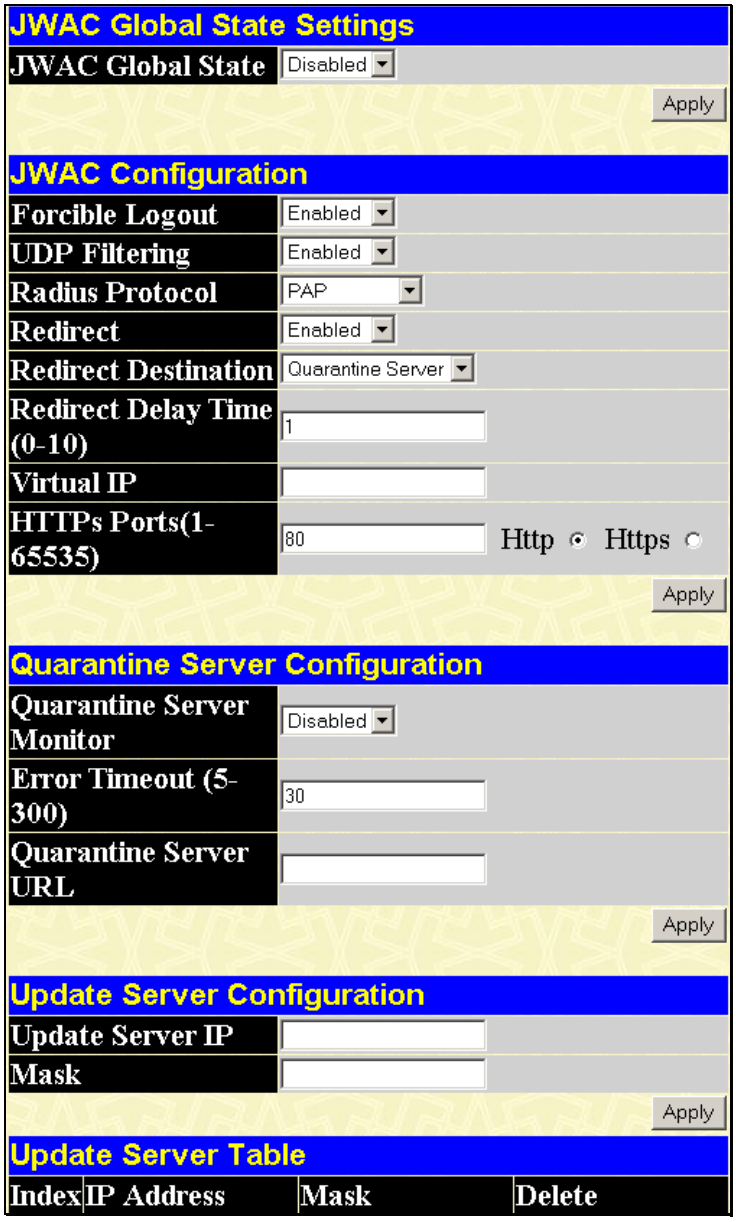


Figure 9- 34. JWAC Global Settings window

To set the Web Authentication for the Switch, complete the following fields:

Parameter	Description
JWAC Global State Settings	
JWAC Global State	Use this drop-down menu to either enable or disable JWAC on the Switch.
JWAC Configuration	
Forcible Logout	This parameter enables or disables JWAC Forcible Logout. When Forcible Logout is *Enabled*, a Ping packet from an authenticated host to the JWAC Switch with TTL=1 will be regarded as a logout request, and the host will move back to the unauthenticated state.
UDP Filtering	This parameter enables or disables JWAC UDP Filtering. When UDP Filtering is *Enabled*, all UDP and ICMP packets except DHCP and DNS packets from unauthenticated hosts will be dropped
RADIUS Protocol	This parameter specifies the RADIUS protocol used by JWAC to complete a RADIUS authentication. The options include *Local*, *EAP MD5*, *PAP*, *CHAP*, *MS CHAP*, and *MS CHAPv2*.
Redirect	This parameter enables or disables JWAC Redirect. When the redirect quarantine server is enabled, the unauthenticated host will be redirected to the quarantine server when it tries to access a random URL. When the redirect JWAC login page is enabled, the unauthenticated host will be redirected to the JWAC login page in the Switch to finish authentication. When redirect is disabled, only access to the quarantine server and the JWAC login page from the unauthenticated host are allowed, all other web access will be denied. NOTE: When enabling redirect to the quarantine server, a quarantine server must be configured first.
Redirect Destination	This parameter specifies the destination before an unauthenticated host is redirected to either the *Quarantine Server* or the *JWAC Login Page*.
Redirect Delay Time (0-10)	This parameter specifies the Delay Time before an unauthenticated host is redirected to the Quarantine Server or JWAC Login Page. Enter a value between *0* and *10* seconds. A value of *0* indicates no delay in the redirect.
Virtual IP	This parameter specifies the JWAC Virtual IP address that is used to accept authentication requests from an unauthenticated host. Only requests sent to this IP will get a correct response. NOTE: This IP does not respond to ARP requests or ICMP packets.
HTTPs Ports (1-65535)	This parameter specifies the TCP port that the JWAC Switch listens to and uses to finish the authentication process.
Quarantine Server Configuration	
Quarantine Server Monitor	This parameter enables or disables the JWAC Quarantine Server Monitor. When *Enabled*, the JWAC Switch will monitor the Quarantine Server to ensure the server is okay. If the Switch detects no Quarantine Server, it will redirect all unauthenticated HTTP access attempts to the JWAC Login Page forcibly if the Redirect is enabled and the Redirect Destination is configured to be a Quarantine Server.
Error Timeout (5-300)	This parameter is used to set the Quarantine Server Error Timeout. When the Quarantine Server Monitor is enabled, the JWAC Switch will periodically check if the Quarantine works okay. If the Switch does not receive any response from the Quarantine Server during the configured Error Timeout, the Switch then regards it as not working properly. Enter a value between *5* and *300* seconds.
Quarantine Server URL	This parameter specifies the JWAC Quarantine Server URL. If the Redirect is enabled and the Redirect Destination is the Quarantine Server, when an unauthenticated host sends the HTTP request packets to a random Web server, the Switch will handle this HTTP packet and send back a message to the host to allow it access to the Quarantine Server with the

	configured URL. When a computer is connected to the specified URL, the quarantine server will request the computer user to input the user name and password to complete the authentication process.
Update Server Configuration	
Update Server IP	This parameter specifies the Update Server IP address.
Mask	This parameter specifies the Server IP net mask.
Update Server Table	
Index	This parameter displays the Index of the Server.
IP Address	This parameter displays the Server IP Address.
Mask	This parameter displays the Server IP net mask.
Delete	This button allows you to delete an existing Server entry.

Click **Apply** to implement changes made.

JWAC Port Settings

To view JWAC port settings for the Switch, go to the **Security** folder, open **JWAC**, and click **JWAC Port Settings**, which will open the following window:

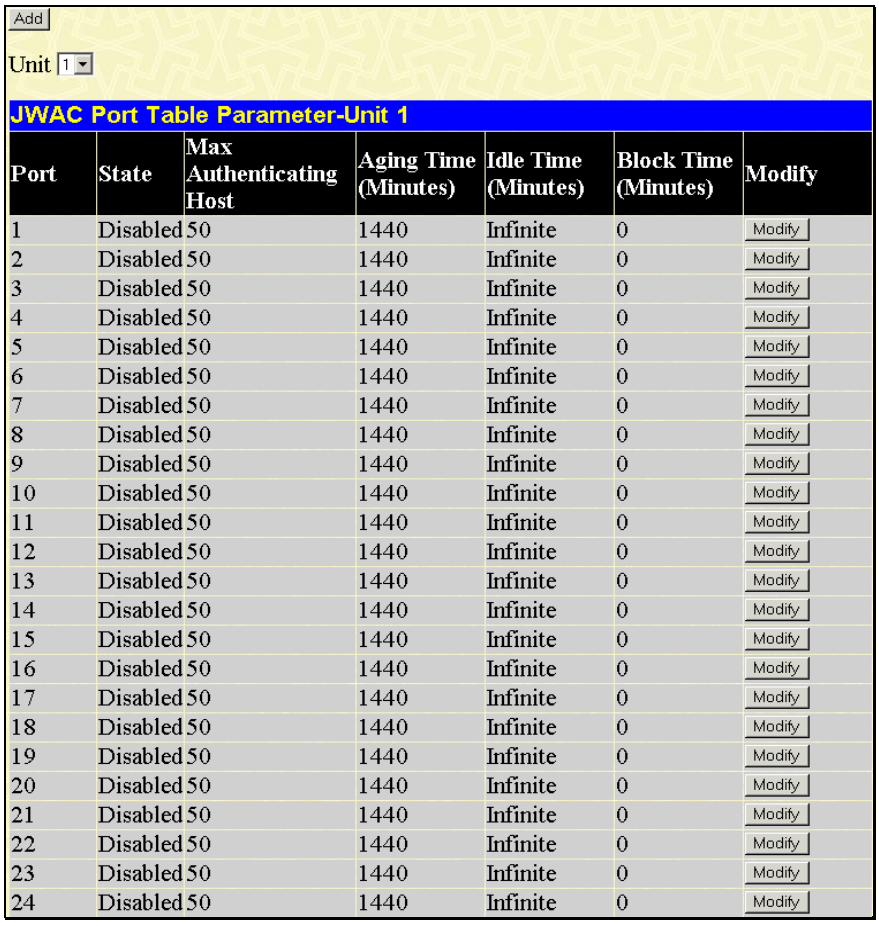


Figure 9- 35. JWAC Port Settings window

To configure JWAC port settings for the Switch, go to the **Security** folder, open **JWAC**, click **JWAC Port Settings**, and click the **Add** button, which will open the following window:

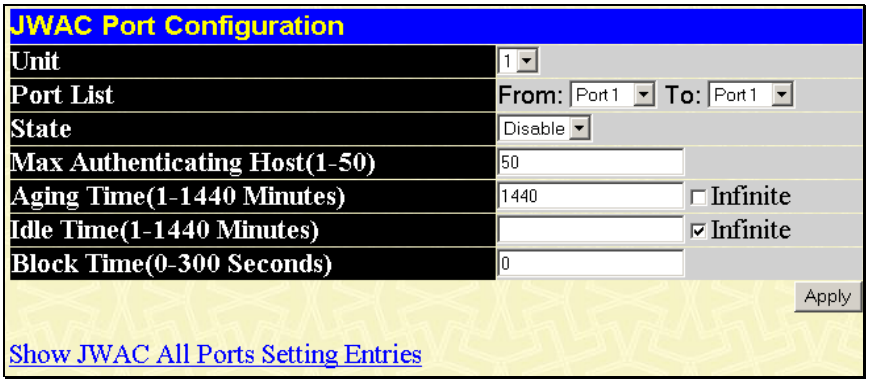


Figure 9- 36. JWAC Port Configuration window

To set the JWAC on individual ports for the Switch, complete the following fields:

Parameter	Description
Port List	Lists the range of Ports that will be configured in this window.
State	This parameter specifies the state of the configured ports.
MAX Authenticating Host	This parameter specifies the maximum number of host process authentication attempts allowed on each port at the same time.
Aging Time (1-1440 Minutes)	This parameter specifies the period of time a host will keep in authenticated state after it successes to authenticate. Enter a value between 0 and 1440 minutes. The default setting is *1440* minutes. To maintain a constant Port Configuration check the **Infinite** box in the JWAC configuration window.
Idle Time (1-1440 Minutes)	This parameter specifies the period of time during which there is no traffic for an authenticated host and the host will be moved back to the unauthenticated state. Enter a value between *1* and *1440* minutes. A value of **Infinite** indicates the Idle state of the authenticated host on the port will never be checked. The default setting is **Infinite**.
Block Time (0-300 Seconds)	This parameter specifies the period of time a host will keep in a blocked state after it fails to authenticate. Enter a value between *0* and *300* seconds. The default setting is *0* seconds.

Click **Apply** to implement changes made.

To view the JWAC Port Table click on the hyperlinked **Show JWAC All Ports Setting Entries**, which will open the following window:

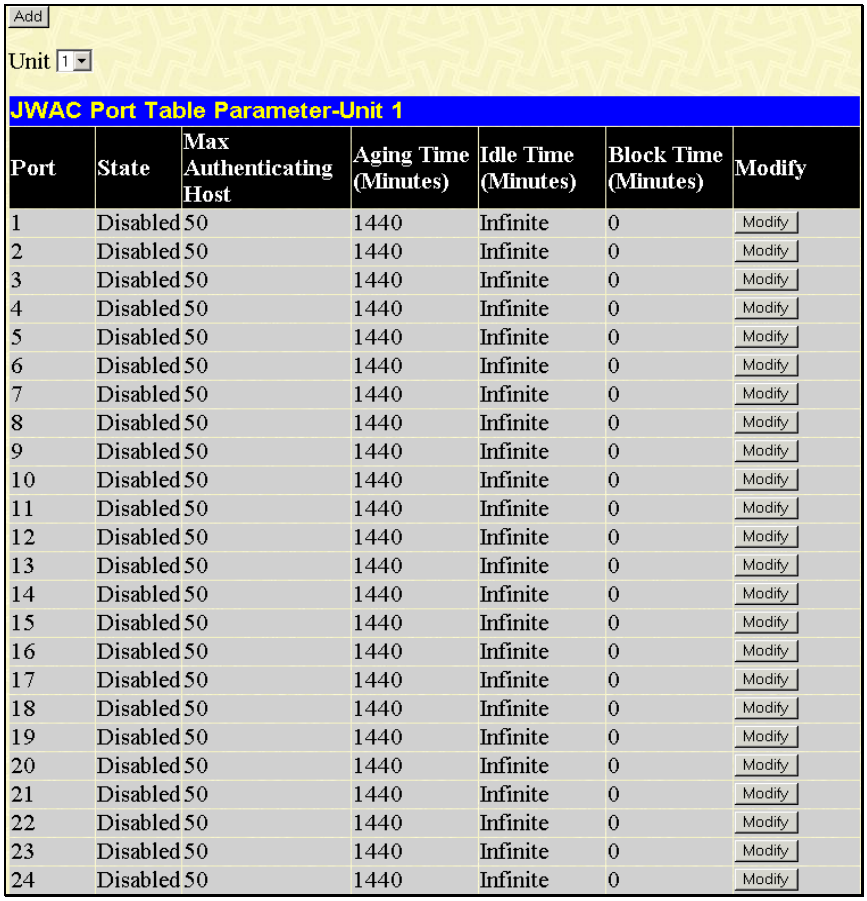


Figure 9- 37. JWAC Port Table window

To configure the settings by port, click on the **Modify** button in the corresponding column, which will bring you to the following window:

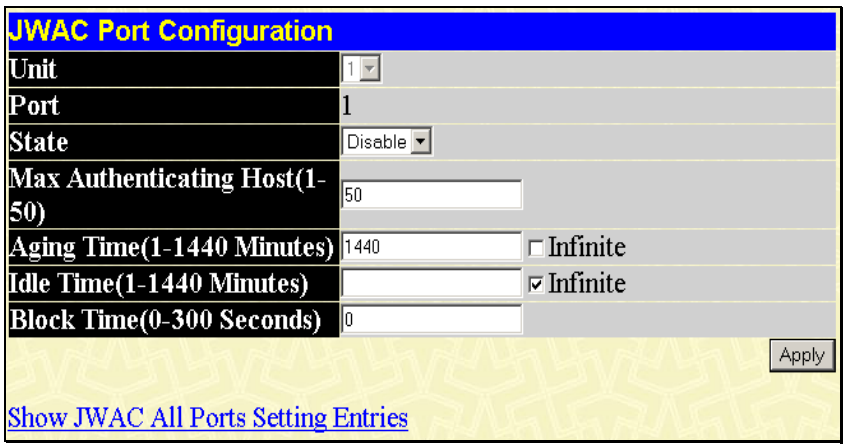


Figure 9- 38. JWAC Port Configuration window

JWAC User Account

To view JWAC user settings for the Switch, go to the **Security** folder, open **JWAC**, and click **JWAC User Account**, which will open the following window:

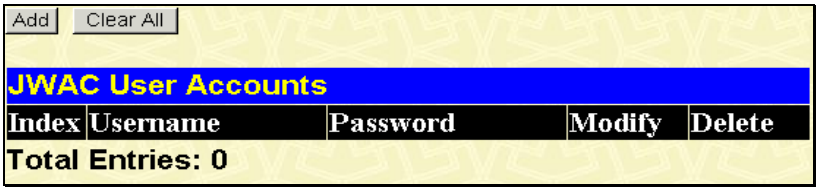


Figure 9- 39. JWAC User Account window

To configure JWAC user settings for the Switch, go to the **Security** folder, open **JWAC**, click **JWAC User Account**, and click the **Add** button, which will open the following window:

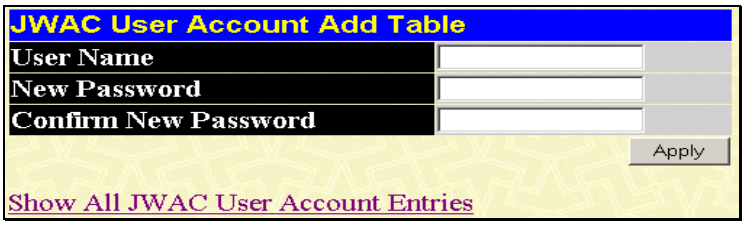


Figure 9- 4041. JWAC User Account Add Table window

To set the User Account settings for the JWAC by the Switch, complete the following fields and then click the **Add** button. To clear the current JWAC user settings in the table at the bottom of the window, click the **Delete All** button.

Parameter	Description
User Name	Enter a username of up to 15 alphanumeric characters.
New Password	Enter the password of the user. This field is case-sensitive and must be a complete alphanumeric string.
Confirm New Password	Retype the password entered in the previous field.

Click **Apply** to implement changes made.

To view JWAC user settings for the Switch, click on the Hyperlinked **Show All JWAC User Accounts**, which will open the following window:

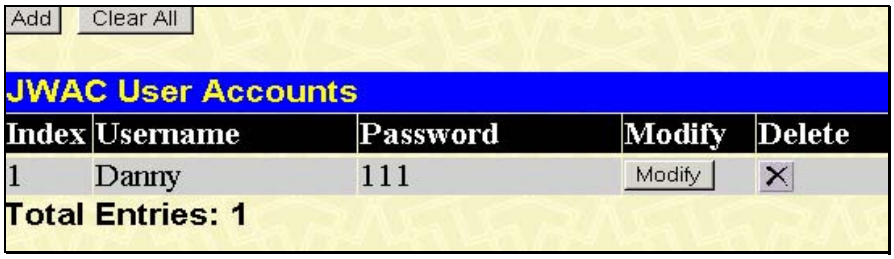


Figure 9- 41. JWAC User Account Table window

To add another JWAC user account for the Switch, click the **Add** button, to clear the existing entries click the **Clear All** button.

JWAC Host Information

The JWAC Host information Table allows the user to show or delete the hosts, which are handling or have been handled by the switch.

To access the JWAC Host Table Settings for the Switch, go to the **Security** folder, open **JWAC**, and click **JWAC Host Information**, which will open the following window:

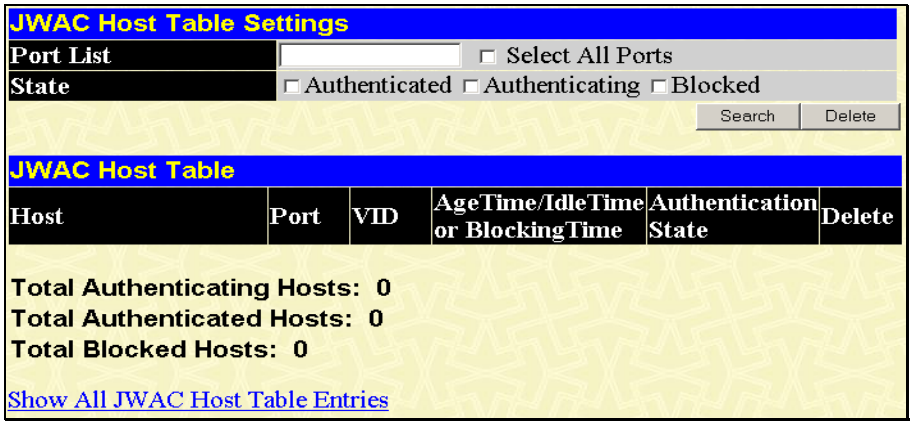


Figure 9- 42. JWAC Host Table Settings window

To search for hosts hanlded by the switch enter the Port list information and select the state, then click the **Search** button. This will give you a list on the JWAC Host Table and their states. To clear an entry click on the **Delete** button.

Section 10

Monitoring

Device Status
Module Information
CPU Utilization
Port Utilization
Packets
Errors
Packet Size
Browse Router Port
Browse MLD Router Port
VLAN Status
Port Access Control
MAC Address Table
IGMP Snooping Group
MLD Snooping Group
Switch Logs
Browse ARP Table
Session Table
IP Forwarding Table
Browse Routing Table

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

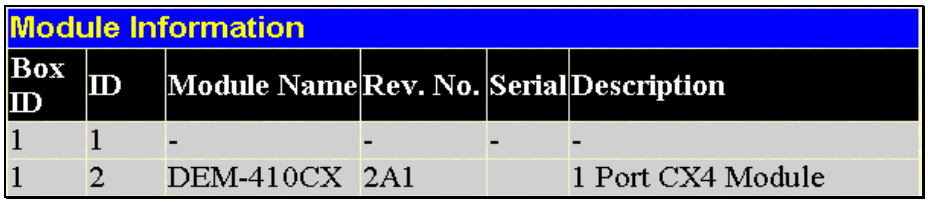
Figure 10- 1. Device Status window

The following fields may be viewed in this window:

Parameter	Description
Internal Power	Displays Active if the internal power supply is powering the system.
External Power (RPS)	Displays Active if the RPS is powering the system.
Side Fan	Indicates fan status.
Back Fan	Indicates fan status.

Module Information

The **Module Information** display in the **Monitoring** menu shows information about any installed modules.



Module Information

Box ID	ID	Module Name	Rev. No.	Serial	Description
1	1	-	-	-	-
1	2	DEM-410CX	2A1		1 Port CX4 Module

Figure 10- 2. Module Information

Module information displayed:

Parameter	Description
ID	The slot number where the module is installed.
Module Name	The full name of the module installed.
Rev. No.	The version of the installed module.
Serial	The serial number of the module.
Description	A brief description of the type of module.

CPU Utilization

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

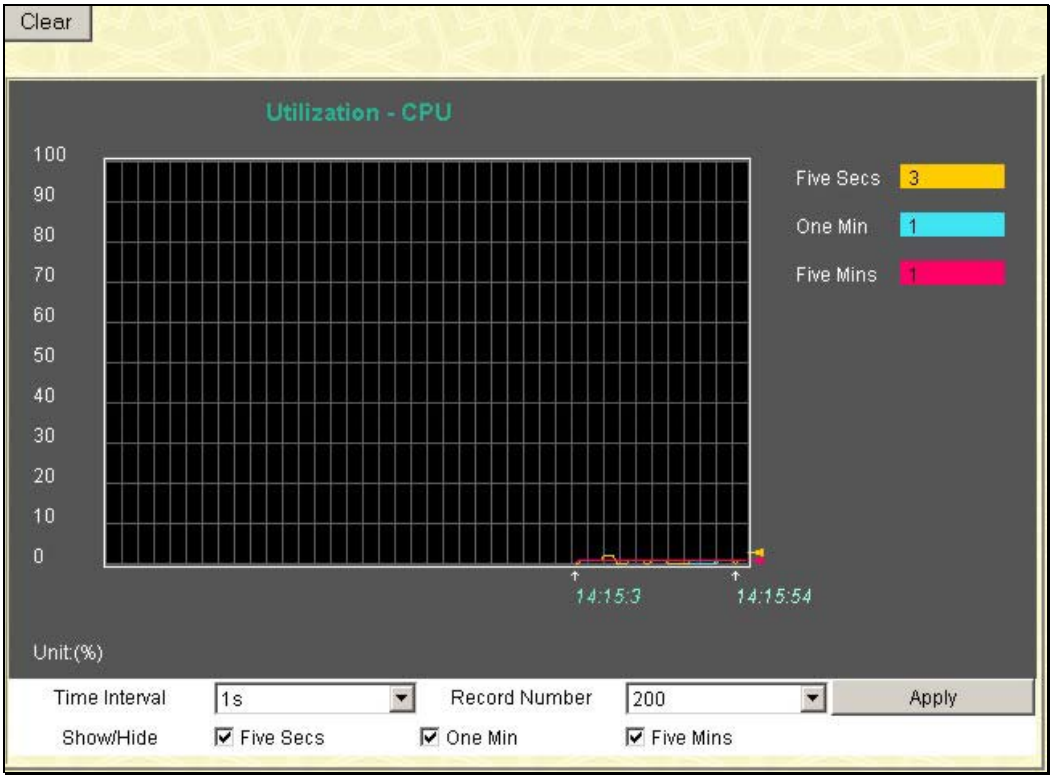


Figure 10- 3. CPU Utilization graph

To view the CPU utilization by port, 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. Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics.

Change the view parameters as follows:

Parameter	Description
Time Interval ***[1s]***	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number ***[200]***	Select number of times the Switch will be polled between 20 and 200. The default value is 200.

Port Utilization

The **Port Utilization** page 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:

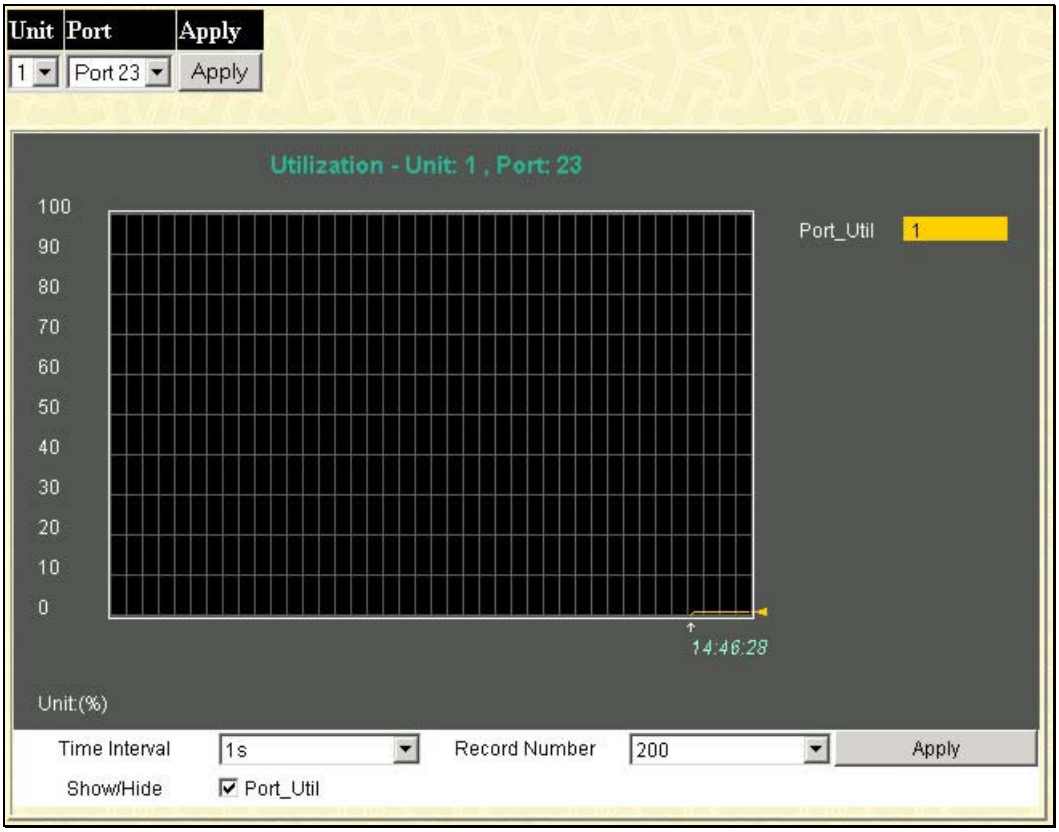


Figure 10- 4. Port Utilization window

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.

Change the view parameters as follows:

Parameter	Description
Time Interval ***[1s]***	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number ***[200]***	Select number of times the Switch will be polled between 20 and 200. The default value is 200.

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. 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.

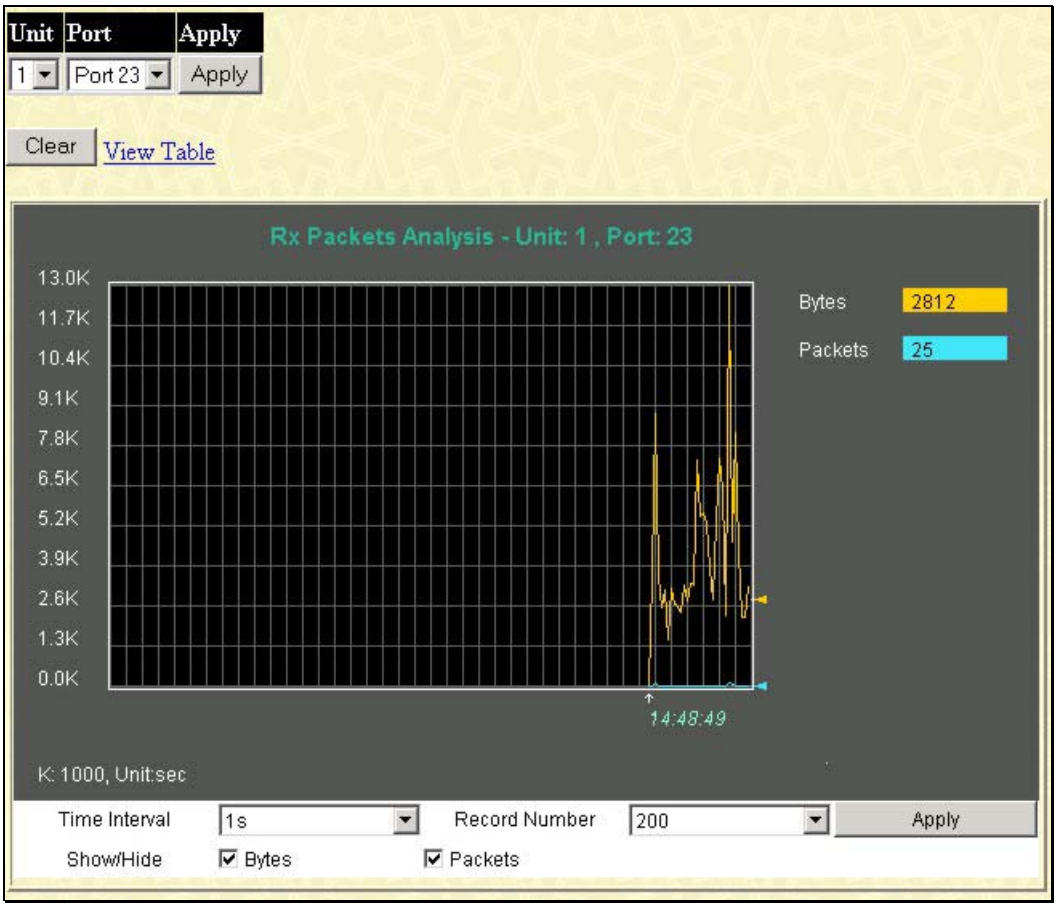


Figure 10- 5. Rx Packets Analysis (line graph for Bytes and Packets)

To view the **Received Packets Table**, click the link View Table.

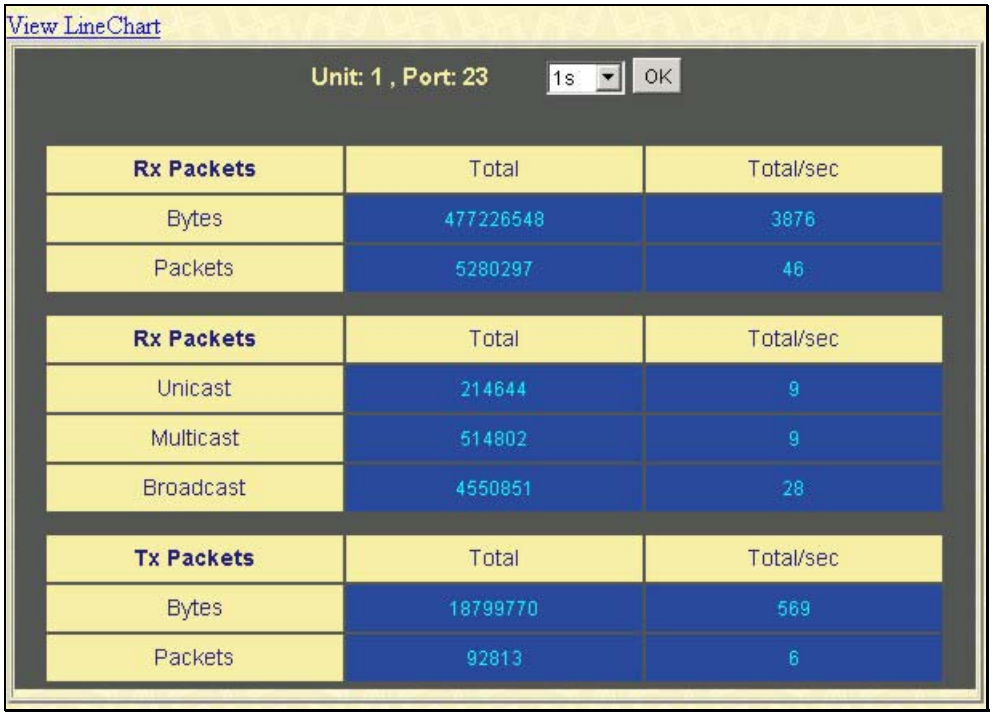


Figure 10- 6. Rx Packets Analysis Table

The following fields may be set or viewed:

Parameter	Description
Time Interval [1s]	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number [200]	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.
Clear	Clicking this button clears all statistics counters on this window.
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.

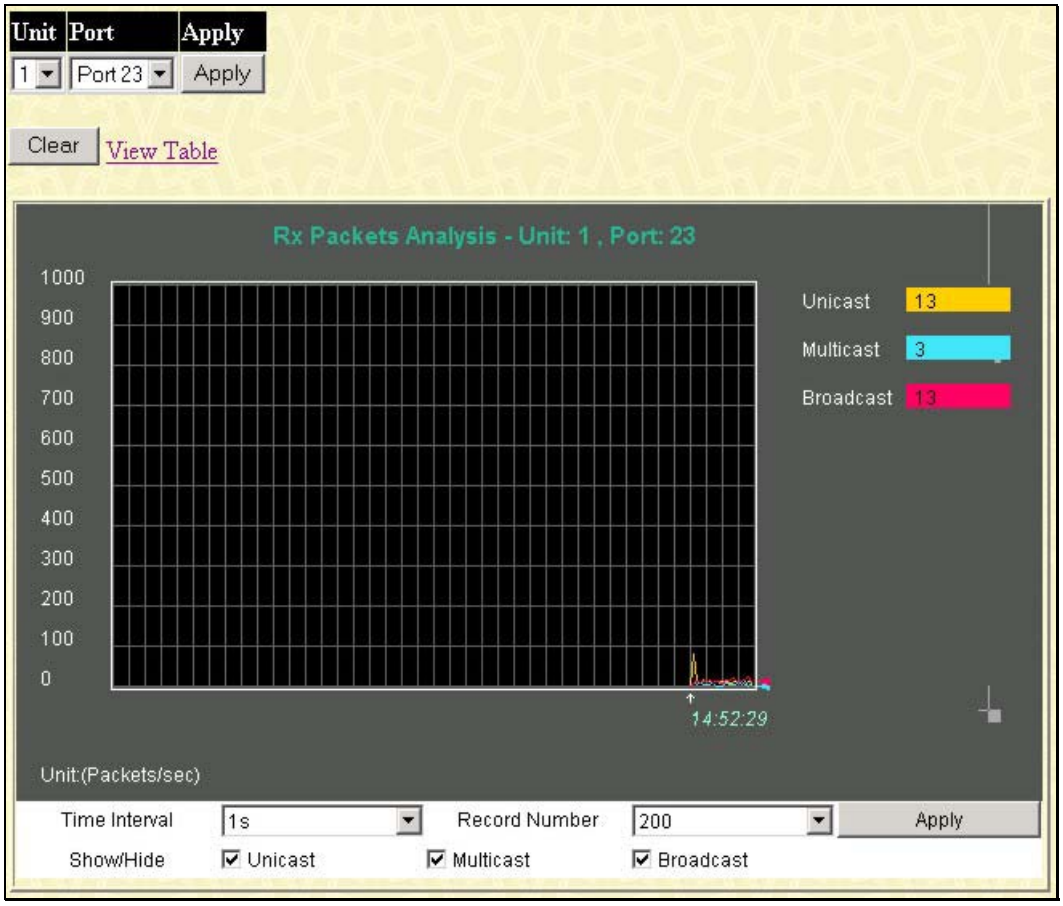


Figure 10- 7. Packets Analysis (line graph for Unicast, Multicast, and Broadcast Packets)

To view the **UMB Cast Table**, click the View Table link.

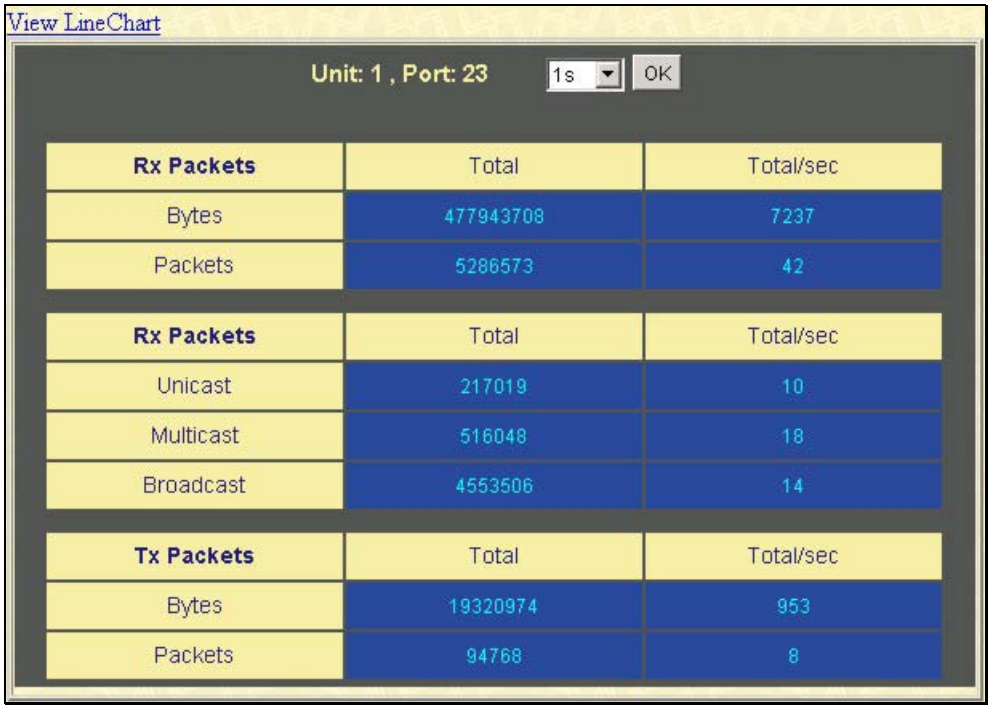


Figure 10- 8. Rx Packets Analysis window (table for Unicast, Multicast, and Broadcast Packets)

The following fields may be set or viewed:

Parameter	Description
Time Interval [1s]	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number [200]	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.
Clear	Clicking this button clears all statistics counters on this window.
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.

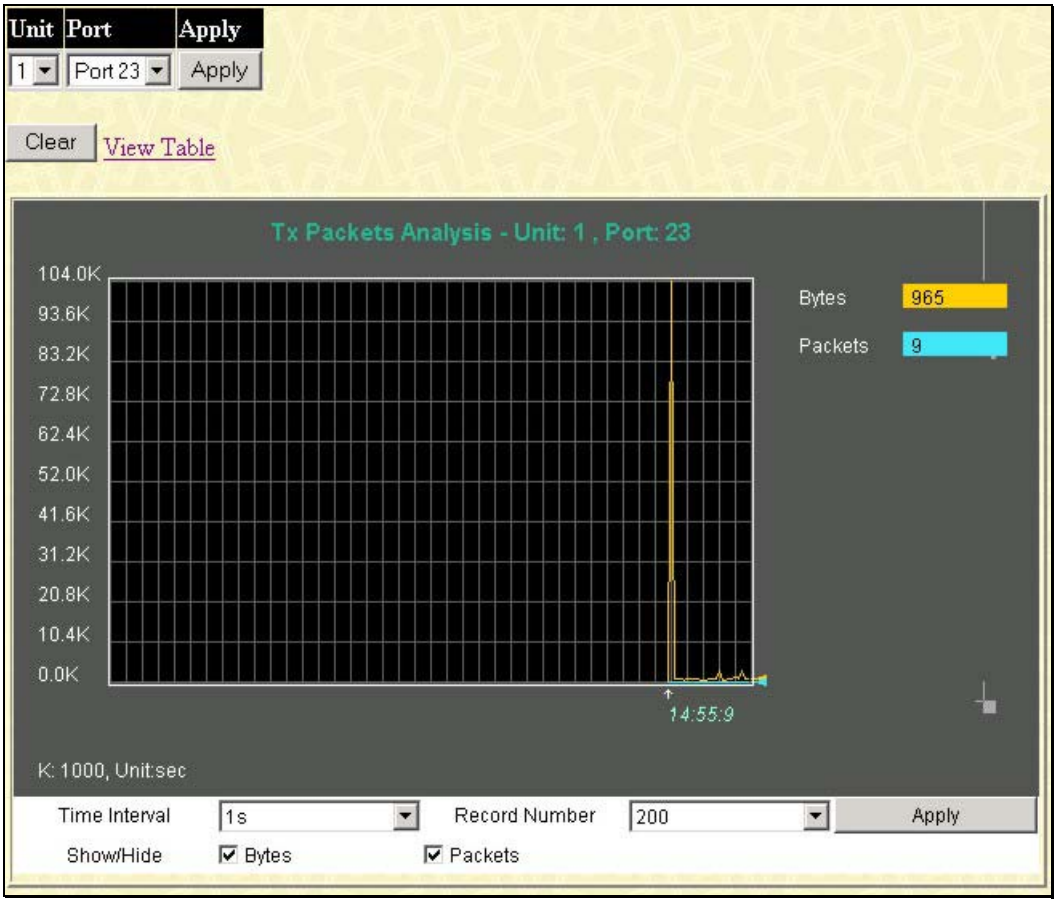


Figure 10- 9. Tx Packets Analysis window (line graph for Bytes and Packets)

To view the **Transmitted (TX) Table**, click the link View Table.

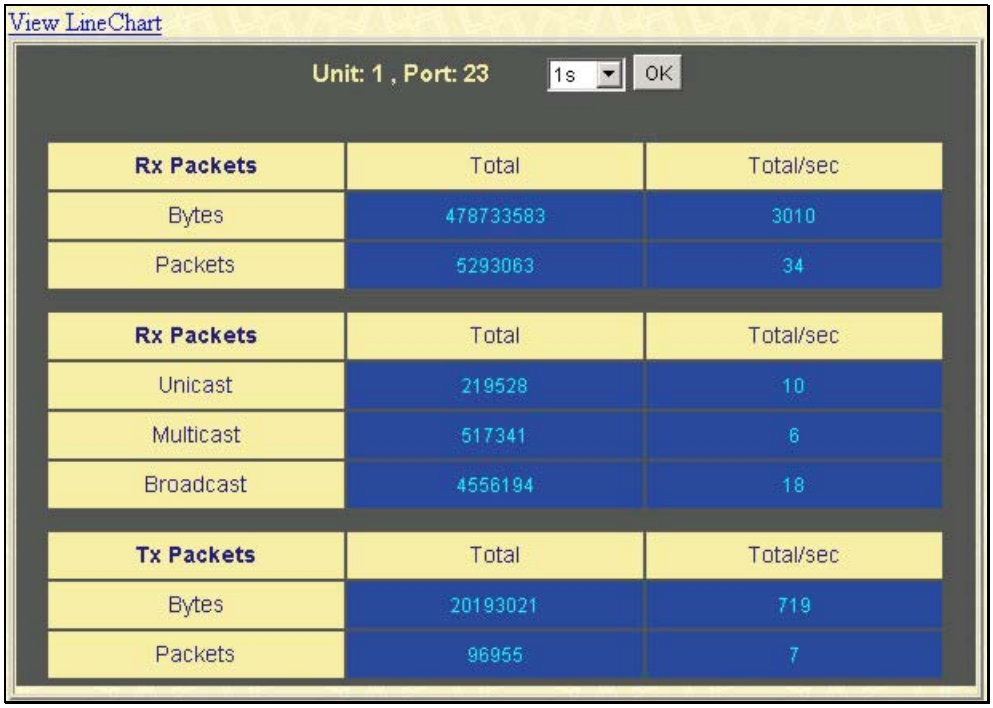


Figure 10- 10. Tx Packets Analysis window (table for Bytes and Packets)

The following fields may be set or viewed:

Parameter	Description
Time Interval [1s]	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number [200]	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 on 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.
Clear	Clicking this button clears all statistics counters on this window.
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 **Error** 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.

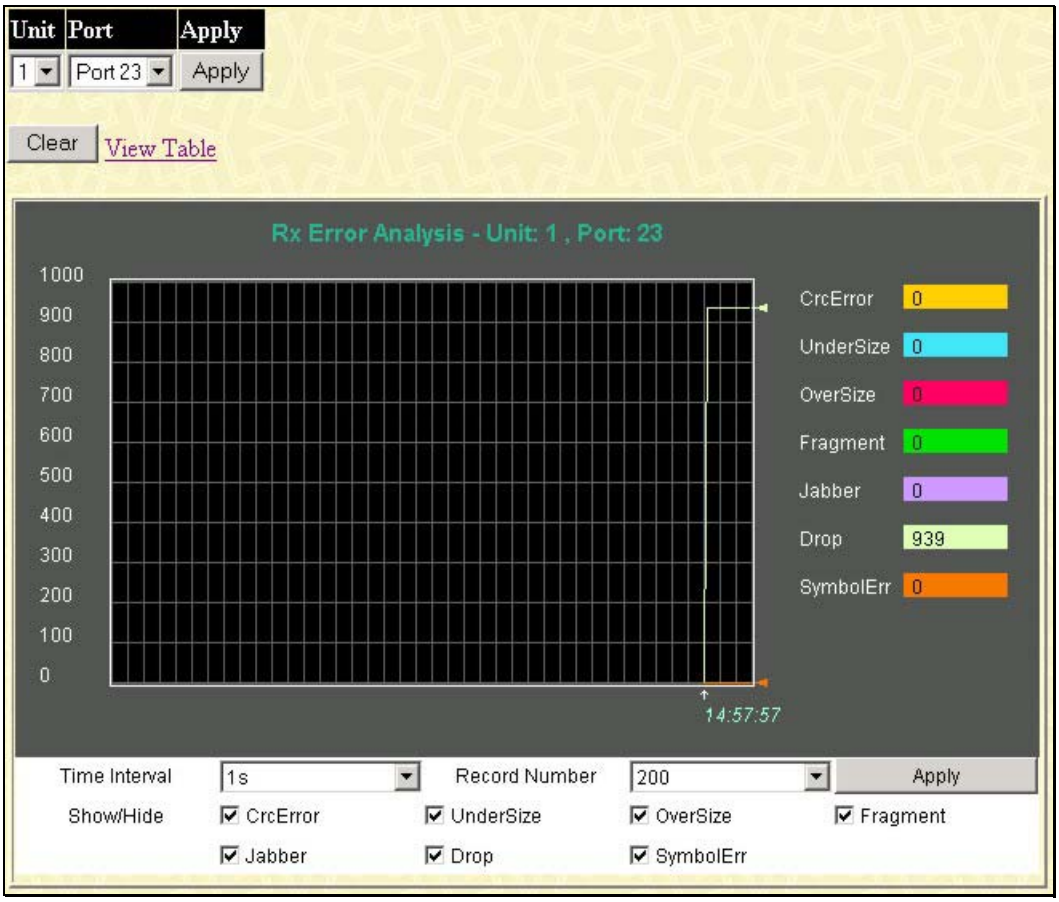


Figure 10- 11. Rx Error Analysis window (line graph)

To view the **Received Error Packets Table**, click the link **View Table**, which will show the following table:

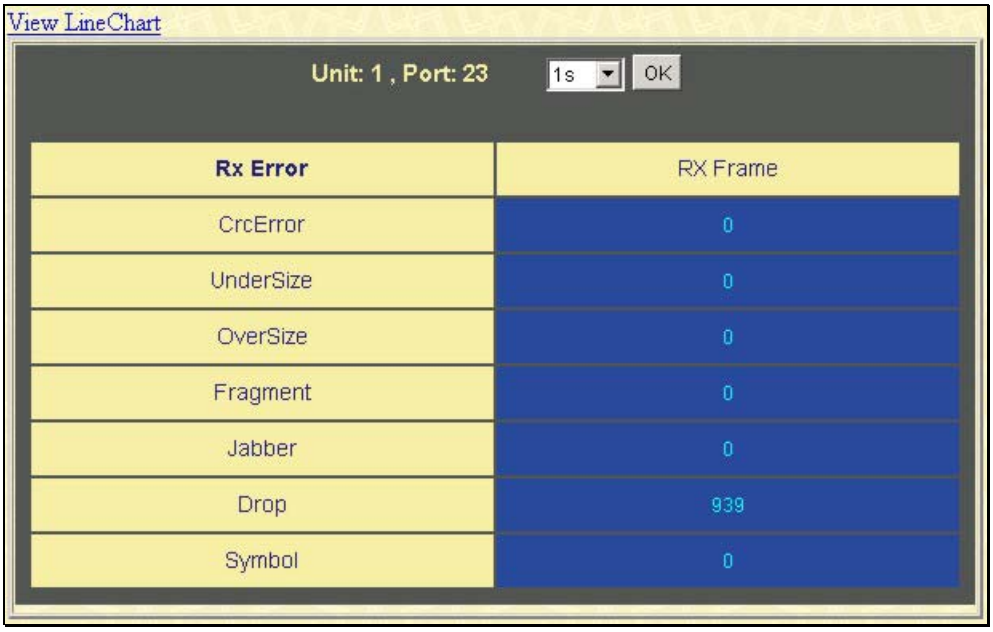


Figure 10- 12. Rx Error Analysis window (table)

The following fields can be set:

Parameter	Description
Time Interval [1s]	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number [200]	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.
UnderSize	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 valid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
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	Counts invalid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Drop	The number of packets that are dropped by this port since the last Switch reboot.
Symbol	Counts the number of packets received that have errors received in the symbol on the physical labor.
Show/Hide	Check whether or not to display CRC Error, Under Size, Over Size, Fragment, Jabber, and Drop errors.
Clear	Clicking this button clears all statistics counters on this window.
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 Error 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.

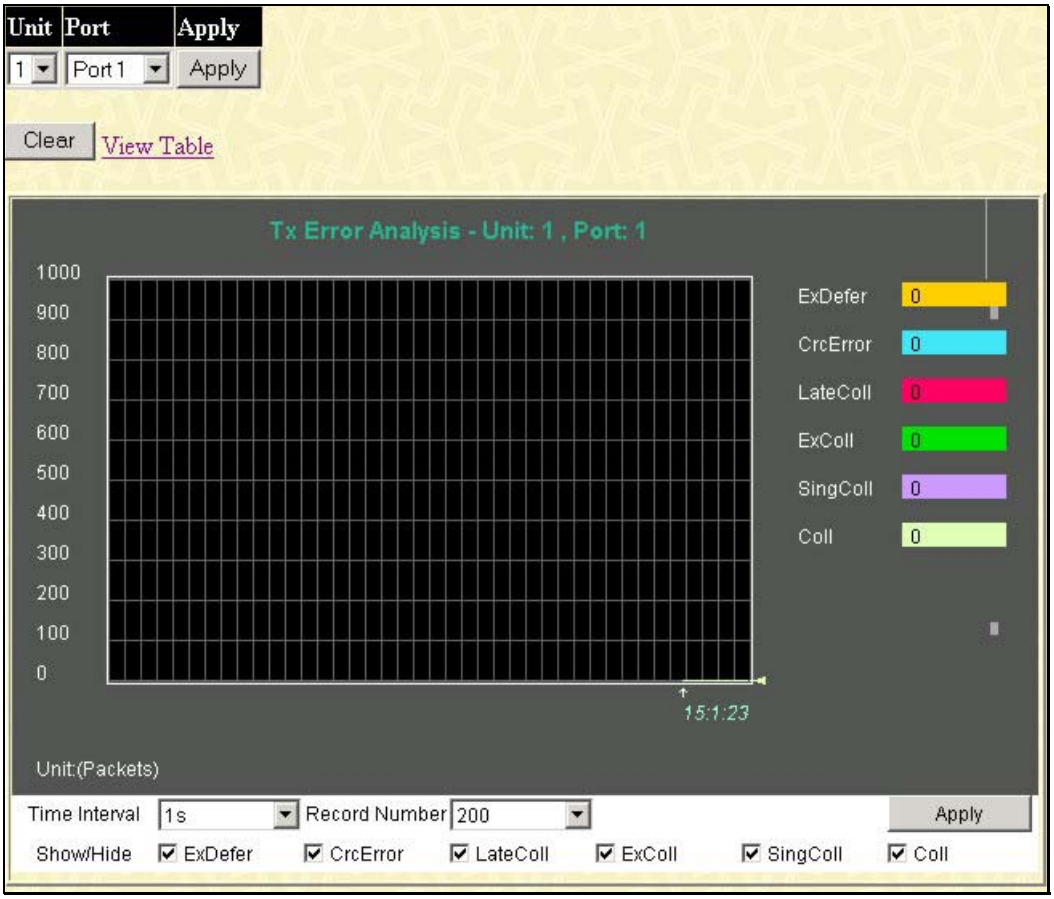


Figure 10- 13. Tx Error Analysis (line graph)

To view the **Transmitted Error Packets Table**, click the link View Table, which will show the following table:

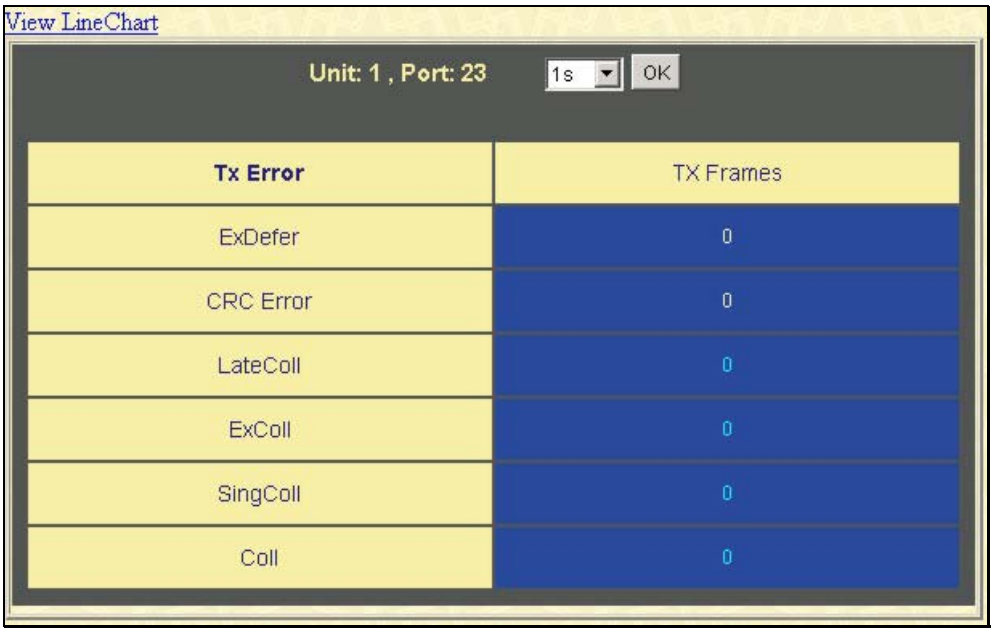


Figure 10- 14. Tx Error Analysis window (table)

The following fields may be set or viewed:

Parameter	Description
Time Interval *[1s]*	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number *[200]*	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.
CRC Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
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.
Clear	Clicking this button clears all statistics counters on this window.
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.

Packet 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.

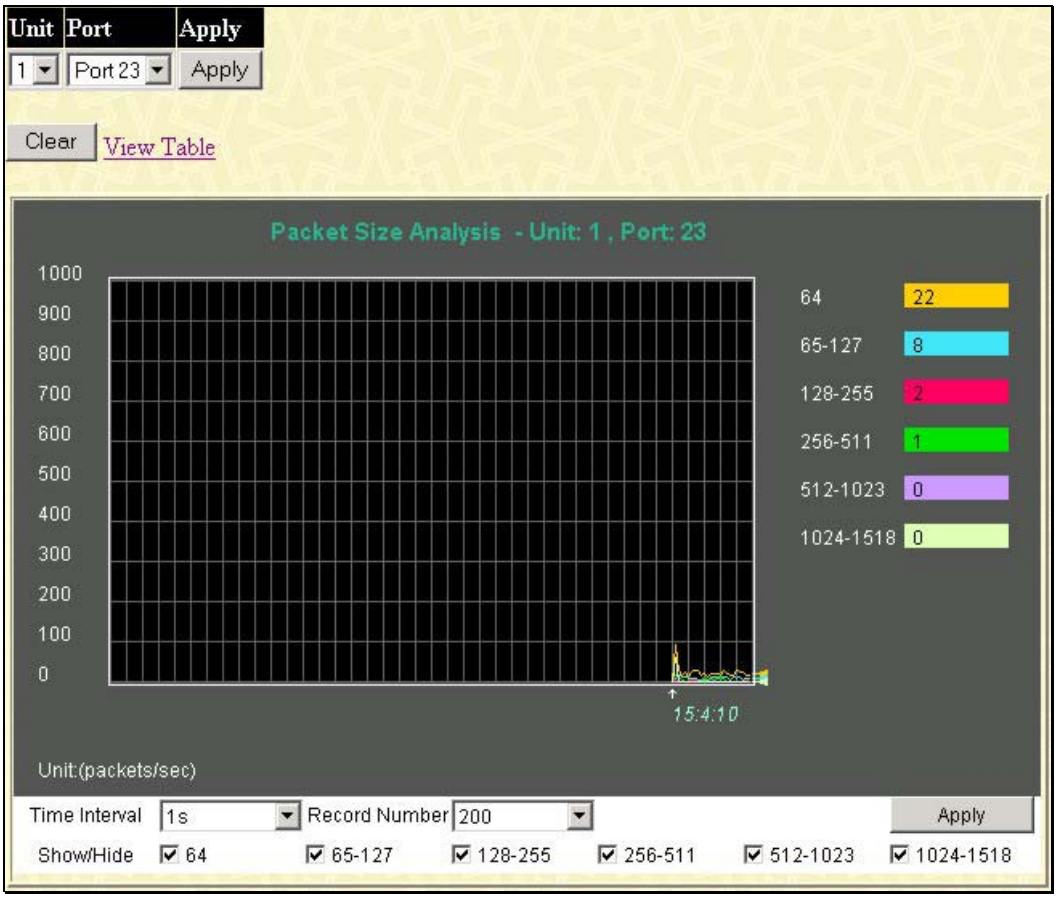
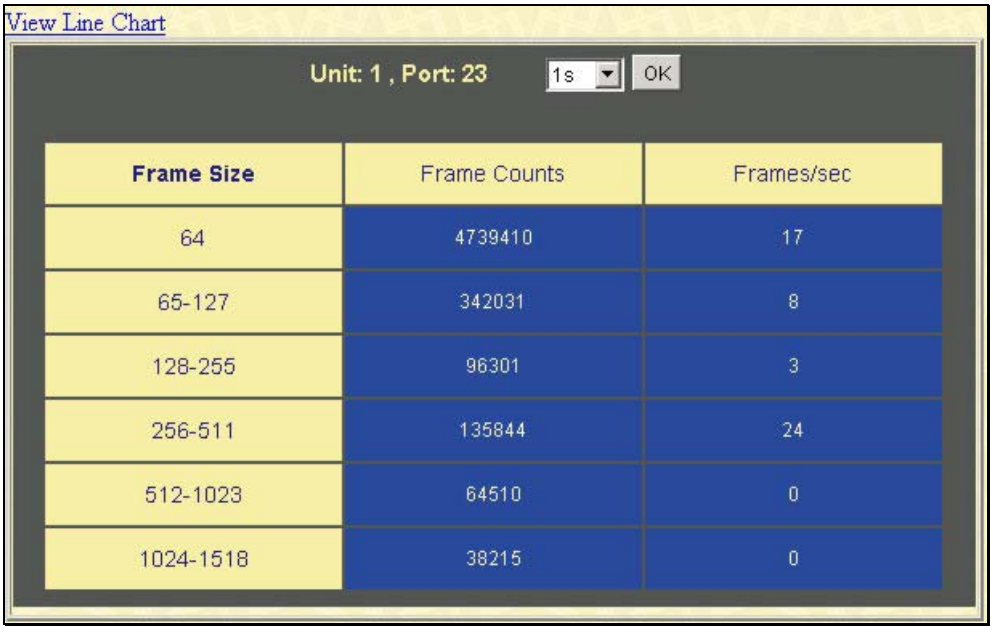


Figure 10- 15. Rx Size Analysis window (line graph)

To view the **Packet Size Analysis Table**, click the link View Table, which will show the following table:



Frame Size	Frame Counts	Frames/sec
64	4739410	17
65-127	342031	8
128-255	96301	3
256-511	135844	24
512-1023	64510	0
1024-1518	38215	0

Figure 10- 16. Rx Size Analysis window (table)

The following fields can be set or viewed:

Parameter	Description
Time Interval [1s]	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number [200]	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.
Clear	Clicking this button clears all statistics counters on this window.
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.

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** and a Forbidden port is designated by **F**. To view the following window, open the **Monitoring** folder and click the **Browse Router Port** link.

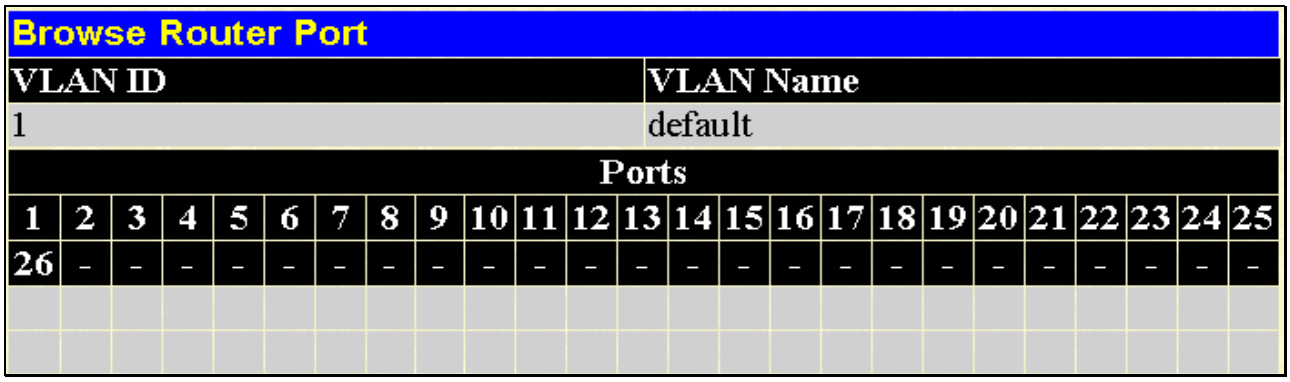


Figure 10- 17. Browse Router Port Browse MLD Router Port

Browse MLD Router Port

This displays which of the Switch's ports are currently configured as router ports in IPv6. 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** and a Forbidden port is designated by **F**.

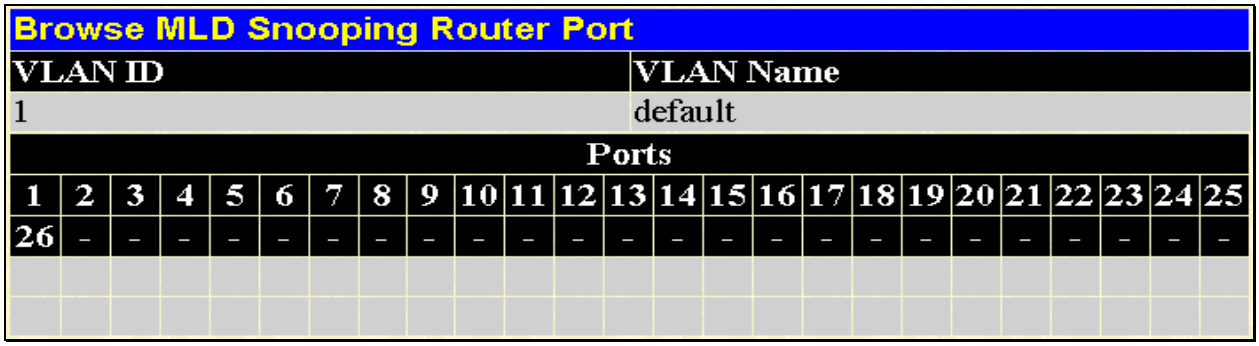
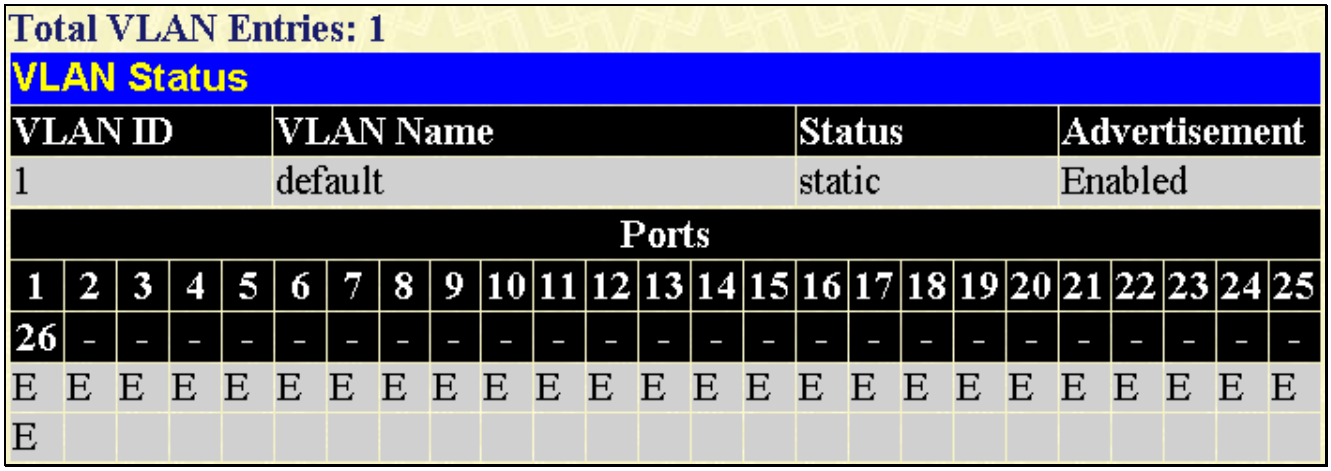


Figure 10- 18. Browse MLD Snooping Router Port window

VLAN Status

This allows the VLAN status for each of the Switch's ports to be viewed by VLAN. This window displays the ports on the Switch that are currently Egress (**E**) or Tag (**T**) ports. To view the following table, open the **Monitoring** folder and click the **VLAN Status** Link.



Total VLAN Entries: 1

VLAN Status

VLAN ID	VLAN Name	Status	Advertisement
1	default	static	Enabled

Ports																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
26	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
E																								

Figure 10- 19. VLAN Status window

Port Access Control

The following screens are used to monitor 802.1X statistics of the Switch, on a per port basis. To view the **Port Access Control** screens, open the monitoring folder and click the **Port Access Control** folder. There are two screens to monitor.

RADIUS Authentication

This table contains information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol. To view the **RADIUS Authentication**, click **Monitoring > Port Access Control > RADIUS Authentication**.

Figure 10- 20. RADIUS Authentication information 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 information is displayed:

Parameter	Description
InvalidServerAddresses	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.)
ServerIndex	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.
AuthServerAddress	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.
AccessRetransmissions	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 Account Client

This window shows managed objects used for managing RADIUS accounting clients, and the current statistics associated with them. To view the **RADIUS Accounting**, click **Monitoring > Port Access Control > RADIUS Account Client**.

Figure 10- 21. RADIUS Account Client information

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 information is displayed:

Parameter	Description
ClientInvalidServerAddresses	The number of RADIUS Accounting-Response packets received from unknown addresses.
ClientIdentifier	The NAS-Identifier of the RADIUS accounting client. (This is not necessarily the same as sysName in MIB II.)
ServerIndex	The identification number assigned to each RADIUS Accounting server that the client shares a secret with.
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.
ClientRoundTripTime	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
ClientRequests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
ClientRetransmissions	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.
ClientResponses	The number of RADIUS packets received on the accounting port from this server.
ClientMalformedResponses	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.
ClientBadAuthenticators	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
ClientPendingRequests	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.
ClientTimeouts	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.
ClientUnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
ClientPacketsDropped	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 xStack switch, go to the **Administration** folder and select **Port Access Entity**.

MAC Address Table

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 Table** link:

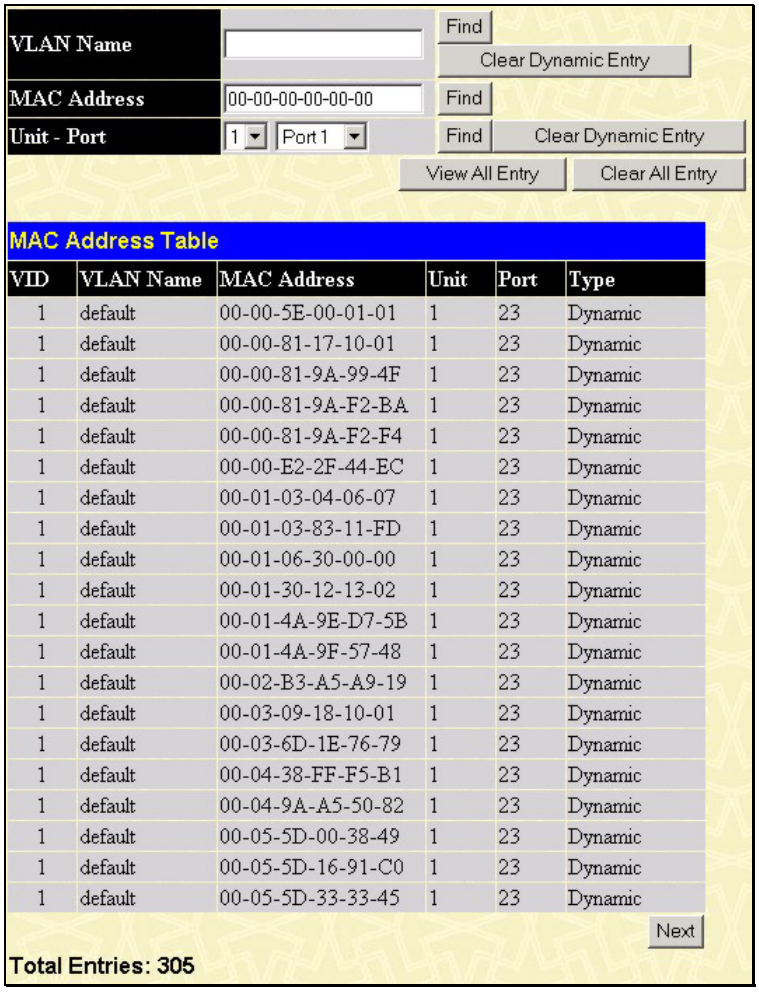


Figure 10- 22. MAC Address Table

The functions are used in the MAC address table:

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 unit of the switch in the switch stach, and a port on that switch, where to find the MAC address.
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 of which the port is a member.
VLAN Name	The VLAN Name of the VLAN of which the port is a member.
MAC Address	The MAC address entered into the address table.
Unit - Port	The unit and port to which the MAC address above corresponds.
Type	Describes the method which 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.
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.

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**, click **IGMP Snooping Group** on the **Monitoring** menu:

Figure 10- 23. IGMP Snooping Group Table

The user may search the **IGMP Snooping Group Table** by VLAN name by entering it in the top left hand 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	The ports that are members of the group.

NOTE: To configure IGMP snooping for the xStack DGS-3400 Series switch, go to the **Administration** folder and select **IGMP Snooping**. Configuration and other information concerning IGMP snooping may be found in Section 7 of this manual under **IGMP Snooping**.

MLD Snooping Group

The following window allows the user to view MLD Snooping Groups present on the Switch. MLD Snooping is an IPv6 function comparable to IGMP Snooping for IPv4. The user may browse this table by VLAN Name present in the switch by entering that VLAN Name in the empty field shown below, and clicking the Search button. The number of MLD reports that were snooped is displayed in the **Reports** field.

To view the **MLD Snooping Group Table**, click **MLD Snooping Group** on the **Monitoring** menu:

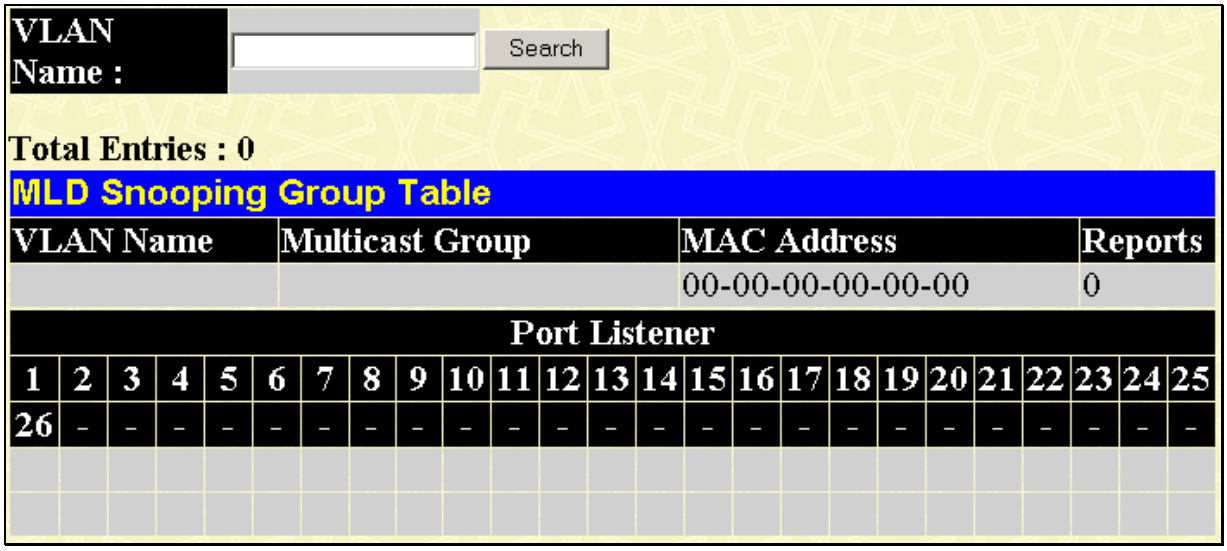


Figure 10- 24. MLD Snooping Group Table

The following field can be viewed:

Parameter	Description
VLAN Name	The VLAN Name of the MLD multicast group.
Multicast Group	The IP address of the MLD multicast group.
MAC Address	The MAC address of the MLD multicast group.
Reports	The total number of reports received for this group.

NOTE: To configure MLD snooping for the xStack DGS-3400 Series switch, go to the **Administration** folder and select **MLD Snooping**. Configuration and other information concerning MLD snooping may be found in Section 7 of this manual under **MLD Snooping**.

Switch Logs

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 Log** link.

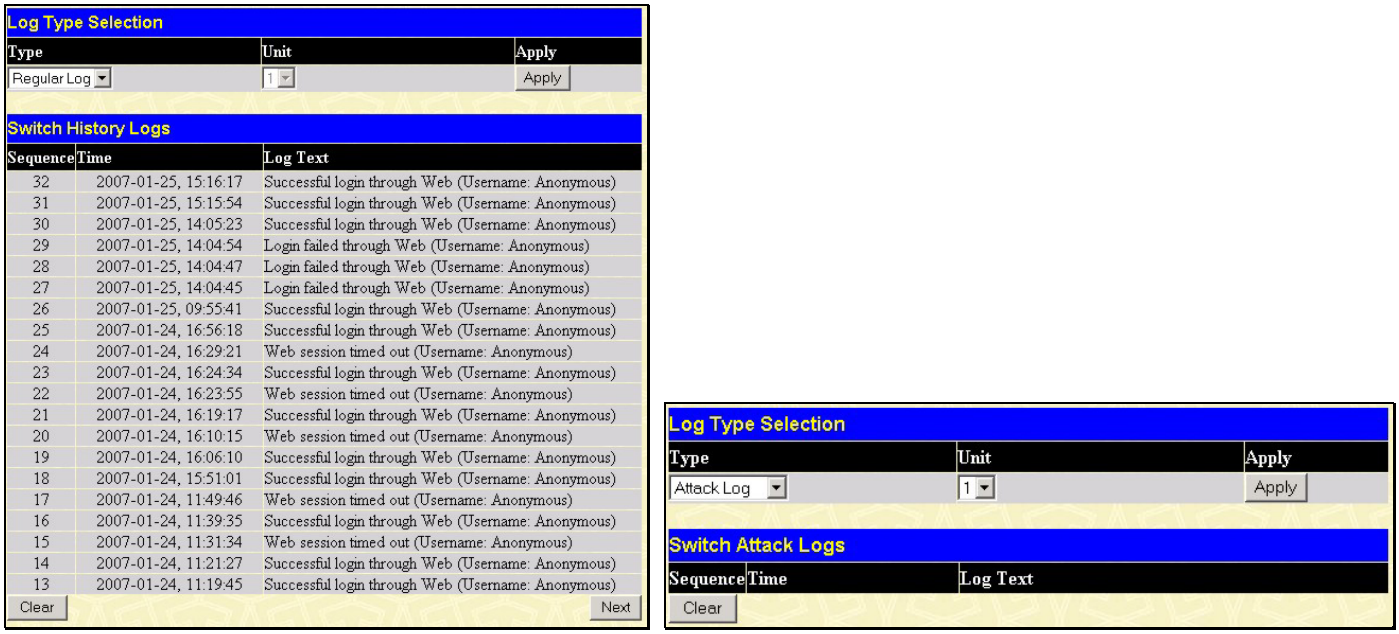


Figure 10- 25. Switch History Log window

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 in the table is categorized as:

Parameter	Description
Type	Choose the type of log to view. There are two choices: *Regular Log* – Choose this option to view regular switch log entries, such as logins or firmware transfers. *Attack Log* – Choose this option to view attack log files, such as spoofing attacks.
Unit	Choose the Unit ID of the switch in the switch stack for which to view the switch log.
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.

Browse ARP Table

The **Browse ARP Table** window may be found in the **Monitoring** menu. 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.**

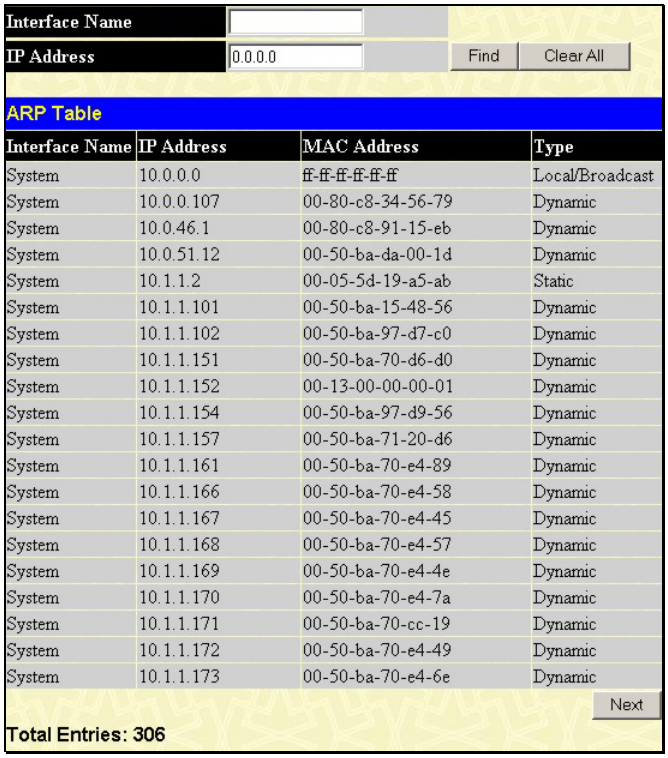


Figure 10- 26. Browse ARP Table window

Session Table

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

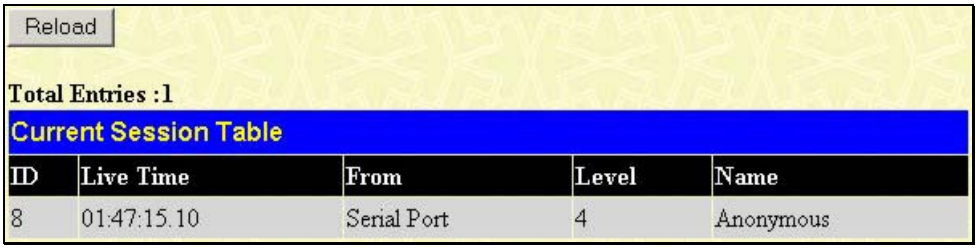


Figure 10- 27. Current Session Table

IP Forwarding Table

The **IP Forwarding Table** may be found in the **Monitoring** menu. The **IP Forwarding Table** is a read-only screen 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 screen and click **Find** to begin your search.

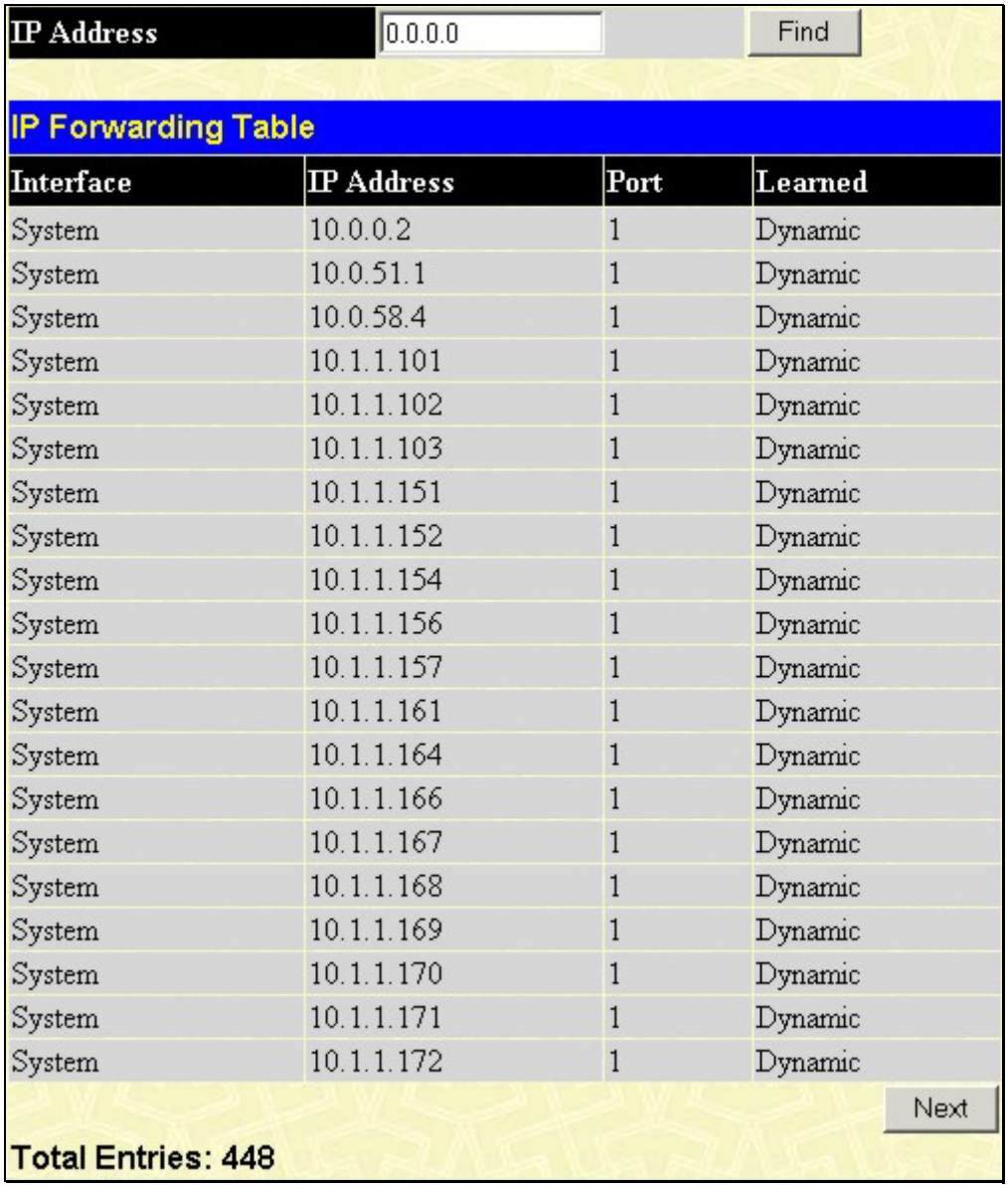


Figure 10- 28. IP Forwarding Table

Browse Routing Table

The **Browse Routing Table** window may be found in the **Monitoring** menu. This screen shows the current IP routing table of the Switch. To find a specific IP route, enter an IP address into the **IP Address** field along with a proper subnet mask into the **Netmask** field and click **Find**.

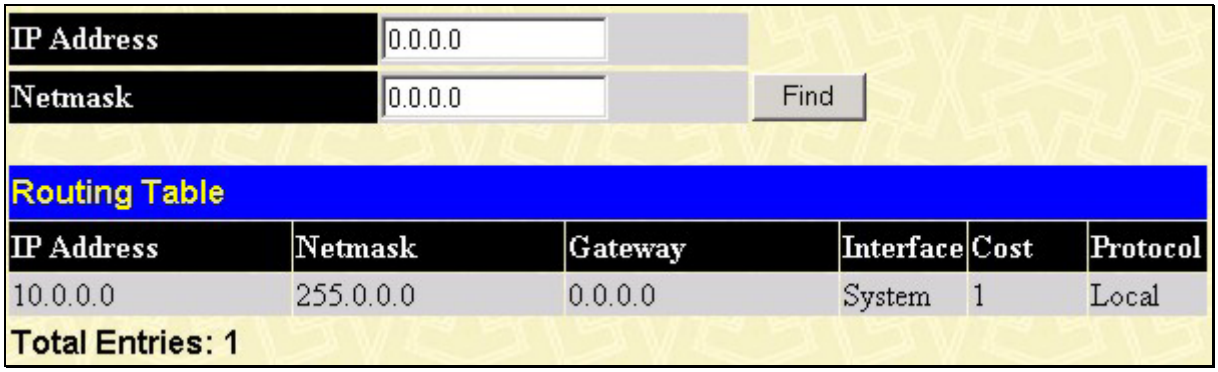


Figure 10- 29. Browse Routing Table

Section 11

Save, Reset and Reboot

Reset

Reboot System

Save Services

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

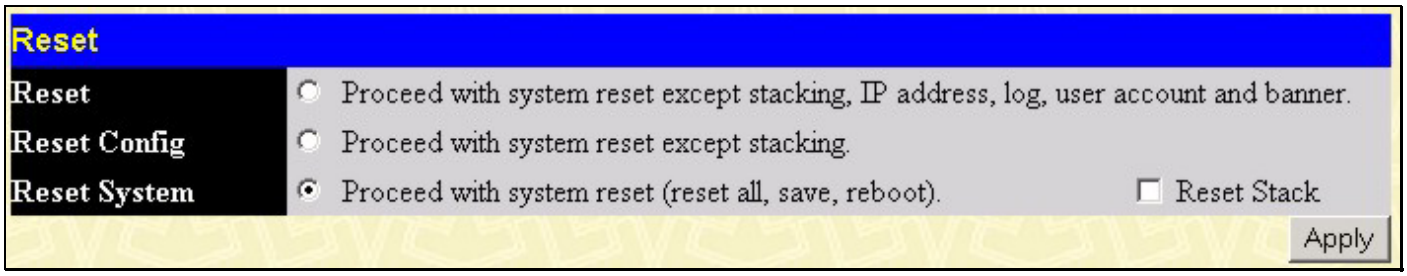


Figure 11- 1. Reset options

Reboot System

The following menu is used to restart the Switch.

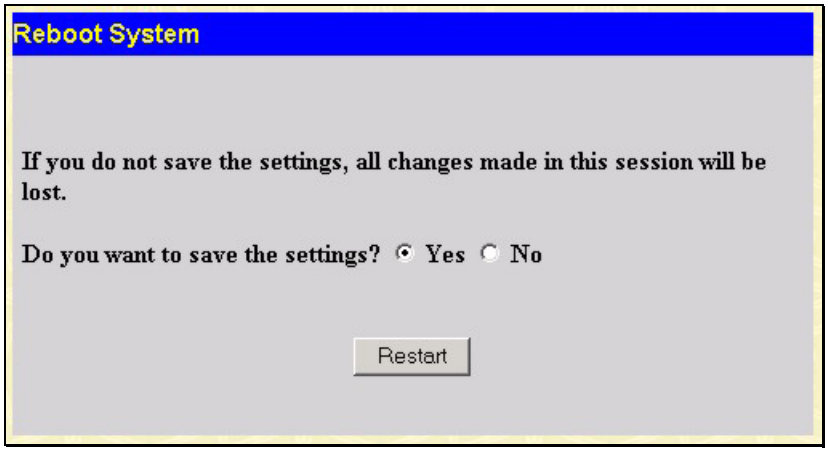


Figure 11- 2. Reboot System

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.

Save Services

The following three windows will aid the user in saving configurations to the Switch's memory.

Save Changes

The Switch has two levels of memory, normal RAM and non-volatile or NV-RAM. Configuration changes are made effective clicking the **Save** 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 Changes** menu. The save options allow one alternative configuration image to be stored.

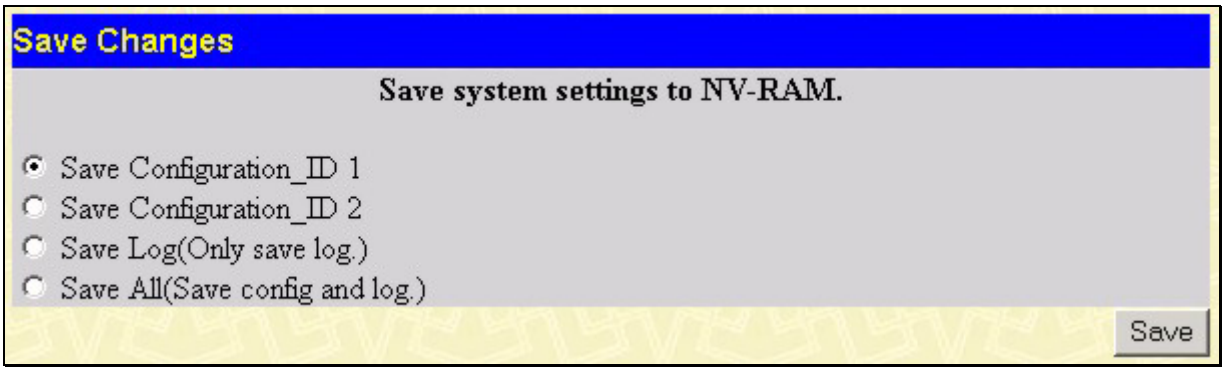


Figure 10- 30. Save Changes menu

The Save Changes options include:

- **Save Configuration_ID_1** to save the configuration file indexed as Image file 1. To use this file for configuration it must be designated as the *Boot* configuration using the **Config Current Setting** menu (**Save Services > Config Current Setting**)
- **Save Configuration_ID_2** to save the configuration file indexed as Image file 2. To use this file for configuration it must be designated as the *Boot* configuration using the **Config Current Setting** menu (**Save Services > Config Current Setting**)
- **Save Log** to save only the current log.
- **Save All** to save the current configuration file indexed as Image file 1 and save the current log.

Configuration Information

The following window is used to view information regarding configuration files saved in the Switch. The Switch can hold two configuration files in its memory. Configuration Files any be uploaded to the Switch using the TFTP services located in the Administration folder.

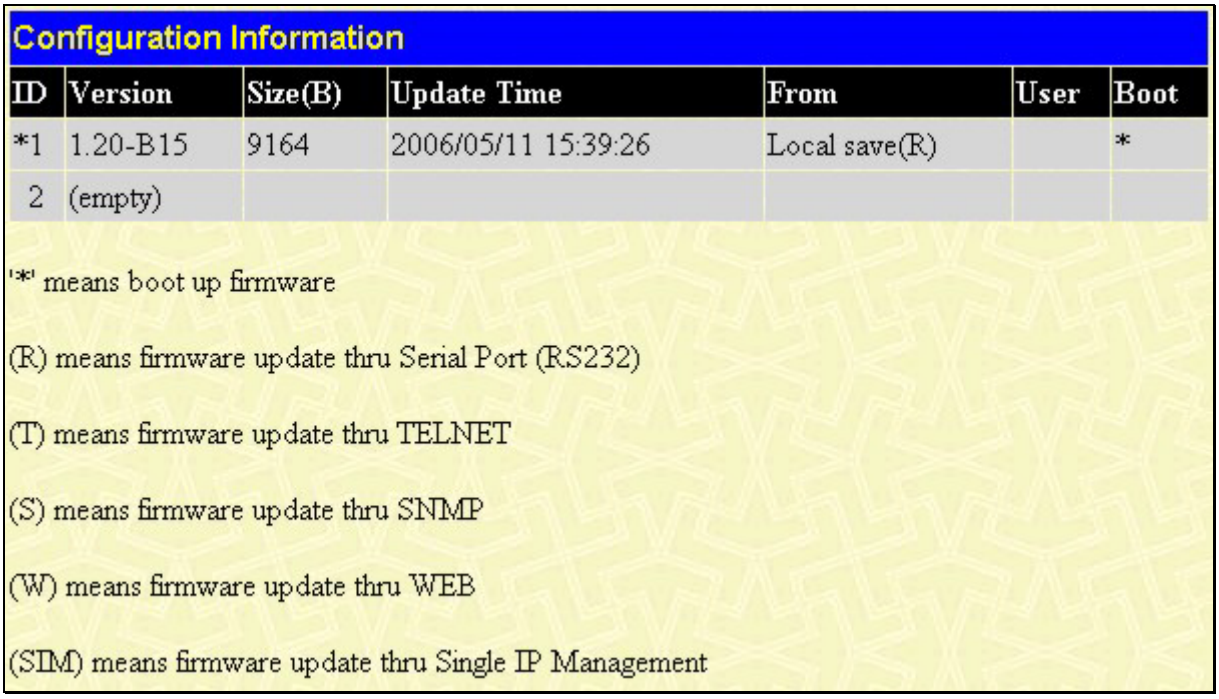


Figure 10- 31. Configuration Information window

This window holds the following information:

Parameter	Description
ID	States the image ID number of the configuration file in the Switch's memory. The Switch can store 2 configuration files for use. Image ID 1 will be the default boot up configuration file for the Switch unless otherwise configured by the user.
Version	States the firmware version.
Size	States the size of the corresponding configuration file, in bytes.
Update Time	States the specific time the configuration file was downloaded to the Switch.
From	States the origin of the firmware. There are five ways configuration files may be uploaded to the Switch. **R** – If the IP address has this letter attached to it, it denotes a configuration file upgrade through the Console Serial Port (RS-232). **T** - If the IP address has this letter attached to it, it denotes a configuration file upgrade through Telnet. **S** - If the IP address has this letter attached to it, it denotes a configuration file upgrade through the Simple Network Management Protocol (SNMP). **W** - If the IP address has this letter attached to it, it denotes a configuration file upgrade through the web-based management interface. **SIM** – If the IP address has this letter attached to it, it denotes a configuration file upgrade through the Single IP Management feature.
User	States the user who uploaded the configuration file. This field may read "Anonymous" or "Unknown" for users that are not identified.
Boot	If this field reads an asterisk (*), then this configuration file is the boot up configuration file for the Switch.

Current Configuration Settings

The following window is used to select one of the two possible configuration files that can be stored in the Switch as a boot up configuration file, or to select it for deletion from the Switch's memory. To access the following screen, click **Save Services > Config Current Setting**.

Figure 11- 3. Configuration Settings window

This window holds the following information to be configured:

Parameter	Description
Configuration ID	Select the configuration file ID to be configured using the pull-down menu. The Switch allows two configuration file ID's to be stored in the Switch's memory.
Action	This field has three options for configuration. • *Delete* – Select this option to delete the configuration file ID specified in the **Configuration ID** field above. • *Boot_up* – Select this option to set the configuration file ID specified above as the boot up configuration file ID for the Switch. This firmware will be set as the boot up configuration file ID after a Switch reboot has been performed. The default setting has Configuration ID 1 as the boot up firmware image for the Switch unless specified here. • *Active* – Select this option to set the configuration file ID specified above as the file to be immediately implemented. Once selected and Apply is clicked, the Switch will upload this Configuration file for current use.

Click Apply to implement changes made.

Logout

Use the **Logout** page to logout of the Switch's Web-based management agent by clicking on the **Logout** hyperlink.

Appendix A Technical Specifications

Specifications listed here apply to all Switches in the DGS-3400 series except where otherwise noted.

General	
Standards	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z 1000BASE-T (SFP "Mini GBIC") IEEE 802.3ae (10G Optional Modules) IEEE 802.1D/w/s Spanning Tree (Rapid, Multiple) IEEE 802.1P/Q VLAN IEEE 802.1p Priority Queues IEEE 802.1v Protocol VLAN IEEE 802.1X Network Access Control IEEE 802.3 Nway auto-negotiation IEEE 802.3ad Link Aggregation Control IEEE 802.3x Full-duplex Flow Control IEEE 802.1u Fast Ethernet IEEE 802.3af Power-over-Ethernet
Protocols	CSMA/CD
Data Transfer Rates:	Half-duplex Full-duplex
Ethernet	10 Mbps 20Mbps
Fast Ethernet	100Mbps 200Mbps
Gigabit Ethernet	1000Mbps 2000Mbps
Fiber Optic	SFP (Mini GBIC) Support IEEE 802.3z 1000BASE-LX (DEM-310GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-311GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-312GT2 transceiver) IEEE 802.3z 1000BASE-LH (DEM-314GT transceiver) IEEE 802.3z 1000BASE-ZX (DEM-315GT transceiver) WDM Single Mode Transceiver 10km (DEM-330T/R) WDM Single Mode Transceiver 40km (DEM-331T/R)
Topology	Duplex Ring, Duplex Chain
Network Cables	Cat.5 Enhanced for 1000BASE-T UTP Cat.5, Cat. 5 Enhanced for 100BASE-TX UTP Cat.3, 4, 5 for 10BASE-T EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)

Physical and Environmental		
Internal Power Supply **Redundant Power Supply**	AC Input: 100 - 240 VAC, 50-60 Hz	
Power Consumption	**DGS-3400 Series Switch** DGS-3426 (70.8 Watts) DGS-3426P (433 Watts) DGS-3427 (71.6 Watts) DGS-3450 (131.34 Watts)	**Module Inserts** DEM-410CX (0.015 Watts) DEM-410X (6.16 Watts)
DC Fan:	12v	
Operating Temperature	0 - 40°C	
Storage Temperature	-40 - 70°C	
Humidity	5 - 95% non-condensing	
Dimensions	441mm x 389mm x 44mm	
Weight	**DGS-3400 Series Switch** DGS-3426 (5.42 kg) DGS-3426P (6 kg) DGS-3427 (5.51 kg) DGS-3450 (5.74 kg)	**Module Inserts** DEM-410CX (0.16 kg) DEM-410X (0.18 kg)
EMI:	CE class A, FCC Class A	
Safety:	CSA International, CB Report	

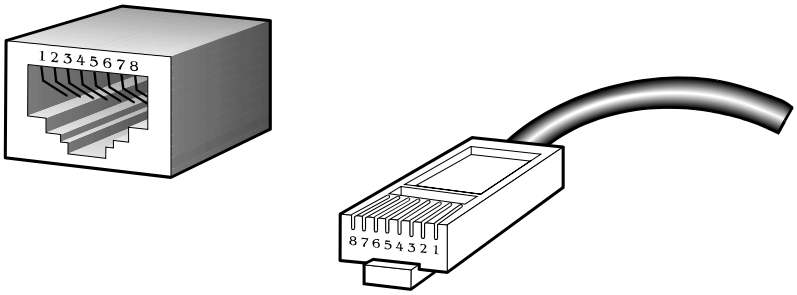
Performance	
Transmission Method	Store-and-forward
Packet Buffer	0.75 MB per device
Packet Filtering / Forwarding Rate	Full-wire speed for all connections 1,488,095 pps per port (for 1000Mbps)
MAC Address Learning	Automatic update. Supports 8K MAC address.
Priority Queues	8 Priority Queues per port.
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 1- 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	1000BASE-T	1000BASE-T
5	1000BASE-T	1000BASE-T
6	TD- (transmit)	RD- (receive)
7	1000BASE-T	1000BASE-T
8	1000BASE-T	1000BASE-T

Appendix 1- 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 1000BASE-SX, Multi-mode fiber module 1000BASE-LHX, Single-mode fiber module 1000BASE-ZX, Single-mode fiber module	10km 550m / 2km 40km 80km
1000BASE-T	Category 5e UTP Cable Category 5 UTP Cable (1000 Mbps)	100m
100BASE-TX	Category 5 UTP Cable (100 Mbps)	100m
10BASE-T	Category 3 UTP Cable (10 Mbps)	100m

Appendix D

Switch Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

Category	Event Description	Log Information	Severity	Remark
system	System started up	**Unit <unitID>, System started up**	Critical	
	System warm start	**Unit <unitID>, System warm start**	Critical	
	System cold start	**Unit <unitID>, System cold start**	Critical	
	Configuration saved to flash	**Unit <unitID>, Configuration saved to flash by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	"by console" and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, there will no IP and MAC information for logging.
	System log saved to flash	**Unit <unitID>, System log saved to flash by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	"by console"and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, there will no IP and MAC information for logging.
	Configuration and log saved to flash	**Unit <unitID>, Configuration and log saved to flash by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	"by console" and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, there will no IP and MAC information for logging.
	Internal Power failed	**Unit <unitID>, Internal Power failed**	Critical	
	Internal Power is recovered	**Unit <unitID>, Internal Power is recovered**	Critical	
	Redundant Power failed	**Unit <unitID>, Redundant Power failed**	Critical	
	Redundant Power is working	**Unit <unitID>, Redundant Power is working**	Critical	
	Side Fan failed	**Unit <unitID>, Side Fan failed**	Critical	
	Side Fan recovered	**Unit <unitID>, Side Fan recovered**	Critical	
	Back Fan failed	**Unit <unitID>, Back Fan failed**	Critical	
	Back Fan recovered	**Unit <unitID>, Back Fan recovered**	Critical	
up/down-load	Firmware upgraded successfully	**Unit <unitID>, Firmware upgraded by console successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging

	Firmware upgrade was unsuccessful	**Unit <unitID>, Firmware upgrade by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration successfully downloaded	**Configuration successfully downloaded by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration download was unsuccessful	**Configuration download by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration successfully uploaded	**Configuration successfully uploaded by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration upload was unsuccessful	**Configuration upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Log message successfully uploaded	**Log message successfully uploaded by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Log message upload was unsuccessful	**Log message upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
Interface	Port link up	**Port <unitID:portNum> link up, <link state>**	Informational	link state, for ex: , 100Mbps FULL duplex
	Port link down	**Port <unitID:portNum> link down**	Informational	
	Port GBIC module occur errors	**Port <unitID:portNum> GBIC module is abnormal**	Warning	
Stacking	Hot insert	**<unitID> Hot insert**	Informational	
	Hot remove	**<unitID> Hot remove**	Informational	
	Firmware upgraded to SLAVE successfully	**Firmware upgraded to SLAVE by console successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information

				for logging
	Firmware upgraded to SLAVE unsuccessfully	**Firmware upgraded to SLAVE by console unsuccessfully! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
Console	Successful login through Console	**Unit <unitID>, Successful login through Console (Username: <username>)**	Informational	There are no IP and MAC if login by console.
	Login failed through Console	**Unit <unitID>, Login failed through Console (Username: <username>)**	Warning	There are no IP and MAC if login by console.
	Logout through Console	**Unit <unitID>, Logout through Console (Username: <username>)**	Informational	There are no IP and MAC if login by console.
	Console session timed out	**Unit <unitID>, Console session timed out (Username: <username>)**	Informational	There are no IP and MAC if login by console.
Web	Successful login through Web	**Successful login through Web (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	
	Login failed through Web	**Login failed through Web (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	
	Logout through Web	**Logout through Web (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	
	Web session timed out	**Web session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	
	Successful login through Web (SSL)	**Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	
	Login failed through Web (SSL)	**Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	
	Logout through Web (SSL)	**Logout through Web (SSL) (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	
	Web (SSL) session timed out	**Web (SSL) session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	
Telnet	Successful login through Telnet	**Successful login through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	
	Login failed through Telnet	**Login failed through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	

	Logout through Telnet	**Logout through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	
	Telnet session timed out	**Telnet session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	
SNMP	SNMP request received with invalid community string	**SNMP request received from <ipAddress> with invalid community string!**	Informational	
STP	Topology changed	**Topology changed**	Informational	
	New Root selected	**New Root selected**	Informational	
	BPDU Loop Back on port	**BPDU Loop Back on Port <unitID:portNum>**	Warning	
	Spanning Tree Protocol is enabled	**Spanning Tree Protocol is enabled**	Informational	
	Spanning Tree Protocol is disabled	**Spanning Tree Protocol is disabled**	Informational	
DoS	Spoofing attack	**Possible spoofing attack from <macAddress> port <portNum>**	Critical	
SSH	Successful login through SSH	**Successful login through SSH (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	
	Login failed through SSH	**Login failed through SSH (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	
	Logout through SSH	**Logout through SSH (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	
	SSH session timed out	**SSH session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	
	SSH server is enabled	**SSH server is enabled**	Informational	
	SSH server is disabled	**SSH server is disabled**	Informational	
AAA	Authentication Policy is enabled	**Authentication Policy is enabled (Module: AAA)**	Informational	
	Authentication Policy is disabled	**Authentication Policy is disabled (Module: AAA)**	Informational	
	Successful login through Console authenticated by AAA local method	**Successful login through Console authenticated by AAA local method (Username: <username>)**	Informational	
	Login failed through Console authenticated by AAA local method	**Login failed through Console authenticated by AAA local method (Username: <username>)**	Warning	
	Successful login through Web authenticated by AAA local method	**Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Informational	

	Login failed through Web authenticated by AAA local method	**Login failed failed through Web from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful login through Web (SSL) authenticated by AAA local method	**Successful login through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Informational	
	Login failed through Web (SSL) authenticated by AAA local method	**Login failed through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful login through Telnet authenticated by AAA local method	**Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Informational	
	Login failed through Telnet authenticated by AAA local method	**Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful login through SSH authenticated by AAA local method	**Successful login through SSH from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Informational	
	Login failed through SSH authenticated by AAA local method	**Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful login through Console authenticated by AAA none method	**Successful login through Console authenticated by AAA none method (Username: <username>)**	Informational	
	Successful login through Web authenticated by AAA none method	**Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)**	Informational	
	Successful login through Web (SSL) authenticated by AAA none method	**Successful login through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)**	Informational	
	Successful login through Telnet authenticated by AAA	**Successful login through Telnet from <userIP> authenticated by AAA none**	Informational	

	none method	**method (Username: <username>, MAC: <macaddr>)**		
	Successful login through SSH authenticated by AAA none method	**Successful login through SSH from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)**	Informational	
	Successful login through Console authenticated by AAA server	**Successful login through Console authenticated by AAA server <serverIP> (Username: <username>)**	Informational	There are no IP and MAC if login by console.
	Login failed through Console authenticated by AAA server	**Login failed through Console authenticated by AAA server <serverIP> (Username: <username>)**	Warning	There are no IP and MAC if login by console.
	Login failed through Console due to AAA server timeout or improper configuration	**Login failed through Console due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful login through Web authenticated by AAA server	**Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational	
	Login failed through Web authenticated by AAA server	**Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning	
	Login failed through Web due to AAA server timeout or improper configuration	**Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful login through Web (SSL) authenticated by AAA server	**Successful login through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational	
	Login failed through Web (SSL) authenticated by AAA server	**Login failed through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning	
	Login failed through Web (SSL) due to AAA server timeout or improper configuration	**Login failed through Web (SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful login through Telnet authenticated by AAA	**Successful login through Telnet from <userIP> authenticated by AAA server**	Informational	

	server	**<serverIP> (Username: <username>, MAC: <macaddr>)**		
	Login failed through Telnet authenticated by AAA server	**Login failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning	
	Login failed through Telnet due to AAA server timeout or improper configuration	**Login failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful login through SSH authenticated by AAA server	**Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational	
	Login failed through SSH authenticated by AAA server	**Login failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning	
	Login failed through SSH due to AAA server timeout or improper configuration	**Login failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful Enable Admin through Console authenticated by AAA local_enable method	**Successful Enable Admin through Console authenticated by AAA local_enable method (Username: <username>)**	Informational	
	Enable Admin failed through Console authenticated by AAA local_enable method	**Enable Admin failed through Console authenticated by AAA local_enable method (Username: <username>)**	Warning	
	Successful Enable Admin through Web authenticated by AAA local_enable method	**Successful Enable Admin through Web from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Informational	
	Enable Admin failed through Web authenticated by AAA local_enable method	**Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful Enable Admin through Web(SSL) authenticated by AAA local_enable method	**Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Informational	

	Enable Admin failed through Web (SSL) authenticated by AAA local_enable method	**Enable Admin failed through Web (SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful Enable Admin through Telnet authenticated by AAA local_enable method	**Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Informational	
	Enable Admin failed through Telnet authenticated by AAA local_enable method	**Enable Admin failed through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful Enable Admin through SSH authenticated by AAA local_enable method	**Successful Enable Admin through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Informational	
	Enable Admin failed through SSH authenticated by AAA local_enable method	**Enable Admin failed through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful Enable Admin through Console authenticated by AAA none method	**Successful Enable Admin through Console authenticated by AAA none method (Username: <username>)**	Informational	
	Successful Enable Admin through Web authenticated by AAA none method	**Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)**	Informational	
	Successful Enable Admin through Web (SSL) authenticated by AAA none method	**Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)**	Informational	
	Successful Enable Admin through Telnet authenticated by AAA none method	**Successful Enable Admin through Telnet from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)**	Informational	
	Successful Enable Admin through SSH authenticated by AAA none method	**Successful Enable Admin through SSH from <userIP> authenticated by AAA none method (Username:**	Informational	

		<username>, MAC: <macaddr>)		
	Successful Enable Admin through Console authenticated by AAA server	**Successful Enable Admin through Console authenticated by AAA server <serverIP> (Username: <username>)**	Informational	
	Enable Admin failed through Console authenticated by AAA server	**Enable Admin failed through Console authenticated by AAA server <serverIP> (Username: <username>)**	Warning	
	Enable Admin failed through Console due to AAA server timeout or improper configuration	**Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	Successful Enable Admin through Web authenticated by AAA server	**Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational	
	Enable Admin failed through Web authenticated by AAA server	**Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning	
	Enable Admin failed through Web due to AAA server timeout or improper configuration	**Enable Admin failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful Enable Admin through Web (SSL) authenticated by AAA server	**Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational	
	Enable Admin failed through Web (SSL) authenticated by AAA server	**Enable Admin failed through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning	
	Enable Admin failed through Web (SSL) due to AAA server timeout or improper configuration	**Enable Admin failed through Web (SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning	

	Successful Enable Admin through Telnet authenticated by AAA server	**Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational	
	Enable Admin failed through Telnet authenticated by AAA server	**Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning	
	Enable Admin failed through Telnet due to AAA server timeout or improper configuration	**Enable Admin failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning	
	Successful Enable Admin through SSH authenticated by AAA server	**Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational	
	Enable Admin failed through SSH authenticated by AAA server	**Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning	
	Enable Admin failed through SSH due to AAA server timeout or improper configuration	**Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning	
	AAA server timed out	**AAA server <serverIP> (Protocol: <protocol>) connection failed**	Warning	<protocol> is one of TACACS, XTACACS, TACACS+, RADIUS
	AAA server ACK error	**AAA server <serverIP> (Protocol: <protocol>) response is wrong**	Warning	<protocol> is one of TACACS, XTACACS, TACACS+, RADIUS
	AAA does not support this functionality	**AAA doesn't support this functionality**	Informational	
IP-MAC-PORT Binding	Unauthenticated ip address and discard by ip mac port binding	**Unauthenticated IP-MAC address and discarded by ip mac port binding (IP: <ipaddr>, MAC: <macaddr>, Port <unitID:portNum>)**	Warning	
	Unauthenticated IP address encountered and discarded by ip IP-MAC port binding	**Unauthenticated IP-MAC address and discarded by IP-MAC port binding (IP: <ipaddr>, MAC: <macaddr>, Port: <unitID:portNum>)**	Warning	

IP and Password Changed	IP Address change activity	**Unit <unitID>, Management IP address was changed by (Username: <username>,IP:<ipaddr>,MAC :<macaddr>)**	Informational	
	Password change activity	**Unit <unitID>, Password was changed by (Username: <username>,IP:<ipaddr>,MAC :<macaddr>)**	Informational	
Dual Configuration	Excution error encountered druring system boot-up	**Configuration had <int> syntax error and <int> execute error**	Warning	
RIP	RIP enabled	**RIP is enabled**	Informational	
	RIP disabled	**RIP is disabled**	Informational	
OSPF	OSPF enabled	**OSPF is enabled**	Informational	
	OSPF disabled	**OSPF is disabled**	Informational	
VRRP	VRRP enabled	**VRRP is enabled**	Informational	
	VRRP disabled	**VRRP is disabled**	Informational	
	Invalid version packet received	**VRRP receives an invalid version packet**	Warning	
	Invalid virtual ID packet received	**VRRP receives an invalid virtual ID packet**	Warning	
	Invalid checksum packet received	**VRRP receives an invalid checksum packet**	Warning	
	Invalid TTL packet received	**Interface <string>, VRID <id> receives an invalid VRRP TTL packet**	Warning	string is "interface name"
	Invalid length packet received	**Interface <string>, VRID <id> receives an invalid VRRP length packet**	Warning	string is "interface name"
	Different advertisement interval received	**Interface <string>, VRID <id> receives a different VRRP advertisement interval packet**	Warning	string is "interface name"
	Master has shutdown	**Interface <string>, VRID <id> VRRP master has shutdown**	Warning	string is "interface name"
	Authentication fail packet received	**Interface <string>, VRID <id> receives a VRRP authentication fail packet**	Warning	string is "interface name"
	Invalid virtual IP packet received	**Interface <string>, VRID <id> receives an invalid VRRP virtual IP packet**	Warning	string is "interface name"
	Authentication type mismatch packet received	**Interface <string>, VRID <id> receives a VRRP authentication type mismatch packet**	Warning	string is "interface name"
Safeguard Engine	Safeguard Engine is in normal mode	**Safeguard Engine enters NORMAL mode**	Informational	
	Safeguard Engine is in filtering packet mode	**Safeguard Engine enters EXHAUSTED mode**	Warning	

Packet Storm	Broadcast strom occurrence	**Port <unitID:portNum> Broadcast storm is occurring**	Warning	
	Broadcast storm cleared	**Port <unitID:portNum> Broadcast storm has cleared**	Informational	
	Multicast storm occurrence	**Port <unitID:portNum> Multicast storm is occurring**	Warning	
	Multicast storm cleared	**Port <unitID:portNum> Multicast storm has cleared**	Informational	
	Port shut down due to a packet storm	**Port <unitID:portNum> is currently shut down due to a packet storm**	Warning	

Glossary

1000BASE-SX: A short laser wavelength on multimode fiber optic cable for a maximum length of 550 meters

1000BASE-LX: A long wavelength for a "long haul" fiber optic cable for a maximum length of 10 kilometers

100BASE-FX: 100Mbps Ethernet implementation over fiber.

100BASE-TX: 100Mbps Ethernet implementation over Category 5 and Type 1 Twisted Pair cabling.

10BASE-T: The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.

ageing: The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.

ATM: Asynchronous Transfer Mode. A connection oriented transmission protocol based on fixed length cells (packets). ATM is designed to carry a complete range of user traffic, including voice, data and video signals.

auto-negotiation: A feature on a port which allows it to advertise its capabilities for speed, duplex and flow control. When connected to an end station that also supports auto-negotiation, the link can self-detect its optimum operating setup.

backbone port: A port which does not learn device addresses, and which receives all frames with an unknown address. Backbone ports are normally used to connect the Switch to the backbone of your network. Note that backbone ports were formerly known as designated downlink ports.

backbone: The part of a network used as the primary path for transporting traffic between network segments.

bandwidth: Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10Mbps, the bandwidth of Fast Ethernet is 100Mbps.

baud rate: The switching speed of a line. Also known as line speed between network segments.

BOOTP: The BOOTP protocol allows automatic mapping of 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 CSMA/CD network access method.

Flow Control: (IEEE 802.3X) 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 the user 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 the user 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.

Warranties/Registration

LIMITED WARRANTY

D-Link provides this limited warranty for its product only to the person or entity who originally purchased the product from D-Link or its authorized reseller or distributor. D-Link would fulfill the warranty obligation according to the local warranty policy in which you purchased our products.

Limited Hardware Warranty: D-Link warrants that the hardware portion of the D-Link products described below ("Hardware") will be free from material defects in workmanship and materials from the date of original retail purchase of the Hardware, for the period set forth below applicable to the product type ("Warranty Period") if the Hardware is used and serviced in accordance with applicable documentation; provided that a completed Registration Card is returned to an Authorized D-Link Service Office within ninety (90) days after the date of original retail purchase of the Hardware. If a completed Registration Card is not received by an authorized D-Link Service Office within such ninety (90) period, then the Warranty Period shall be ninety (90) days from the date of purchase.

Product Type	***Warranty Period***
Product (including Power Supplies and Fans)	One (1) Year
Spare parts and pare kits	Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. 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 of an identical make, model or part; D-Link may in its discretion may 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. The Warranty Period shall extend for an additional ninety (90) days after any repaired or replaced Hardware is delivered. 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 delivery of the Software for a period of ninety (90) days ("Warranty Period"), if 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. 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. The Warranty Period shall extend for an additional ninety (90) days after any replacement Software is delivered. 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.

What You Must Do For Warranty Service:

Registration Card. The Registration Card provided at the back of this manual must be completed and returned to an Authorized D-Link Service Office for each D-Link product within ninety (90) days after the product is purchased and/or licensed. The addresses/telephone/fax list of the nearest Authorized D-Link Service Office is provided in the back of this manual. FAILURE TO

PROPERLY COMPLETE AND TIMELY RETURN THE REGISTRATION CARD MAY AFFECT THE WARRANTY FOR THIS PRODUCT.

Submitting A Claim. Any claim under this limited warranty must be submitted in writing before the end of the Warranty Period to an Authorized D-Link Service Office. The claim must include 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. The packaged product shall be insured and shipped to Authorized D-Link Service Office with all shipping costs prepaid. 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 that 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;

and Any hardware, software, firmware or other products or services provided by anyone other than D-Link.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND 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, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, 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.

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

Copyright Statement

FCC Warning

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

D-Link®
Building Networks for People

Limited Warranty
(USA Only)

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for 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, or addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link product described below ("Hardware") will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below ("Warranty Period"), except as otherwise stated herein.

- Hardware: For as long as the original customer/end user owns the product, or five (5) 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

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any 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, at its option, 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 or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual 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 ("Software 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 Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, 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 the portion of the actual purchase price paid that is attributable to the Software. 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. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. 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 portions 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, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer.

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: The Limited Warranty provided herein by D-Link does not cover: Products that, 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; and 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. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited 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 THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. 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 you 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 owners.

CE Mark Warning: This is a Class A product. In a residential 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 commercial 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. Operation of this equipment in a residential environment is likely to cause harmful interference to radio or television reception. 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 information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Product Registration:

Register online your D-Link product at http://support.dlink.com/register/

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

D-Link Europe Limited Lifetime Warranty

Dear Customer,

please read below to understand the details of the warranty coverage you have.

Warranty terms for D-LINK xStack products:

All D-Link xStack products* are supplied with a 5 year warranty as standard. To enable the Limited Lifetime Warranty on this product you must register the product, within the first three months of purchase**, on the following website: **http://www.dlink.biz/productregistration/**

D-Link will then provide you with a Limited Lifetime Warranty reference number for this product. Please retain your original dated proof of purchase with a note of the serial number, and Limited Lifetime Warranty reference number together with this warranty statement and place each document in a safe location. When you make a warranty claim on a defective product, you may be asked to provide this information.

Nothing in this Limited Lifetime Warranty affects your statutory rights as a consumer. The following are special terms applicable to your Limited Lifetime hardware warranty.

Warranty beneficiary

The warranty beneficiary is the original end user. The original end user is defined as the person that purchases the product as the first owner.

Duration of Limited Lifetime Warranty

As long as the original end-user continues to own or use the product with the following conditions:

- fan and power supplies are limited to a five (5) year warranty only
- in the event of discontinuance of product manufacture, D-Link warranty support is limited to five (5) years from the announcement of discontinuance. If a product is no longer available for replacement, D-Link will issue a product comparable or better to the one originally purchased.

Replacement, Repair or Refund Procedure for Hardware

D-Link or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of the RMA request. Actual delivery times may vary depending on customer location. D-Link reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive a Return Materials Authorization (RMA) Number, please visit: http://service.dlink.biz and for Italy and Spain, please use: http://rma.dlink.es or http://rma.dlink.it.

D-Link Limited Lifetime Warranty

Hardware: D-Link warrants the D-Link hardware named above against defects in materials and workmanship for the period specified above. If D-Link receives notice of such defects during the warranty period, D-Link will, at its option, either repair or replace products proving to be defective. Replacement products may be either new or like-new.

***Software*.** D-Link warrants that D-Link software will not fail to execute its programming instructions, for the period specified above, due to defects in material and workmanship when properly installed and used. If D-Link receives notice of such defects during the warranty period, D-Link will replace software media that does not execute its programming instructions due to such defects.

Warranty exclusions

This warranty does not apply if the software, product or any other equipment upon which the software is authorized to be used (a) has been altered, except by D-Link or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by D-Link (improper use or improper maintenance), (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; (d) is licensed, for beta, evaluation, testing or demonstration purposes for which D-Link does not charge a purchase price or license fee or (e) defects are caused by force majeure (lightning, floods, war, etc.), soiling, by extraordinary environmental influences or by other circumstances of which D-Link is not responsible.

Disclaimer of warranty

Please note, some countries do not allow the disclaimer of implied terms in contracts with consumers and the disclaimer below may not apply to you.

To the extend allowed by local law, the above warranties are exclusive and no other warranty, condition or other term, whether written or oral, is expressed or implied. D-Link specifically disclaims any implied warranties, conditions and terms of merchantability, satisfactory quality, and fitness for a particular purpose.

To the extent allowed by local law, the remedies in this warranty statement are customer's sole and exclusive remedies. Except as indicated above, in no event will D-Link or its suppliers be liable for loss of data or for indirect, special, incidental, consequential (including lost profit or data), or other damage, whether based in a contract, tort, or otherwise.

To the extent local law mandatorily requires a definition of "Lifetime Warranty" different from that provided here, then the local law definition will supersede and take precedence.

Valid law

The warranty is subject to the valid laws in the country of purchase and is to be interpreted in the warranty terms with the said laws. You may have additional legal rights that are not restricted by this warranty. Nothing in this Limited Lifetime Warranty affects your statutory rights as a consumer.

* DES-6500 series is excluded from the Limited Lifetime Warranty offering and will be supplied with a standard 5 year warranty.

** Failure to register this product within the first three months of purchase [by the first user only] will invalidate the Limited Lifetime Warranty.

Technical Support

Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States and Canada for the duration of the service period, and warranty confirmation service, during the warranty period on this product. U.S. and Canadian customers can contact D-Link technical support through our website, or by phone.

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:

(877) 354-6555

Monday to Friday 8:00am to 5:00pm PST

D-Link Technical Support over the Internet:

http://support.dlink.com

email:support@dlink.com

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:

(877) 354-6560

Monday to Friday 7:30am to 9:00pm EST

D-Link®
Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link websites.

If you require product support, we encourage you to browse our FAQ section on the website before contacting the support line. We have many FAQ's that may provide a quick solution your problem.

For Customers within the United Kingdom & Ireland:

D-Link UK & Ireland Technical Support over the Internet:

http://www.dlink.co.uk

ftp://ftp.dlink.co.uk

D-Link UK & Ireland Technical Support over the Telephone:

08456 12 0003 (United Kingdom)

+1890 886 899 (Ireland)

Lines Open

8.00am-10.00pm Mon-Fri

10.00am-7.00pm Sat & Sun

For Customers within Canada:

D-Link Canada Technical Support over the Telephone:

1-800-361-5265 (Canada)

Mon. to Fri. 7:30AM to 9:00PM EST

D-Link Canada Technical Support over the Internet:

http://support.dlink.ca

email: support@dlink.ca

D-Link®
Building Networks for People

Technische Unterstützung

Aktualisierte Versionen von Software und Benutzerhandbuch finden Sie auf der Website von D-Link.

D-Link bietet kostenfreie technische Unterstützung für Kunden innerhalb Deutschlands, Österreichs, der Schweiz und Osteuropas.

Unsere Kunden können technische Unterstützung über unsere Website, per E-Mail oder telefonisch anfordern.

Web: http://www.dlink.de

E-Mail: support@dlink.de

Telefon: +49 (1805)2787

0,12€/Min aus dem Festnetz der Deutschen Telekom.

Telefonische technische Unterstützung erhalten Sie Montags bis Freitags von 09.00 bis 17.30 Uhr.

Unterstützung erhalten Sie auch bei der Premiumhotline für D-Link Produkte unter der Rufnummer 09001-475767

Montag bis Freitag von 6-22 Uhr und am Wochenende von 11-18 Uhr.

1,75€/Min aus dem Festnetz der Deutschen Telekom.

Wenn Sie Kunde von D-Link außerhalb Deutschlands, Österreichs, der Schweiz und Osteuropas sind, wenden Sie sich bitte an die zuständige Niederlassung aus der Liste im Benutzerhandbuch.

D-Link®
Building Networks for People

Assistance technique

Vous trouverez la documentation et les logiciels les

plus récents sur le site web **D-Link.**

Vous pouvez contacter le service technique de

D-Link par notre site internet ou par téléphone.

Support technique destiné aux clients établis en France:

Assistance technique D-Link par téléphone :

0820 0803 03

N° INDIGO - 0,12€ TTC/min*

*Prix en France Métropolitaine au 3 mars 2005

Du lundi au samedi – de 9h00 à 19h00

Assistance technique D-Link sur internet :

http://www.dlink.fr

e-mail : support@dlink.fr

Support technique destiné aux clients établis au Canada :

Assistance technique D-Link par téléphone :

(800) 361-5265

Lun.-Ven. 7h30 à 21h00 HNE.

Assistance technique D-Link sur internet :

http ://support.dlink.ca

e-mail : support@dlink.ca

D-Link®

Building Networks for People

Asistencia Técnica

Puede encontrar las últimas versiones de software así como documentación técnica en el sitio web de **D-Link**.

D-Link ofrece asistencia técnica gratuita para clientes residentes en España durante el periodo de garantía del producto.

Asistencia Técnica de D-Link por teléfono:

+34 902 30 45 45

Lunes a Viernes de 9:00 a 14:00 y de 15:00 a 18:00

Asistencia Técnica de D-Link a través de Internet:

http://www.dlink.es/support/

e-mail: soporte@dlink.es

D-Link®
Building Networks for People

Supporto tecnico

Gli ultimi aggiornamenti e la documentazione sono disponibili sul sito D-Link.

Supporto tecnico per i clienti residenti in Italia

D-Link Mediterraneo S.r.L.

Via N. Bonnet 6/B 20154 Milano

Supporto Tecnico dal lunedì al venerdì dalle ore 9.00 alle ore 19.00 con orario continuato
Telefono: 02-39607160

URL : http://www.dlink.it/supporto.html

Email: tech@dlink.it

D-Link®
Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within Benelux for the duration of the warranty period on this product.

Benelux customers can contact D-Link technical support through our website, or by phone.

Tech Support for customers within the Netherlands:

D-Link Technical Support over the Telephone:

0900 501 2007

Monday to Friday 9:00 am to 10:00 pm

D-Link Technical Support over the Internet:

www.dlink.nl

Tech Support for customers within Belgium:

D-Link Technical Support over the Telephone:

070 66 06 40

Monday to Friday 9:00 am to 10:00 pm

D-Link Technical Support over the Internet:

www.dlink.be

Tech Support for customers within Luxemburg:

D-Link Technical Support over the Telephone:

+32 70 66 06 40

Monday to Friday 9:00 am to 10:00 pm

D-Link Technical Support over the Internet:

www.dlink.be

D-Link®
Building Networks for People

Pomoc techniczna

Najnowsze wersje oprogramowania i dokumentacji użytkownika można znaleźć w serwisie internetowym firmy D-Link.

D-Link zapewnia bezpłatną pomoc techniczną klientom w Polsce w okresie gwarancyjnym produktu.

Klienci z Polski mogą się kontaktować z działem pomocy technicznej firmy D-Link za pośrednictwem Internetu lub telefonicznie.

Telefoniczna pomoc techniczna firmy D-Link:

(+48 12) 25-44-000

D-Link®
Building Networks for People

Technická podpora

Aktualizované verze software a uživatelských příruček najdete na webové stránce firmy D-Link.

D-Link poskytuje svým zákazníkům bezplatnou technickou podporu

Zákazníci mohou kontaktovat oddělení technické podpory přes webové stránky, mailem nebo telefonicky

Web: http://www.dlink.cz/suppport/

E-mail: support@dlink.cz

Telefon: 224 247 503

D-Link®
Building Networks for People

Technikai Támogatás

Meghajtó programokat és frissítéseket a **D-Link** Magyarország weblapjáról tölthet le.
Telefonon technikai segítséget munkanapokon hétfőtől-csütörtökig 9.00 – 16.00 óráig és pénteken 9.00 – 14.00 óráig kérhet a **(1) 461-3001** telefonszámon vagy a **support@dlink.hu** emailcímen.

Magyarországi technikai támogatás :

D-Link Magyarország

1074 Budapest, Alsóerdősor u. 6. – R70 Irodaház 1 em.

Tel. : 06 1 461-3001

Fax : 06 1 461-3004

email : support@dlink.hu

URL : http://www.dlink.hu

D-Link®
Building Networks for People

Teknisk Support

Du kan finne programvare oppdateringer og bruker dokumentasjon på D-Links web sider.

D-Link tilbyr sine kunder gratis teknisk support under produktets garantitid.

Kunder kan kontakte D-Links teknisk support via våre hjemmesider, eller på tlf.

Teknisk Support:

D-Link Teknisk telefon Support:

800 10 610

(Hverdager 08:00-20:00)

D-Link Teknisk Support over Internett:

http://www.dlink.no

D-Link®

Building Networks for People

Teknisk Support

Du finder software opdateringer og bruger-dokumentation på D-Link's hjemmeside.

D-Link tilbyder gratis teknisk support til kunder i Danmark i hele produktets garantiperiode.

Danske kunder kan kontakte D-Link's tekniske support via vores hjemmeside eller telefonisk.

D-Link teknisk support over telefonen:

Tlf. 7026 9040

Hverdager: kl. 08:00 – 20:00

D-Link teknisk support på Internettet:

http://www.dlink.dk

D-Link®

Building Networks for People

Teknistä tukea asiakkaille Suomessa:

D-Link tarjoaa teknistä tukea asiakkailleen.

Tuotteen takuun voimassaoloajan.

Tekninen tuki palvelee seuraavasti:

Arkisin klo. 9 - 21
numerosta
0800-114 677

Internetin kautta
Ajurit ja lisätietoja tuotteista.
http://www.dlink.fi

Sähköpostin kautta
voit myös tehdä kyselyitä.

D-Link®
Building Networks for People

Teknisk Support

På vår hemsida kan du hitta mer information om mjukvaru uppdateringar och annan användarinformation.

D-Link tillhandahåller teknisk support till kunder i Sverige under hela garantitiden för denna produkt.

Teknisk Support för kunder i Sverige:

D-Link Teknisk Support via telefon:

0770-33 00 35

Vardagar 08.00-20.00

D-Link Teknisk Support via Internet:

http://www.dlink.se

D-Link®
Building Networks for People

Suporte Técnico

Você pode encontrar atualizações de software e documentação de utilizador no site de D-Link Portugal http://www.dlink.pt.

A D-Link fornece suporte técnico gratuito para clientes no Portugal durante o período de vigência de garantia deste produto.

Suporte Técnico para clientes no Portugal:

Assistência Técnica:

Email: soporte@dlink.es

http://www.dlink.pt/support/

ftp://ftp.dlink.es

D-Link®
Building Networks for People

Τεχνική Υποστήριξη

Μπορείτε να βρείτε software updates και πληροφορίες για τη χρήση των προϊόντων στις ιστοσελίδες της D-Link

Η D-Link προσφέρει στους πελάτες της δωρεάν υποστήριξη

στον Ελλαδικό χώρο

Μπορείτε να επικοινωνείτε με το τμήμα τεχνικής υποστήριξης μέσω της ιστοσελίδας ή μέσω τηλεφώνου

Για πελάτες εντός του Ελλαδικού χώρου:

Τηλεφωνική υποστήριξη D-Link :

Τηλ: 210 86 11 114
Φαξ: 210 86 53 172

(Δευτέρα-Παρασκευή 09:00-17:00)

e-mail: support@dlink.gr

Τεχνική υποστήριξη D-Link μέσω Internet:

D-Link®
Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers in

Australia:

Tel: 1300-766-868

Monday to Friday 8:00am to 8:00pm EST

Saturday 9:00am to 1:00pm EST

http://www.dlink.com.au

e-mail: support@dlink.com.au

India:

Tel: 1800-222-002

Monday to Friday 9:30AM to 7:00PM

http://www.dlink.co.in/support/productsupport.aspx

Indonesia, Malaysia, Singapore and Thailand:

Tel: +62-21-3851275 (Indonesia)

Tel: 1800-882-880 (Malaysia)

Tel: +65 66229355 (Singapore)

Tel: +66-2-719-8978/9 (Thailand)

Monday to Friday 9:00am to 6:00pm

http://www.dlink.com.sg/support/

e-mail: support@dlink.com.sg

Korea:

Tel: +82-2-890-5496

D-Link®

Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers in

Egypt:

Tel: +202-2919035 or +202-2919047

Sunday to Thursday 9:00am to 5:00pm

http://support.dlink-me.com

e-mail: amostafa@dlink-me.com

Iran:

Tel: +98-21-88822613

Sunday to Thursday 9:00am to 6:00pm

http://support.dlink-me.com

e-mail: support.ir@dlink-me.com

Israel:

Tel: +972-9-9715701

Sunday to Thursday 9:00am to 5:00pm

http://www.dlink.co.il/support/

e-mail: support@dlink.co.il

Pakistan:

Tel: +92-21-4548158 or +92-21-4548310

Sunday to Thursday 9:00am to 6:00pm

http://support.dlink-me.com

e-mail: support.pk@dlink-me.com

South Africa and Sub Sahara Region:

Tel: +27-12-665-2165

08600 DLINK (for South Africa only)

Monday to Friday 8:30am to 9:00pm South Africa Time

http://www.d-link.co.za

Turkey:

Tel: +90-212-2895659

Monday to Friday 9:00am to 6:00pm

http://www.dlink.com.tr

e-mail: turkiye@dlink-me.com

e-mail: support@d-link.co.za

U.A.E and North Africa:

Tel: +971-4-391-6480 (U.A.E)

Sunday to Wednesday 9:00am to 6:00pm GMT+4

Thursday 9:00am to 1:00pm GMT+4

D-Link®

Building Networks for People

Техническая поддержка

Обновления программного обеспечения и документация доступны на Интернет-сайте D-Link.

D-Link предоставляет бесплатную поддержку для клиентов в течение гарантийного срока.

Клиенты могут обратиться в группу технической поддержки D-Link по телефону или через Интернет.

Техническая поддержка D-Link:
+495-744-00-99

Техническая поддержка через Интернет
http://www.dlink.ru
e-mail: support@dlink.ru

D-Link®
Building Networks for People

Asistencia Técnica

D-Link Latin América pone a disposición de sus clientes, especificaciones, documentación y software mas reciente a través de nuestro Sitio Web
www.dlinkla.com

El servicio de soporte técnico tiene presencia en numerosos países de la Región Latino América, y presta asistencia gratuita a todos los clientes de D-Link, en forma telefónica e internet, a través de la casilla
soporte@dlinkla.com

Soporte Técnico Help Desk Argentina:

TTeléfono: 0800-12235465 Lunes a Viernes 09:00 am a 22:00 pm

Soporte Técnico Help Desk Chile:

Teléfono: 800 8 35465 Lunes a Viernes 08:00 am a 21:00 pm

Soporte Técnico Help Desk Colombia:

Teléfono: 01800-9525465 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk Ecuador:

Teléfono: 1800-035465 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk El Salvador:

Teléfono: 800-6335 Lunes a Viernes 06:00 am a 19:00 pm

Soporte Técnico Help Desk Guatemala:

Teléfono: 1800-8350255 Lunes a Viernes 06:00 am a 19:00 pm

Soporte Técnico Help Desk Panamá:

Teléfono: 00800 0525465 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk Costa Rica:

Teléfono: 0800 0521478 Lunes a Viernes 06:00 am a 19:00 pm

Soporte Técnico Help Desk Perú:

Teléfono: 0800-00968 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk República Dominicana:

Teléfono: 1888 7515478 Lunes a Viernes 06:00 am a 19:00 pm

Soporte Técnico Help Desk Venezuela:

D-Link®
Building Networks for People

Suporte Técnico

Você pode encontrar atualizações de software e documentação de usuário no site da D-Link Brasil www.dlinkbrasil.com.br.

A D-Link fornece suporte técnico gratuito para clientes no Brasil durante o período de vigência da garantia deste produto.

Suporte Técnico para clientes no Brasil:

Telefone

São Paulo +11-2185-9301

Segunda à sexta

Das 8h30 às 18h30

Demais Regiões do Brasil 0800 70 24 104

D-Link®
Building Networks for People

D-Link 友訊科技 台灣分公司

技術支援資訊

如果您還有任何本使用手冊無法協助您解決的產品相關問題，台灣地區用戶可以透過我們的網站、電子郵件或電話等方式與D-Link台灣地區技術支援工程師聯絡。

D-Link 免付費技術諮詢專線

0800-002-615

服務時間：週一至週五，早上8:30 到 晚上7:00

(不含周六、日及國定假日)

網　　站：http://www.dlink.com.tw

電子郵件：dssqa_service@dlink.com.tw

如果您是台灣地區以外的用戶，請參考D-Link網站 全球各地分公司的聯絡資訊以取得相關支援服務。

產品保固期限、台灣區維修據點查詢，請參考以下網頁說明：

http://www.dlink.com.tw

產品維修：

使用者可直接送至全省聯強直營維修站或請洽您的原購買經銷商。

D-Link®
Building Networks for People

Dukungan Teknis

Update perangkat lunak dan dokumentasi pengguna dapat diperoleh pada situs web D-Link.

Dukungan Teknis untuk pelanggan:

Dukungan Teknis D-Link melalui telepon:

Tel: +62-21-3851275

Senin sampai Jumat 9:00 - 12:30, 14:00 - 18:00

Waktu Singapura

Dukungan Teknis D-Link melalui Internet:

e-mail: support@dlink.com.sg

D-Link®

Building Networks for People

技术支持

办公地址：北京市朝阳区建国路 71 号惠通时代广场 C1 座 202 室 邮编: 100025

技术支持中心电话：8008296688/(028) 66052968

技术支持中心传真：(028)85176948

维修中心地址：北京市朝阳区建国路 71 号惠通时代广场 C1 座 202 室
邮编: 100025

维修中心电话：(010) 58635800

维修中心传真：(010) 58635799

网址：http://www.dlink.com.cn

办公时间：周一到周五，早09:00到晚18:00

D-Link®
Building Networks for People

International Offices

U.S.A
17595 Mt. Herrmann Street
Fountain Valley, CA 92708
TEL: 1-800-326-1688
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.)
D-Link (Europe) Ltd
D-Link House, Abbey Road
Park Royal, London NW10 7BX
United Kingdom
TEL: +44 (0)20 8955 9000
FAX: +44 (0)20 8955 9001
URL: www.dlink.co.uk

Austria
Millennium Tower
Handelskai 94-96
A-1200 WIEN,
Austria
TEL: +43 (0)1 240 27 270
FAX: +43 (0)1 240 27 271
URL: www.dlink.at

Belgium
Rue des Colonies 11
B-1000 Brussels,
Belgium
TEL: +32 (0)2 517 7111
FAX: +32 (0)2 517 6500
URL: www.dlink.be

Bulgaria
60A Bulgaria Blvd., Office 1,
Sofia 1680,
Bulgaria
TEL: +359 2 958 22 42
FAX: +359 2 958 65 57
URL: www.dlink.eu

Czech Republic
Vaclavske namesti 36
110 00 Praha 1
Czech Republic
TEL: +420 224 247 500
FAX: +420 224 234 967
Hot line CZ: +420 225 281 553
Hot line SK: +421 263 813 628
URL: www.dlink.cz
URL: www.dlink.sk

Denmark
Naverland 2,
DK-2600 Glostrup, Copenhagen,
Denmark
TEL: +45 43 96 9 040
FAX: +45 43 42 43 47
URL: www.dlink.dk

Finland
Latokartanontie 7A
FIN-00700 Helsinki,
Finland
TEL : +358 10 309 8840
FAX: + 358 10 309 8841
URL: www.dlink.fi

France
41 boulevard Vauban
78280 Guyancourt
France
TEL: +33 (0)1 30 23 86 88
FAX: +33 (0)1 30 23 86 89
URL: www.dlink.fr

Germany
Schwalbacher Strasse 74
D-65760 Eschborn,
Germany
TEL: +49 (0)6196 77 99 0
FAX: +49 (0)6196 77 99 300
URL: www.dlink.de

Greece
101, Panagoulis Str. 163-43
Heliopolis, Athens,
Greece
TEL: +30 210 9914512
FAX:+30 210 9916902
URL: www.dlink.gr

Hungary
Rákóczi út 70-72
HU-1074 Budapest,
Hungary
TEL: +36 (0) 1 461 30 00
FAX: +36 (0) 1 461 30 04
URL: www.dlink.hu

Italy
Via Nino Bonnet n. 6/b
20154 – Milano,
Italy
TEL: +39 02 2900 0676
FAX: +39 02 2900 1723
URL: www.dlink.it

Luxembourg
Rue des Colonies 11
B-1000 Brussels,
Belgium
TEL: +32 (0)2 517 7111
FAX: +32 (0)2 517 6500
URL: www.dlink.be

Netherlands
Weena 290
3012NJ Rotterdam,
Netherlands
TEL: +31 (0)10 282 1445
FAX: +31 (0)10 282 1331
URL: www.dlink.nl

Norway
Karihaugveien 89
N-1086 Oslo,
Norway
TEL: +47 99 300 100
FAX: +47 22 30 90 85
URL: www.dlink.no

Poland
Budynek Aurum
ul. Waliców 11
00-851 Warszawa,
Poland
TEL: +48 (0) 22 583 92 75
FAX: +48 (0) 22 583 92 76
URL: www.dlink.pl

Portugal
Rua Fernando Palha, 50 Edificio Simol
1900 Lisbon,
Portugal
TEL: +351 21 8688493
FAX: +351 21 8622492
URL: www.dlink.es

Romania
B-dul Unirii nr. 55, bl. E4A, sc.2, et. 4, ap. 39,
sector 3, Bucuresti,
Romania
TEL: +40(0)21 320 23 05
FAX: +40(0)21 320 23 07
URL: www.dlink.eu

Spain
Avenida Diagonal, 593-95, 9th floor
08014 Barcelona,
Spain
TEL: +34 93 409 07 70
FAX: +34 93 491 07 95
URL: www.dlink.es

Sweden
Gustavslundsvägen 151B
S-167 51 Bromma
Sweden
TEL: +46 (0)8 564 619 00
FAX: +46 (0)8 564 619 01
URL: www.dlink.se

Switzerland
Glatt Tower, 2.OG
Postfach
CH-8301 Glattzentrum
Switzerland
TEL: +41 (0)1 832 11 00
FAX: +41 (0)1 832 11 01
URL: www.dlink.ch

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, Plot No.5,
Kurla-Bandra Complex Road, Off.
CST Road,
Santacruz (E), Mumbai - 400 098
India
TEL: 91-22-26526696/ 30616666
FAX: 91-22-26528914/ 8476
URL: www.dlink.co.in

Middle East (Dubai)
P.O.Box: 500376
Office: 103, Building:3
Dubai Internet City
Dubai, United Arab Emirates
TEL: +971-4-3916480
FAX: +971-4-3908881
URL: www.dlink-me.com

Turkey
Cayazaya Maslak Yolu
S/A Kat: 5,
Istanbul, Turkey
TEL: 0212-289-5659
FAX:0212-289-7606
URL: www.dlink.com.tr

Iran
Unit 6, No. 39, 6th Alley,
Sanaei St. Karimkhan Ave
Tehran-IRAN
TEL: 9821 8882 2613
FAX: 9821 8883 5492

Pakistan
Office#311, Business Avenue
Main Shahrah-e-Faisal
Karachi-Pakistan
TEL: 92-21-4548158, 4548310
FAX: 92-21-4535103

Egypt
47,El Merghany street, Heliopolis
Cairo-Egypt
TEL: +202-2919035, +202-2919047
FAX: +202-2919051
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
Av. Vitacura # 2939, floor 6th
Las Condes, Santiago
RM Chile
TEL: 56-2-5838-960
FAX: 56-2-5838-952
URL: www.dlinkla.com

Brazil
Av das Nacoes Unidas
11857 – 14- andar - cj 141/142
Brooklin Novo
Sao Paulo - SP - Brazil
CEP 04578-000 (Zip Code)
TEL: (55 11) 21859300
FAX: (55 11) 21859322
URL: www.dlinkbrasil.com.br

South Africa
Einstein Park II
Block B
102-106 Witch-Hazel Avenue
First Floor Block B
Einstein Park II
Highveld Techno Park
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: 7-495-744-0099
FAX: 7-495-744-0099 #350
URL: www.dlink.ru

Japan K.K.
Level 6 Konan YK Building, Konan
2-4-12
Minato-Ku Tokyo 108-0075, Japan
URL: www.dlink-jp.com

China
No.202, C1 Building, Huitong Office Park, No. 71, Jianguo Road,
Chaoyang District, Beijing
100025, China
TEL +86-10-58635800
FAX: +86-10-58635799
URL: www.dlink.com.cn

Taiwan
No. 289, Sinhu 3rd Rd.,
Neihu District,
Taipei City 114,Taiwan
TEL: 886-2-6600-0123
FAX: 886-2-6600-1188
URL: www.dlink.com.tw

Registration Card

All Countries and Regions Excluding USA

Print, type or use block letters.

Your name: Mr./Ms _____
Organization: _____ Dept. _____
Your title at organization: _____
Telephone: _____ Fax:_____
Organization's e-mail address: _____
Organization's full address: _____
_____
Country: _____
Date of purchase (Month/Day/Year): _____

Product Model	Product Serial No.	* Product installed in type of computer	* Product installed in computer serial No.

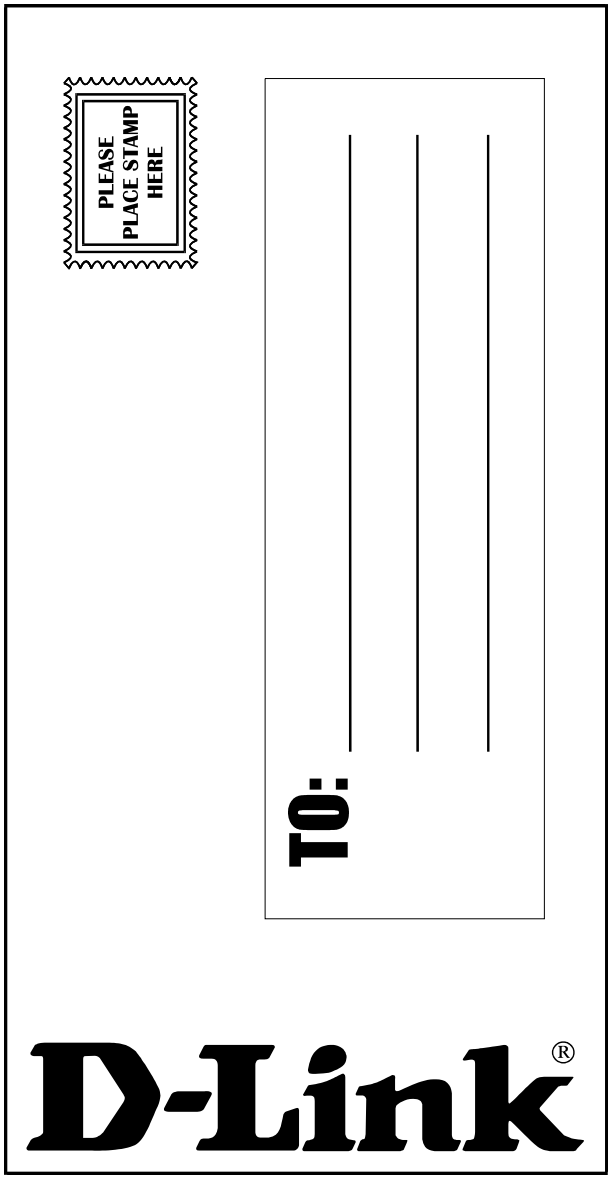
(* Applies to adapters only)

Product was purchased from:

Reseller's name: _____
Telephone: _____

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 ☐Cisco Network
☐Banyan Vines ☐Mac OSX ☐Windows NT ☐Windows 98 ☐Windows 2000/ME ☐Windows XP ☐Windows Vista
☐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 ☐1000BASE-T ☐Wireless 802.11b and 802.11g ☐wireless 802.11a ☐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/Chain store/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?
_____
_____


PLEASE
PLACE STAMP
HERE
TO:
D-Link®