D-Link®

DES-3010F/DES-3010FL/DES-3010G/DES-3016/DES-3018/DES-3026
Managed 8/16/24-port 10/100Mbps N-Way Fast Ethernet Switch

Release 4.2

Manual

Table of Contents

Preface

The DES-3010F/DES-3010FL/DES-3010G/DES-3016/DES-3018/DES-3026 User Manual is divided into sections that describe the system installation and operating instructions with examples.

Section 1, Introduction - Describes the Switch and its features.

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

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

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

Section 5, Introduction to Web-based Switch Management – This section discusses connecting to and using the Web-based switch management feature on the Switch.

Section 6, Administration- A detailed discussion about configuring some of the basic functions of the Switch, including accessing the Switch information, using the Switch's utilities and setting up network configurations, such as assigning an IP address, Port Configurations, User Accounts, Password Encryption, Cable Diagnostics, Port Mirroring, System Log Settings, SNTP Settings, MAC Notification Settings, TFTP Services, Ping Test, SNMP Manager, IP-MAC Binding, Single IP Setting, Forwarding & Filtering, SMTP Service and DHCP/BOOTP Relay.

Section 7, L2 Features - A discussion of the layer 2 features of the Switch, including Static VLAN Entry, VLAN Trunk Settings, Trunking, IGMP Snooping, Spanning Tree and Loopback Detection.

Section 8, CoS - A detailed discussion regarding Port Bandwidth, 802.1p Default Priority, 802.1p User Priority, CoS Scheduling Mechanism, CoS Output Scheduling, Priority Settings, TOS Priority Settings, DSCP Priority Settings, Port Mapping Priority Settings and MAC Priority.

Section 9, CPU Interface Filtering – This section deals with the CPU Interface Filtering features on this Switch, including CPU Interface Filtering State and CPU Interface Filtering Table.

Section 10, **Security –** A detailed discussion about the security features on the Switch including Traffic Control, Port Security, Port Lock Entries, 802.1X, Trusted Host, Traffic Segmentation and SSH.

Section 11, Monitoring - Features graphs and screens used in monitoring features and packets on the Switch including CPU Utilization, Port Utilization, Packers, Packet Errors, Packet Size, VLAN Status, MAC Address, Switch Log, Log Settings, IGMP Snooping Group, Browse Router Port, Browse ARP Table and Session Table.

Appendix A, Technical Specifications – This discusses the technical specifications of the DES 3016, DES-3010F, DES-3010FL, DES-3010G, DES-3018 and DES-3026 switches.

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

Appendix C, Cable Lengths – Gives information on cable types and maximum distances.

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

Intended Readers

The ***DES-3010F/DES-3010FL/DES-3010G/DES-3016/DES-3018/DES-3026   User 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 your screen. For example: You have mail. Bold font is also used to represent filenames, program names and commands. For example: use the copy command.
`Boldface Typewriter Font`	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
Italics	Indicates a window name or a field. Also can indicate a variables or parameter that is replaced with an appropriate word or string. For example: type *filename* means that you should type the actual filename instead of the word shown in italic.
Menu Name > Menu Option	**Menu Name > Menu Option** Indicates the menu structure. **Device > Port > Port Properties** means the Port Properties menu option under the Port menu option that is located under the Device menu.

Notes, Notices, and Cautions

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

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

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

Safety Instructions

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

⚠ Safety Cautions

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

- Observe and follow service markings.

  - Do not service any product except as explained in your system documentation.

  - Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock.

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

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

  - The power cable, extension cable, or plug is damaged.

  - An object has fallen into the product.

  - The product has been exposed to water.

  - The product has been dropped or damaged.

  - The product does not operate correctly when you follow the operating instructions.

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

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

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

- Use the product only with approved equipment.

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

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

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

  - 115 volts (V)/60 hertz (Hz) in most of North and South America and some Far Eastern countries such as South Korea and Taiwan

  - 100 V/50 Hz in eastern Japan and 100 V/60 Hz in western Japan

  - 230 V/50 Hz in most of Europe, the Middle East, and the Far East

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

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

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

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

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

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

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

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

  - Install the power supply before connecting the power cable to the power supply.

  - Unplug the power cable before removing the power supply.

  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.

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

 General Precautions for Rack-Mountable Products

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

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

 CAUTION: Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack. After installing system/components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.

- Always load the rack from the bottom up, and load the heaviest item in the rack first.

- Make sure that the rack is level and stable before extending a component from the rack.

- Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.

- After a component is inserted into the rack, carefully extend the rail into a locking position, and then slide the component into the rack.

- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.

- Ensure that proper airflow is provided to components in the rack.

- Do not step on or stand on any component when servicing other components in a rack.

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

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

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

Protecting Against Electrostatic Discharge

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

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

1. When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
2. When transporting a sensitive component, first place it in an antistatic container or packaging.
3. Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads and an antistatic grounding strap.

$$\boxed{\textbf{Section 1}}$$

Introduction

Ethernet Technology

Switch Description

Features

Ports

Front-Panel Components

Side Panel Description

Rear Panel Description

Gigabit Combo Ports

Ethernet Technology

Fast Ethernet Technology

The following manual describes the installation, maintenance and configurations concerning members of the DES-3010F/DES-3010FL/DES-3010G/DES-3016/DES-3018/DES-3026 Switch group. These switches are identical in configurations and very similar in basic hardware and consequentially, most of the information in this manual will be universal to the total group of Switches. 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. For the remainder of this document, we will refer primarily to the DES-3026 as the switch in question for examples, configurations and explanations.

Switch Description

The DES-3010F/DES-3010FL/DES-3010G/DES-3016/DES-3018/DES-3026 is a high performance 8/16/24-port Fast Ethernet switch. Comprising 10/100Mbps switched unshielded twisted-pair (UTP) and Auto MDI-X/MDI-II convertible ports, and each model having its own uplink port capability, this Switch will be ideal for segmenting networks into smaller, sub-connected networks for optimum throughput capability of the most demanding multimedia and imaging applications available on the network without creating bottlenecks. These ports can also be used for connecting PCs, printers, servers, hubs, routers, switches and other networking devices, each supporting up to 200 Mbps of throughput in full-duplex mode.

The open slots available on the DES-3018/DES-3026 models, the gigabit port on the DES-3010G and the fiber-optic port on the DES-3010F and DES-3010FL can provide an uplink to a server or network backbone. The built-in console interface can be used to configure the Switch's settings for priority queuing, VLANs, and port trunk groups, port monitoring, and port speed.

Features

- IEEE 802.3z compliant

- IEEE 802.3x Flow Control in full-duplex compliant

- IEEE 802.3u compliant

- IEEE 802.3ab compliant

- 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 and IEEE 802.1w Rapid Spanning Tree

- Single IP Management support
- Simple Network Time Protocol support
- System and Port Utilization support
- System Log Support
- Non-blocking store and forward switching scheme capability to support rate adaptation and protocol conversion
- Supports by-port Egress/Ingress rate control
- Address table: Supports up to 8K MAC addresses per device
- Port Trunking with flexible load distribution and fail-over function
- IGMP Snooping support
- SNMP support
- SMTP support
- CPU Interface Filtering
- Port Mirroring support
- MIB support for:
- RFC1213 MIB II
- RFC1493 Bridge
- RFC1757 RMON
- RFC1643 Ether-like MIB
- RFC2233 Interface MIB
- RFC2358 Ether-like 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.

Ethernet Technology

Fast Ethernet

The growing importance of LANs and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies are proposed to provide greater bandwidth and improve client/server response times. Among them, Fast Ethernet, or 100BASE-T, provides a non-disruptive, smooth evolution from 10BASE-T technology.
100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Ethernet protocol.

Gigabit Ethernet Technology

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

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

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

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

Switching Technology

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

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

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

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

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

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

Front-Panel Components and LED Indicators

The front panel of the Switch consists of LED indicators for Power, Console, Link/Act and Speed, 8/16/24 Fast-Ethernet ports (DES-3010F, DES-3010FL, DES-3010G, DES-3016, DES-3018, DES-3026), two optional module ports (DES-3018/3026 only), a gigabit 1000BASE-T copper port (DES-3010F/FL/G), a 100BASE-FX Ethernet port (DES-3010F, DES-3010FL only) and a SFP Gigabit Ethernet port (DES-3010G). Also, the front panel has a RS-232 communication port.
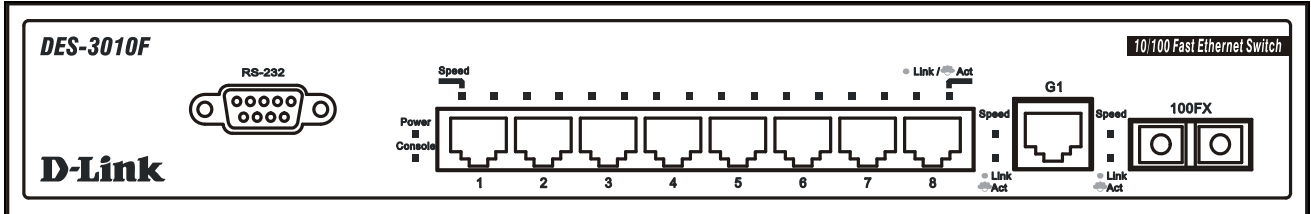
Figure 1- 1. DES-3010F Front Panel
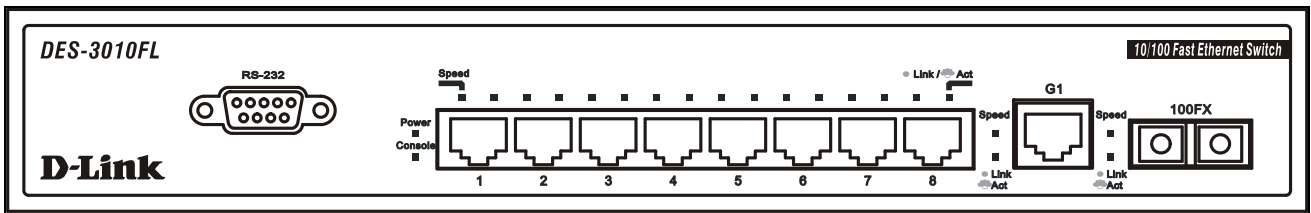
Figure 1- 2. DES-3010FL Front Panel
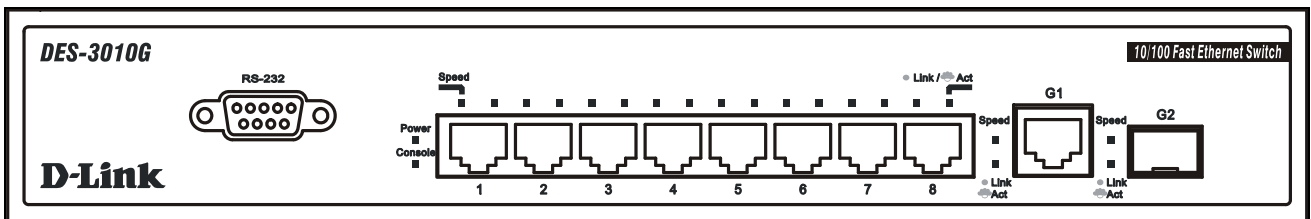
Figure 1- 3. DES-3010G Front Panel
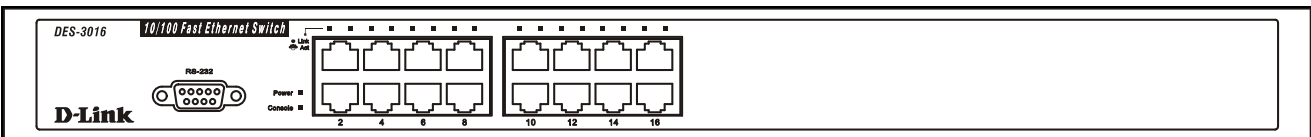
Figure 1- 4. DES-3016 Front Panel
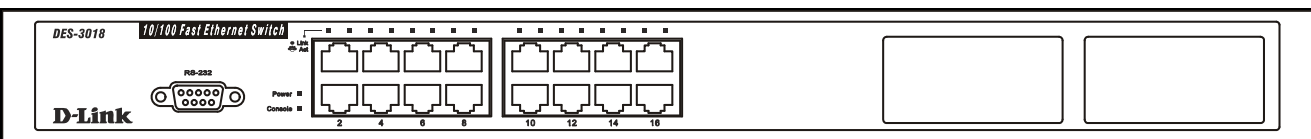
Figure 1- 5. DES-3018 Front Panel
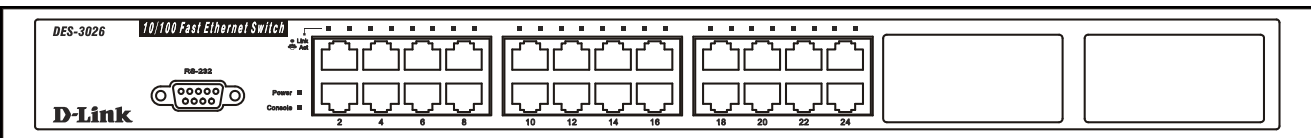
Figure 1- 6. DES-3026 Front Panel
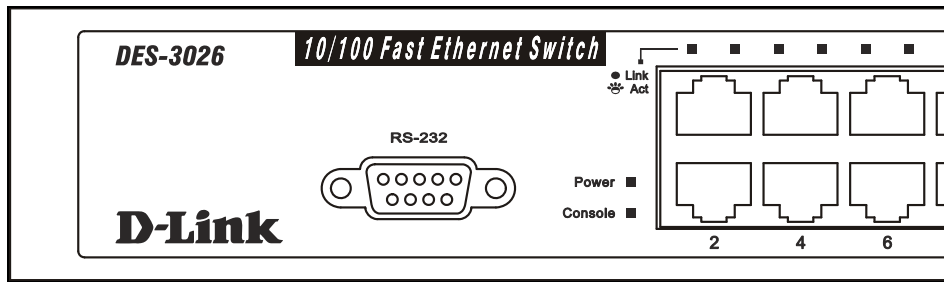
Figure 1- 7. DES-3026 LED indicators

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

LED or Button	Description
Power	This LED will light green after the Switch is powered on to indicate the normal operation of the Switch's power supplies. The indicator is dark when the Switch is powered off.
Console	This LED should blink during the Power-On Self Test (POST). When the POST is finished successfully, the LED goes dark. This indicator will light solid green when the Switch is being logged into via out-of-band/local console management through the RS-232 console port in the front of the Switch using a straight-through serial cable.
Link/Act	When the LED mode has been changed to Link/Act, the LEDs will light steady green to indicate a valid link. A blinking LED indicates activity on the port.
Speed	To the right of every Link/Act LED lies the speed LED, corresponding to every port. Depending on the switch model, these lights will assume different roles. DES-3010F/FL/G – A solid green LED indicates the port is transferring data at 100Mbps while a dark, unlit LED will indicate a rate of 10Mbps. Port 9 – The LED of this port, when lit solid green, indicates a transfer rate of 1000Mbps. When this LED is unlit, it denotes a transfer rate of 10/100Mbps. Port 10 – For the 3010F and 3010FL, a solid green LED indicates a transfer rate of 100Mbps and a dark LED indicates no link. For the 3010G, solid green LED indicates a transfer rate of 1000Mbps and a dark LED indicates no link DES-3018 / DES-3016 / DES-3026 – A solid green LED will indicate a valid link at 100Mbps, and when blinking, indicates the port is currently transferring data. A solid amber LED will indicate a valid link at 10Mbps, and when blinking, indicates the port is currently transferring data.

Rear Panel Description

The rear panels of these switches contain an AC power connector.

Figure 1- 8. Rear Panel of the DES-3010F/DES-3010FL/DES-3010G
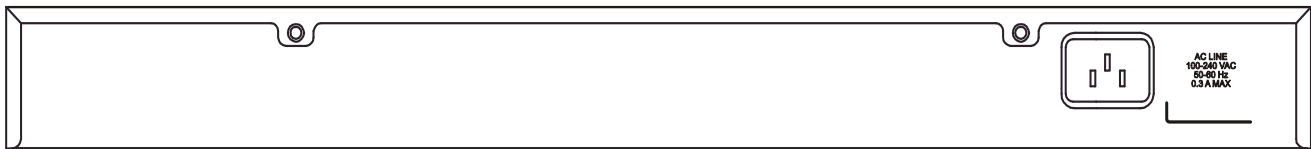
Figure 1- 9. Rear Panel of the DES-3016/DES-3018/DES-3026

Side Panel Description

Both panels of the Switch contain a heat vent used to dissipate heat. Do not block these openings, and leave at least 6 inches of space at the rear and sides of the Switch for proper ventilation. Be reminded that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.

Figure 1- 10. Side panel view

<div style="border:1px solid black; display:inline-block; padding:8px 40px;">

SECTION 2

</div>

Installation

> ***Package Contents***
>
> ***Before You Connect to the Network***
>
> ***Installing the Switch without the Rack***
>
> ***Rack Installation***
>
> ***Power On***
>
> ***The Optional Module***
>
> ***Redundant Power System***

Package Contents

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

- One DES-3010F, DES-3010FL, DES-3010G, DES-3016, DES-3018, or DES-3026 Fast Ethernet Switch
- Mounting kit (two brackets and screws)
- Four rubber feet with adhesive backing
- One AC power cord
- RS-232 console cable
- One CD Kit for User's Guide / CLI / D-View module / SNMP module
- This Manual with Registration Card.

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

Before You Connect to the Network

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

- Install the Switch on a sturdy, level surface that can support the weight of the Switch. Do not place heavy objects on the Switch.
- The power outlet should be within 1.82 meters (6 feet) of the Switch.
- Visually inspect the power cord and see that it is fully secured to the AC power port.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch. Leave at least 10 cm (4 inches) of space at the front and rear of the Switch for ventilation.
- Install the Switch in a fairly cool and dry place for the acceptable temperature and humidity operating ranges.
- Install the Switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.
- When installing the Switch on a level surface, attach the rubber feet to the bottom of the device. The rubber feet cushion the Switch, protect the casing from scratches and prevent it from scratching other surfaces.

Installing the Switch without the Rack

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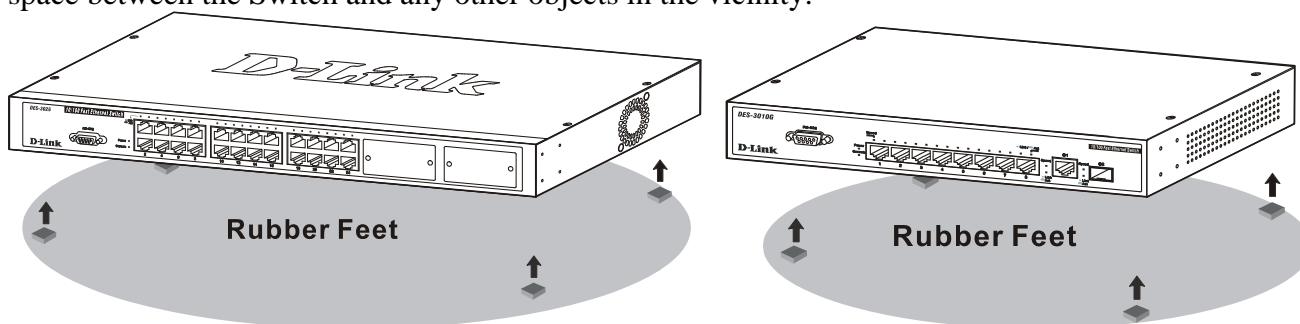
Figure 2- 1. Prepare Switch for installation on a desktop or shelf

Installing the Switch in a Rack

The Switch can be mounted in a standard 19" rack. Use the following diagrams to guide you.
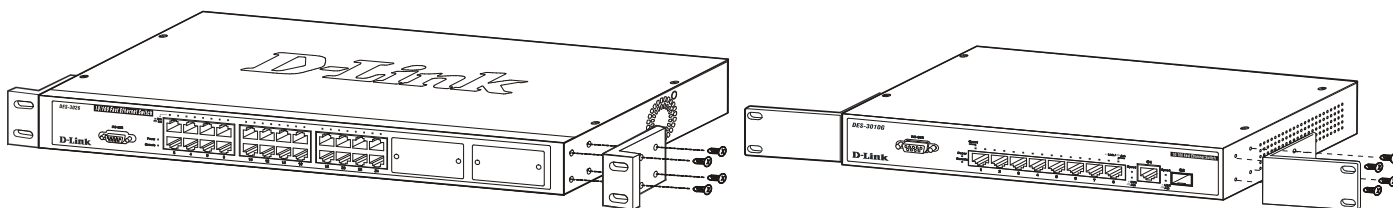
Figure 2- 2. Fasten mounting brackets to Switch

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

Mounting the Switch in a Standard 19" Rack
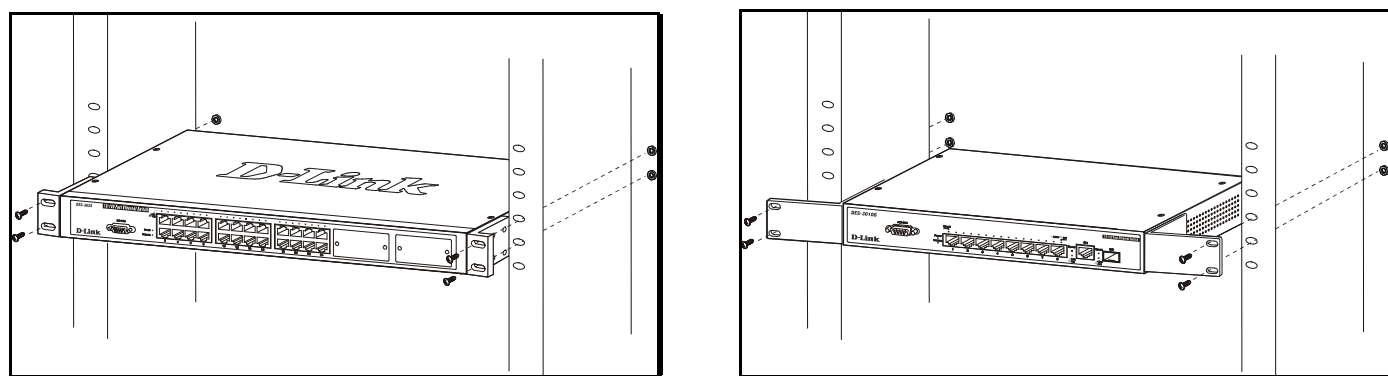
Figure 2- 3. Installing Switch in a rack

Power On

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

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

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

The Optional Modules

At the front right of the DES-3018 and the DES-3026 resides an optional module slot. These optional modules, specially designed for this Switch series, may be used as an uplink to a server or core switch. This slot may be equipped with a single-port Uplink Module, sold separately. See the explanation of the optional modules below.

- Single-Port 1000BASE-T Gigabit-Ethernet uplink module
- Compliant with IEEE802.3, IEEE802.3u, IEEE802.3ab
- Comprehensive LEDs for Speed, Link and Act(ivity)
- Supports auto-negotiation in 10/100/1000M, full-duplex, back-pressure in half-duplex and IEEE802.3x compliant flow control for full-duplex
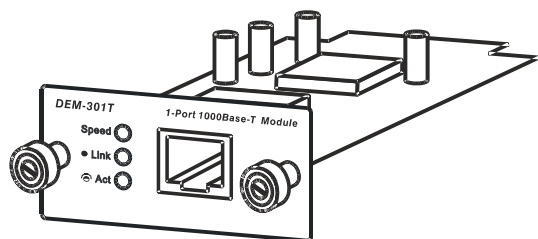
Figure 2- 4. DEM-301T Optional Module

- Single-Port SFP gigabit uplink module
- Compliant with IEEE802.3z
- Link and Act(ivity) LED
- Supports auto-negotiation in full-duplex and IEEE802.3x compliant flow control for full-duplex
- Support for DEM-310GT, DEM-311GT, DEM-314GT, DEM-315GT
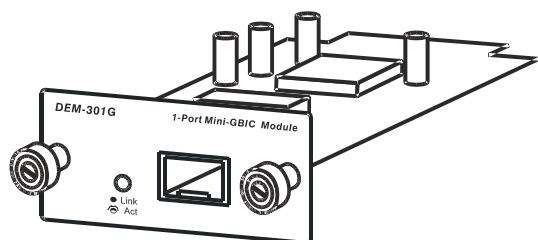
Figure 2- 5. DEM-301G Optional Module

- Single-Port 100BASE-FX fast Ethernet uplink module
- Compliant with IEEE802.3u
- Link and Act(ivity) LED
- Supports forced 100M, full-duplex and IEEE802.3x compliant flow control for full-duplex
- SC Type connector good over 2km distance
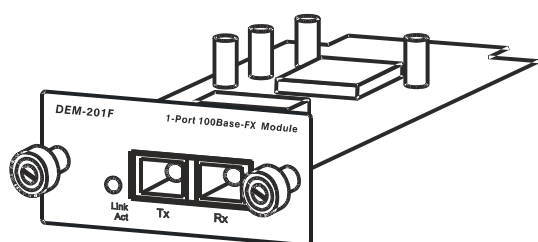
Figure 2- 6. DEM-201F Optional Module

- Single-Port 100BASE-FX fast Ethernet uplink module
- Compliant with IEEE802.3u
- Link and Act(ivity) LED
- Supports forced 100M, full-duplex and IEEE802.3x compliant flow control for full-duplex
- SC Type connector good over 15km distance
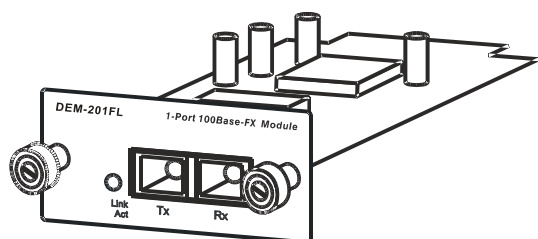
Figure 2- 7. DEM-201FL Optional Module

To install the modules, 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 front of the Switch to the right is the slot for the optional module, as shown in Figure 2-8 and Figure 2-9. This slot should be covered with a faceplate that can be easily removed by loosening the screws and pulling off the plate.
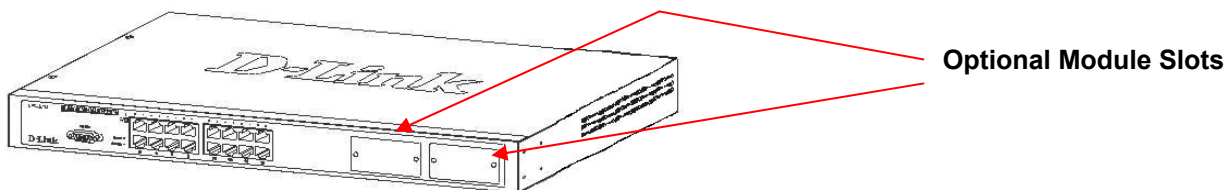
Figure 2- 8. Optional Module slots at the front of the DES-3018
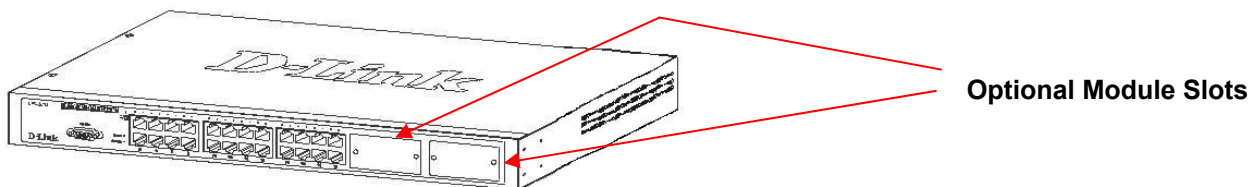
Figure 2- 9. Optional Module slot at the front of the DES-3026

Take the module and gently slide it in to the available slot at the front of the Switch until it reaches the back, as shown in the following figure. At the back of the slot is a plug that must be connected to the module. Gently, but firmly push in on the module to secure it to the Switch. The module should fit snugly into the corresponding receptor.
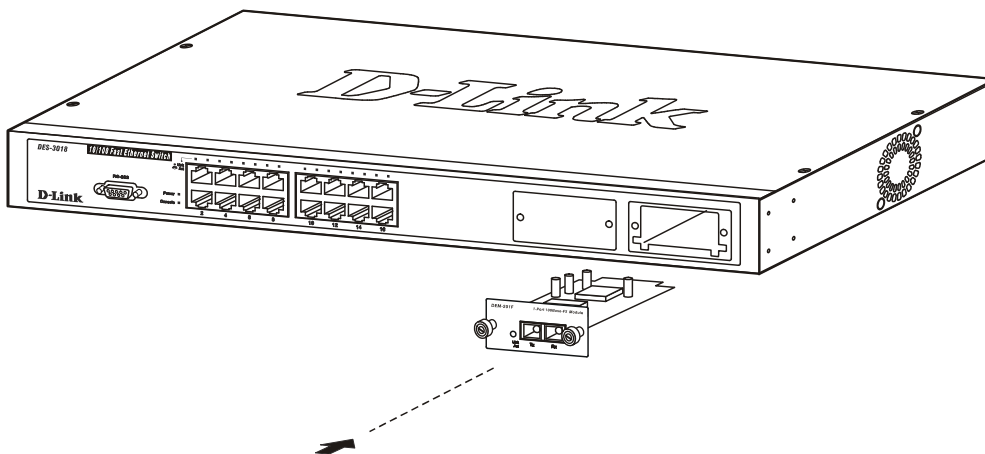
Figure 2- 10. Inserting the optional module into the Switch.

The upgraded DES-3018 / DES-3026 are now ready for use.

Section 3

Connecting the Switch

Switch To End Node

Switch to Hub or 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 most routers.

An end node can be connected to the Switch via a twisted-pair UTP/STP cable. The end node should be connected to any of the 10/100BASE-T ports of the Switch.
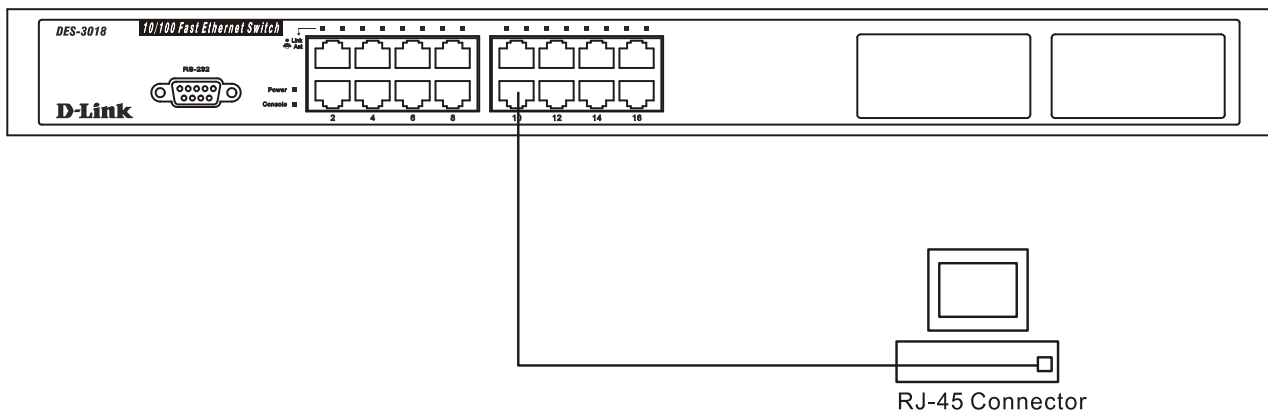
Figure 3- 1. Switch connected to an end node

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

Switch to Hub or Switch

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

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

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

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

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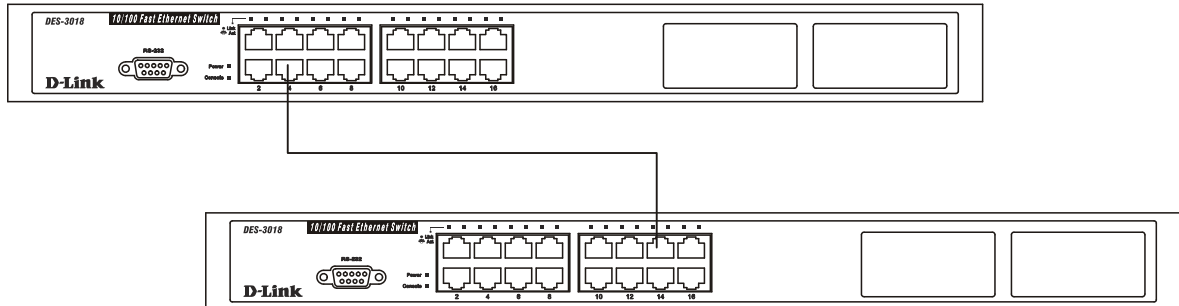
Figure 3- 2. Switch connected to a port on a hub or switch using a straight or crossover cable
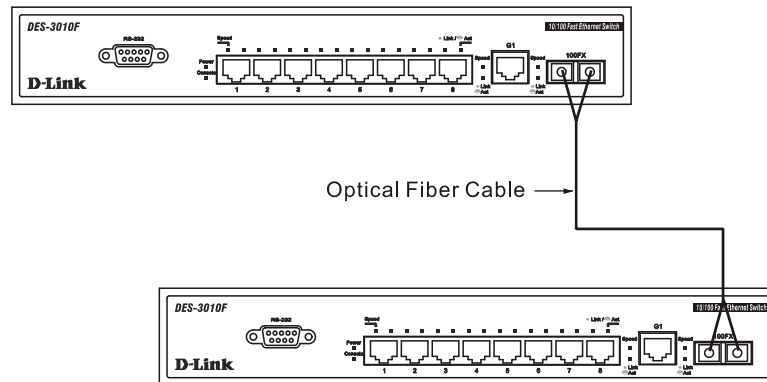
Figure 3- 3. Switch connected to switch using fiber-optic cabling

DES-3010F/FL/G, DES-3016/DES-3018 or DES-3026 as a Network Backbone

The Switch can be employed as a network backbone for offices or buildings that require many Ethernet connections within a confined space. Once a high-speed line has been connected from the ISP, the Switch can farm out connections for various end nodes including PCs, printers, hubs, routers or other switches. The topology configurations are endless but be sure that connections coming from the Switch are at a equal or slower speed than the ISP uplink to avoid bottlenecking.

The copper ports operate at a speed of 100Mbps or 10Mbps in full or half duplex mode. The 100BASE-FX ports can operate at 100Mbps in full duplex mode only. Copper gigabit ports may operate in 1000Mbps in full-duplex only. SFP gigabit ports operate in 1000Mbps in full-duplex 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.
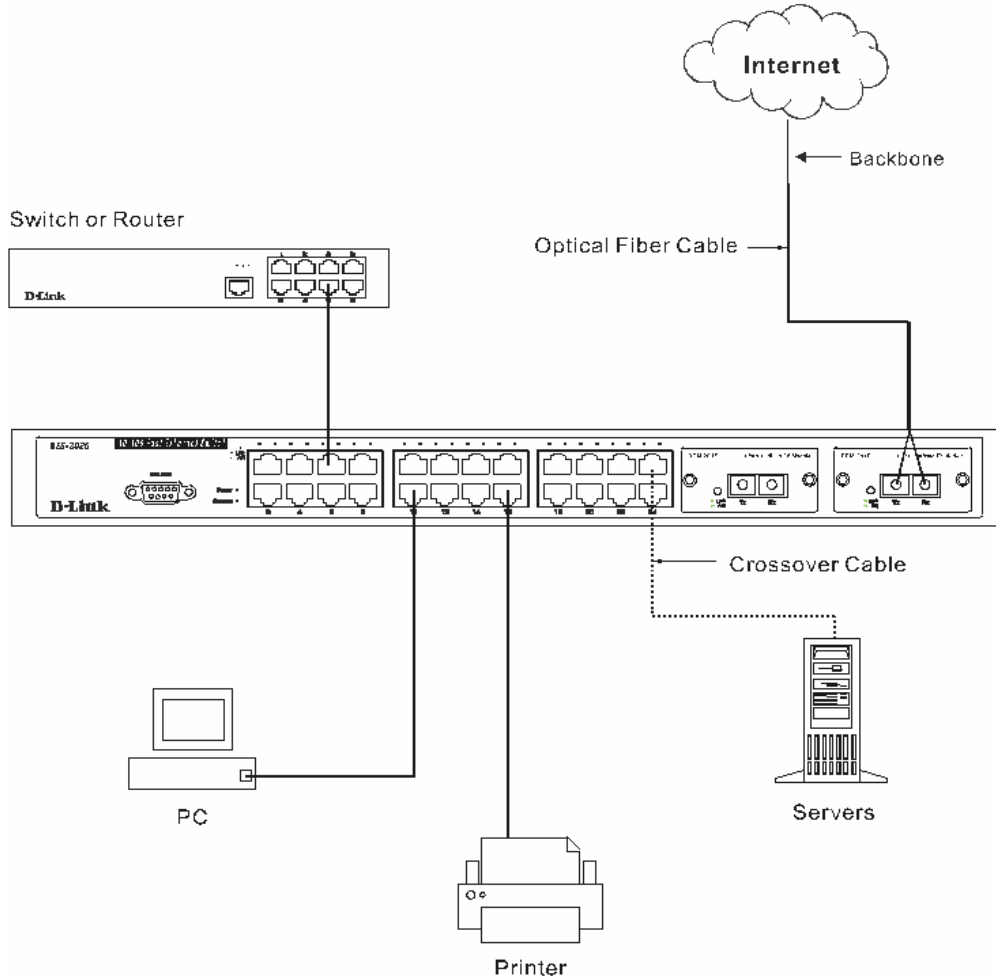
Figure 3- 4. Uplink Connection to a server, PC or switch stack.

<div style="text-align:right">

Section 4

</div>

Introduction to Switch Management

Management Options

Web-based Management Interface

SNMP-Based Management

Managing User Accounts

Command Line Console Interface through the Serial Port

Connecting the Console Port (RS-232 DCE)

First Time Connecting to the Switch

Password Protection

SNMP Settings

IP Address Assignment

Connecting Devices to the Switch

Management Options

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

Web-based Management Interface

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

SNMP-Based Management

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

Command Line Console Interface through the Serial Port

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

Connecting the Console Port (RS-232 DCE)

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

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

- A terminal or a computer with both a serial port and the ability to emulate a terminal.

- A null modem or crossover RS-232 cable with a female DB-9 connector for the console port on the Switch.

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

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

9. After you have correctly set up the terminal, plug the power cable into the power receptacle on the back of the Switch. The boot sequence appears in the terminal.
10. After the boot sequence completes, the console login screen displays.
11. If you have not logged into the command line interface (CLI) program, press the Enter key at the User Name and password prompts. There is no default user name and password for the Switch. User names and passwords must first be created by the administrator. If you have previously set up user accounts, log in and continue to configure the Switch.
12. Enter the commands to complete your desired tasks. Many commands require administrator-level access privileges. Read the next section for more information on setting up user accounts. See the *DES-3026 Command Line Interface Reference Manual* on the documentation CD for a list of all commands and additional information on using the CLI.
13. When you have completed your tasks, exit the session with the logout command or close the emulator program.

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

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

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

```
          DES-3026 Fast Ethernet Switch Command Line Interface

                      Firmware: Build 4.20.B27
          Copyright(C) 2007 D-Link Corporation. All rights reserved.


UserName:
```

Figure 4- 1. Initial screen after first connection.

First Time Connecting to the Switch

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

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

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

```
             DES-3026 Fast Ethernet Switch Command Line Interface

                        Firmware: Build 4.20.B27
            Copyright(C) 2007 D-Link Corporation. All rights reserved.

UserName:
```

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

Press Enter in both the Username and Password fields. You will be given access to the command prompt **DES-3026:4#**, as shown below:
There is no initial username or password. Leave the **Username** and **Password** fields blank.

```
             DES-3026 Fast Ethernet Switch Command Line Interface

                        Firmware: Build 4.20.B27
            Copyright(C) 2007 D-Link Corporation. All rights reserved.

UserName:
PassWord:

DES-3026:4#_
```

Figure 4- 3. Command Prompt

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

Password Protection

The DES-3010F/DES-3010FL/DES-3010G/DES-3016/DES-3018/DES-3026 switch does not have a default user name and password. One of the first tasks when setting up the Switch is to create user accounts. If you log in using a predefined administrator-level user name, you have privileged access to the Switch's management software.

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

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

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

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

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

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

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

The sample below illustrates a successful creation of a new administrator-level account on the DES-3026 with the user name "newmanager". The commands for creating a new administrator-level account are identical for the DES-3010F, DES-3010FL, DES-3010G, DES-3016 and DES-3018 switch models.

```
DES-3026:4#create account admin newmanager
Command: create account admin newmanager

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

Success

DES-3026:4#
```

Figure 4- 4. Creating a new Administrator-level account

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

SNMP Settings

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

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

The DES-3026 switch supports SNMP versions 1, 2c, and 3. You can specify which version of SNMP you want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v.1 and v.2c, 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.2c management access are:

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

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

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

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

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

Traps

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

MIBs

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

IP Address Assignment

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

The Switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found by entering the command "**show switch**" into the command line interface, as shown below.

```
DES-3026:4#show switch
Command: show switch


Device Type         : DES-3026 Fast Ethernet Switch
Module 1 Type       : None
Module 2 Type       : None
MAC Address         : 00-1C-F0-11-69-59
IP Address          : 10.73.21.26 (Manual)
VLAN Name           : default
Subnet Mask         : 255.0.0.0
Default Gateway     : 0.0.0.0
Boot PROM Version   : Build 1.01.009
Firmware Version    : Build 4.20.B27
Hardware Version    : A3
System Name         :
System Location     :
System Contact      :
Spanning Tree       : Disabled
LoopBack Detection  : Disabled
IGMP Snooping       : Disabled
VLAN trunk          : Disabled
802.1X              : Disabled
TELNET              : Enabled(TCP  23)
WEB                 : Enabled(TCP  80)
RMON                : Disabled
 CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Figure 4- 5. "show switch" command

The Switch's MAC address can also be found from the Web management program on the **DES-3028 Web Management Tool**.

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

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

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

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

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

```
              DES-3026 Fast Ethernet Switch Command Line Interface

                        Firmware: Build 4.20.027
              Copyright(C) 2008 D-Link Corporation. All rights reserved.


UserName:
PassWord:

DES-3026:4#config ipif System ipaddress 10.73.21.42/255.0.0.0
Command: congig ipif System ipaddress 10.73.21.42/8

Success

DES-3026:4#
```

Figure 4- 6. Assigning the Switch an IP Address

In the above example, the Switch was assigned an IP address of 10.7.3.21 with a subnet mask of 255.0.0.0. The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management.

Connecting Devices to the Switch

After you assign IP addresses to the Switch, you can connect devices to the Switch.
To connect a device to an SFP transceiver port:

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

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

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

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

Section 5

Introduction to Web-based Switch Configuration

Introduction

All software functions of the DES-3010F/DES-3010FL/DES-3010G/DES-3016/DES-3018/DES-3026 switch can be managed, configured and monitored via the embedded web-based (HTML) interface. The Switch can be managed from remote stations anywhere on the network through a standard browser such as Netscape Navigator/Communicator, Mozilla or Microsoft Internet Explorer. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

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

Logging on to the Web Manager

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

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

Once the IP address has been entered, the management module's user authentication window will be presented, as seen below.
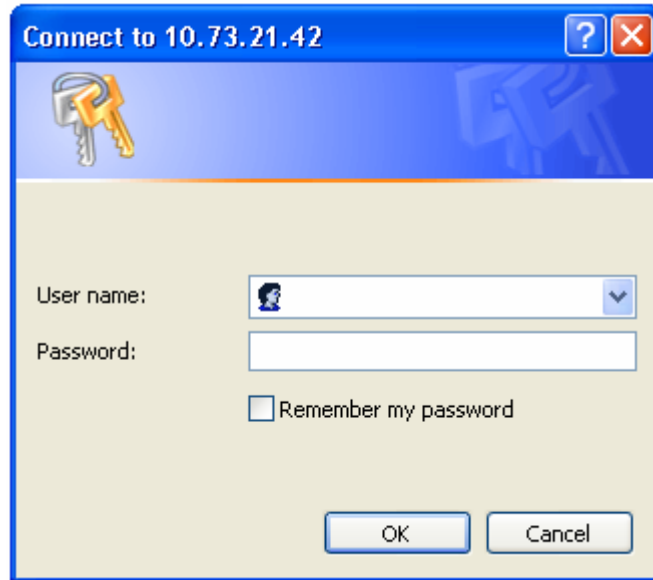
Figure 5- 1. Enter Network Password window

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 you to view performance statistics, and permits you to graphically monitor the system status.

Areas of the User Interface

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

Figure 5- 2. Main Web-Manager Screen

Area	Function
Area 1	Select the menu or window to be displayed. The folder icons can be opened to display the hyper-linked menu buttons and subfolders contained within them. Click the D-Link logo to go to the D-Link website.
Area 2	Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports and expansion modules, showing port activity, duplex mode, or flow control, depending on the specified mode. Various areas of the graphic can be selected for performing management functions, including port configuration. The user may also choose the device statistical refresh interval by using the pull-down menu in this section.
Area 3	Presents switch information based on your selection and the entry of configuration data.

NOTICE: Any changes made to the Switch configuration during the current session must be saved in the Save Changes web menu (explained below) or by using the command line interface (CLI) command *save*.

Web Pages

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

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

Administration - Contains screens concerning configurations for IP Address, Port Configuration, User Accounts, Password Encryption, Cable Diagnostics, Port Mirroring, System Log Settings, SNTP Settings, MAC Notification Settings, TFTP Services, Ping Test, SNMP Manager, IP-MAC Binding, Single IP Setting, Forwarding & Filtering, SMTP Service and DHCP/BOOTP Relay.

Layer 2 Features - Contains screens concerning configurations for Static VLAN Entry, VLAN Trunk Settings, Trunking, IGMP Snooping, Spanning Tree and Loopback Detection.

CoS - Contains screens concerning configurations for Port Bandwidth, 802.1p Default Priority, 802.1p User Priority, CoS Scheduling Mechanism, CoS Output Scheduling, Priority Settings, TOS Priority Settings, DSCP Priority Setttings, Port Mapping Priority Settings, and MAC Priority.

CPU Interface Filtering - Contains screens concerning configurations for CPU Interface Filtering State and the CPU Interface Filtering Table.

Security - Contains screens concerning configurations for Traffic Control, Port Security, Port Lock Entries, 802.1X, Trusted Host, Traffic Segmentation and SSH.

Monitoring - Contains screens concerning monitoring the Switch, pertaining to CPU Utilization, Port Utilization, Packets, Packet Errors, Packet Size, VLAN Status, MAC Address, Switch Log, Log Settings, IGMP Snooping Group, Browse Router Port, Browse ARP Table and Session Table.

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

<div style="text-align: right;">

Section 6

</div>

Administration

Device Information

IP Address

Port Configuration

User Accounts

Password Encryption

Cable Diagnostics

Port Mirroring

System Log Settings

SNTP Settings

MAC Notification Settings

TFTP Services

Ping Test

SNMP Manager

IP-MAC Binding

Single IP Setting

Forwarding and Filtering

SMTP Service

DHCP/BOOTP Relay

Device Information

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. Three of these functions, Spanning Tree, Port Mirror and Single IP Management have a Detail settings link which when clicked will automatically flip to the configuration page for that feature. This serves as a great quick reference for network administrators to promptly assess problems concerning Switch functions.

Device Information	
Device Type	DES-3026 Ethernet Switch
Module1 Type	None
Module2 Type	None
MAC Address	00-1C-F0-11-69-59
IP Address	10.73.21.42 (Manual)
VLAN Name	default
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
Boot PROM Version	Build 1.01.009
Firmware Version	Build 4.20.B27
Hardware Version	A3
System Name	
System Location	
System Contact	
Spanning Tree	Disabled Detail settings
MAC Notification	Disabled Detail settings
Port Mirror	Disabled Detail settings
Single IP Management	Disabled Detail settings
Serial Port Auto Logout	Never
Serial Port Baud Rate	9600
MAC Address Aging Time (10-1000000)	300
IGMP Snooping	Disabled
Multicast Router Only	Disabled
Telnet Status	Enabled
Telnet TCP Port Number(1-65535)	23
Web Status	Enabled
Web TCP Port Number(1-65535)	80
RMON Status	Disabled
Link Aggregation Algorithm	MAC Source
Switch 802.1x	Disabled
Auth Protocol	RADIUS Eap
Forward EAPOL PDU Both	Disabled
Syslog Status	Disabled
Port Security Trap Log	Disabled
ARP Aging Time(0-65535)	20
	Apply

Figure 6- 1. Device Information screen

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 *Command Line Interface Reference Manual* or return to Section 4 of this manual for more information.

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

To configure the Switch's IP address:

The web manager will display the Switch's current IP settings in the IP configuration menu, as seen below. To view this window click **Administration** > **IP Address**.

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 you want to access the Switch from a different subnet from the one it is installed on, enter the IP address of the **Default Gateway**. If you will manage the Switch from the subnet on which it is installed, you can leave the default address (0.0.0.0) in this field.
4.   If no VLANs have been previously configured on the Switch, you can use the *default* **VLAN Name**. The *default VLAN* contains all of the Switch ports as members. If VLANs have been previously configured on the Switch, you will need to enter the *VLAN ID* of the VLAN that contains the port connected to the management station that will access the Switch. The Switch will allow management access from stations with the same VID listed here.

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

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

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

The IP Address Settings 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.
Auto Config State	When autoconfig is enabled, the Switch is instructed to get a configuration file via TFTP, and it becomes a DHCP client automatically. The configuration file will be loaded upon booting up. In order to use Auto Config, 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 running and have the requested configuration file stored in its base directory when the request is received from the Switch. Consult the DHCP server and/or TFTP server software instructions for information on loading a configuration file for use by a client. (Also see the section titled **Error! Reference source not found.** for instructions on uploading a configuration to a TFTP server.) If the Switch is unable to complete the autoconfiguration process the previously saved configuration file present in Switch will be loaded.
Description	Enter a description of up to 128 alphanumeric characters to identify this IP interface. Only one IP interface can be set for this switch.

Click **Apply** to implement changes made.

Setting the Switch's IP Address using the Console Interface

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

The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known. The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

- Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/ yyy.yyy.yyy.yyy.** Where the x's represent the IP address to be assigned to the IP interface named System and the y's represent the corresponding subnet mask.
- Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z.** Where the x's represent the IP address to be assigned to the IP interface named **System** and the z represents the corresponding number of subnets in CIDR notation.

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

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

Port Configuration

This section contains information for configuring various attributes and properties for individual physical ports, including port speed and includes windows for **Port Settings**, **Port Description** and **Port Error Disabled**.

Port Settings

Click **Administration** > **Port Configuration > Port Settings** to display the following window:
To configure switch ports:

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:

Port Configuration

From	To	State	MDIX	Speed/Duplex	Flow Control	Apply
Port 1	Port 1	Enabled	Auto	Auto	Disabled	Apply

The Port Information Table

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

Figure 6- 3. Port Configuration and The Port Information Table window

The following parameters can be configured:

Parameter	Description
State	Toggle the **State** *<Enabled>* field to either enable or disable a given port or group of ports.
MDIX	Medium dependent interface crossover is a female port connection on the Switch used to connect to end stations, servers and hubs. The drop down menu allows the user to choose between **Auto**, **Normal** or **Cross**. *Auto* will automatically switch to the proper configuration once a cable is connected. *Normal* will be selected if a straight-through cable is being used and *Cross* should be selected if a crossover cable is being used.
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 three types of gigabit connections; *1000M/Full*, *1000M/Full_M* and *1000M/Full_S*. Gigabit connections are only supported in 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.
	Fiber optic ports are statically set and unchangeable at 1000Mbps in Full-Duplex. The user may configure these ports to be *Auto* or *1000M/Full*.
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*.

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

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** the following window will be displayed:

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

Figure 6- 4. Port Description Setting and Port Description Table

To remove a description for a port, select the port, leave the description field empty and click **Apply**.

Port Error Disabled

The following window is used to view information about ports that have had their connection status disabled, due to the detection of some storm control anomaly. To view the following window, click **Administration** > **Port Configuration > Port Error Disabled**

Port Error Disabled Table				
Port	State	Connection	Reason	Description

Figure 6- 5. Port Error Disabled window

The following information can be viewed in the preceding window:

Parameter	Description
Port	Denotes the port on the Switch that has been disabled.
State	Describes the current running state of the port in question, whether enabled or disabled.
Connection	Describes the current running state of the port in question. This field will read err-disabled when a port has been disabled due to connection errors.
Reason	Describes the reason for the error of the current running state of the port, which is exceeding the Packet Storm Control threshold.
Description	Displays the pre-configured description of the port, configured by the user.

User Accounts

Use the **User Accounts Management** window to control user privileges of different accounts on the Switch. To view existing User Accounts, click **Administration** > **User Accounts**

Figure 6- 6. User Accounts 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- 7. User Account Modify Table - 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. To return to the User Account window, click the hyperlinked Show All User Account Entries.

Figure 6- 8. User Account Modify Table

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. The user can choose the level of encryption for their new account by selecting *Default*, *plain_text* or *SHA-1*. The level of privilege (*Admin* or *User*) can be viewed in the **Access Right** field. To return to the User Account window, click the hyperlinked Show All User Account Entries.

35

Admin and User Privileges

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

The following table summarizes the Admin and User privileges:

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

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

Figure 6- 9. Admin and User Privileges

After establishing a User Account with Admin-level privileges, be sure to save the changes by opening the **Save Changes** window in the Main Menu and clicking the **Save Configuration** button.

Password Encryption

This window is used to control the password encryption on the Switch. To enable or disable Password Encryption, open **Administration** > **Password Encryption** which will display the following window:

Figure 6- 10. Password Encryption window

Cable Diagnostics

This window is used to control the cable diagnostics and determine where and what kind of errors have occurred on the cable. This function is primarily used for administrators to view tests on copper cables. To view the cable diagnostics, open **Administration** > **Cable Diagnostics** which will display the following window:

Figure 6- 11. Cable Diagnostics window

To view the cable diagnostics for a particular port use the drop down menu to choose the port and click **Test Now,** the information will be displayed in the Cable Diagnostics table.

Port Mirroring

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes. To view the **Port Mirroring** window, click **Administration > Port Mirroring**

Figure 6- 12. Port Mirroring window

To configure a mirror port:

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

- Select the **Source Direction**, **Ingress**, **Egress**, or **Both** and change the **Status** drop-down menu to *Enabled*.

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

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

System Log Settings

The Switch can send Syslog messages to up to four designated servers using the **Current System Log Host** window. Click **Administration > System Log Settings**, to view the screen shown below.

Add						
Current System Log Host						
Index	**Host IP**	**Severity**	**Facility**	**UDP Port**	**Status**	**Delete**
1	10.1.2.3	warning	Local0	514	Disabled	✕

Figure 6- 13. Current System Log Host window

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

System Log Host-Add	
Index(1-4)	1
Host IP	0.0.0.0
Severity	Warning
Facility	Local0
UDP Port(514 or 5000-65535)	514
Status	Disabled
	Apply

Show All System Log Servers

Figure 6- 14. Configure System Log Server - Add

The following parameters can be set:

Parameter	Description
Index(1-4)	Syslog server settings index (1-4).
Host IP	The IP address of the Syslog server.
Severity	This drop-down menu allows you to select the level of messages that will be sent. The options are *Warning*, *Informational*, and *All*.
Facility	Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following. **Bold** font denotes the facility values that the Switch currently implements.

Numerical Code **Facility**

0	kernel messages
1	user-level messages
2	mail system
3	system daemons

39

	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 5000-65535)	Enter the UDP port number used for sending Syslog messages. The default is 514.	
Status	Choose *Enabled* or *Disabled* to activate or deactivate.	

To set the System Log Server configuration, click **Apply**. To delete an entry from the **Current System Log 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.

SNTP Settings

Time Settings

This window is used to configure the time settings for the Switch. To view this window click, **Administration** > **SNTP Settings** > **Time Settings**.

Figure 6- 15. Current Time Settings window

The following parameters can be set or are displayed:

Parameter	Description
Time Settings - Current Time	
Current Time	Displays the current time.
Time Source	Displays the source of the time settings viewed here.
SNTP Settings	
SNTP State	Use this pull-down menu to Enable or Disable SNTP.
SNTP Primary Server	The IP address of the primary server the SNTP information will be taken from.
SNTP Secondary Server	The IP address of the secondary server the SNTP information will be taken from.
SNTP Poll Interval in Seconds	The interval, in seconds, between requests for updated SNTP information.
Time Settings - Set Current Time	
Year	Enter the current year, if you want to update the system clock.
Month	Enter the current month, if you would like to update the system clock.
Day	Enter the current day, if you would like to update the system clock.

Time in HH MM SS	Enter the current time in hours, minutes and seconds, if you would like to update the system clock.

Click **Apply** to implement your changes.

Time Zone and DST

The following are screens used to configure time zones and Daylight Savings time settings for SNTP. To display this window click **Administration** > **SNTP Settings > Time Zone and DST**

Figure 6- 16. Time Zone and DST Settings page

The following parameters can be set:

Parameter	Description
Time Zone and DST	
Daylight Saving Time State	Use this pull-down menu to enable DST Repeating Settings (Repeating) or DST Annual Settings (Annual). Selecting one of these will allow its corresponding field to be configured.
Daylight Saving Time Offset in Minutes	Use this pull-down menu to specify the amount of time that will constitute your local DST offset - 30, 60, 90, or 120 minutes.
Time Zone Offset from GMT in +/- HH:MM	Use these pull-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT).

DST Repeating Settings	
Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.	
From Which Week of the month	Enter the week of the month that DST will start.
From Which Day of the Week	Enter the day of the week that DST will start on.
From Which Month	Enter the month DST will start on.
From What Time HH:MM	Enter the time of day that DST will start on.
To Which Week	Enter the week of the month the DST will end.
To Which Day	Enter the day of the week that DST will end.
To Which Month	Enter the month that DST will end.
To What Time 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: What Month	Enter the month DST will start on, each year.
From What Date	Enter the day of the month DST will start on, each year.
From What Time	Enter the time of day DST will start on, each year.
To What Month	Enter the month DST will end on, each year.
To What Day	Enter the day of the month DST will end on, each year.
To What Time	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 clicking **Administration** > **MAC Notification Settings**.

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
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.

MAC Notification Global Settings

State	Disabled
Interval (1-2147483647 sec)	1
History size (1-500)	1

New MAC Notification Global Settings

State	Disabled
Interval (1-2147483647 sec)	1
History size (1-500)	1

Apply

MAC Notification Port Settings

From	To	State	Apply
Port 1	Port 1	Disabled	Apply

MAC Notification Port State Table

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

Figure 6- 17. 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 or vice versa. Use the pull-down menu to select the service to be completed. **Download Firmware** is used to transfer a firmware file from an outside source to the Switch using the TFTP Protocol. **Download Configuration** is used to transfer a configuration file from an outside source to the Switch using the TFTP Protocol. **Upload Configuration** is used to transfer a configuration file from the Switch to an outside source using the TFTP Protocol. **Upload Log** is used to transfer the Switch's log file from the Switch to an outside source using the TFTP Protocol. Once the user has selected an operation to perform, enter the **Server IP Address** and the path of the filename in use and click **Start** to initiate the file transfer. To view this window, click **Administration** > **TFTP Services**

Figure 6- 18. TFTP Services screen

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. To view this window, click **Administration** > **Ping Test**

Figure 6- 19. Ping Test

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. The user can also choose a **Time Out** for the ping, which will terminate the ping request if no response packet has returned to the Switch in the allotted time. Click **Start** to initiate the Ping program.

SNMP Manager

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 DES-3000 Switch Series supports the SNMP versions 1, 2c, and 3. You can specify which version of the SNMP you want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

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

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

public - Allows authorized management stations to retrieve MIB objects.

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

SNMPv3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMPv1 while assigning a higher level of security to another group, granting read/write privileges using SNMPv3.

Using SNMPv3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMPv3 in that SNMP messages may be encrypted. To read more about how to configure SNMPv3 settings for the Switch read the next section.

MIBs

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

The DES-3000 Series Switch incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.

The DES-3000 Series Switch 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, click **Administration > SNMP Manager > SNMP Trap Settings**

Figure 6- 20. 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 currently configured SNMP Users on the Switch.
To view this window, click **Administration** > **SNMP Manager** > **SNMP User Table**

Figure 6- 21. SNMP User Table

To delete an existing **SNMP User Table** entry, click the ☒ below the **Delete** heading corresponding to the entry you wish to delete.
To display the detailed entry for a given user, click on the hyperlinked **User Name**. This will open the **SNMP User Table Display** page, as shown below.

Figure 6- 22. 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 authorization protocol is in use.
	MD5 - Indicates that the HMAC-MD5-96 authentication level will be used.
	SHA - Indicates that the HMAC-SHA authentication protocol will be used.
Priv-Protocol	*None* - Indicates that no authorization protocol is in use.
	DES - Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.

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

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

Figure 6- 23. SNMP User Table Configuration window

The following parameters can set:

Parameter	Description
User Name	Enter an alphanumeric string of up to 32 characters. This is used to identify the SNMP user.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Encryption	Click the **encrypted** check box to enable encryption for the SNMP protocol. This feature is for users utilizing the SNMP V3 version. The user may configure the encryption in the following two fields.
Auth-Protocol	*MD5* - Specifies that the HMAC-MD5-96 authentication level will be used. This field is only operable when *V3* is selected in the **SNMP Version** field and the **Encryption** field has been checked. This field will require the user to enter a password.
	SHA - Specifies that the HMAC-SHA authentication protocol will be used. This field is only operable when *V3* is selected in the **SNMP Version** field and the **Encryption** field has been checked. This field will require the user to enter a password.
Priv-Protocol	*None* - Specifies that no authorization protocol is in use.
	DES - Specifies that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field is only operable when *V3* is selected in the **SNMP Version** field and the **Encryption** field has been checked. This field will require the user to enter a password between 8 and 16 alphanumeric characters.

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 this table, click **Administration** > **SNMP Manager** > **SNMP View Table**

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

Figure 6- 24. SNMP View Table

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

Figure 6- 25. SNMP View Table Configuration window - Add

The SNMP Group created with this table maps SNMP users (identified in the **SNMP User Table**) to the views created in the previous menu.
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**, click **Administration** > **SNMP Manager** > **SNMP Group Table**

Figure 6- 26. SNMP Group Table

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- 27. SNMP Group Table Display – View 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** page. This will open the **SNMP Group Table Configuration** page, as shown below.

Figure 6- 28. SNMP Group Table Configuration – Add 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, click **Administration** > **SNMP Manager** > **SNMP Community Table**

Figure 6- 29. SNMP Community Table window

The following parameters can set:
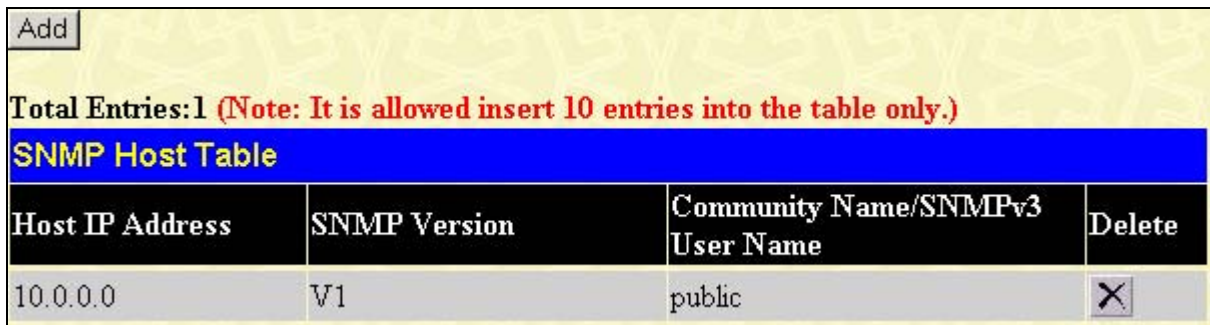
Parameter	Description
Community Name	Type an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name	Type an alphanumeric string of up 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 corresponding ☒ button under the **Delete** heading.

SNMP Host Table

Use the **SNMP Host Table** to set up SNMP trap recipients.
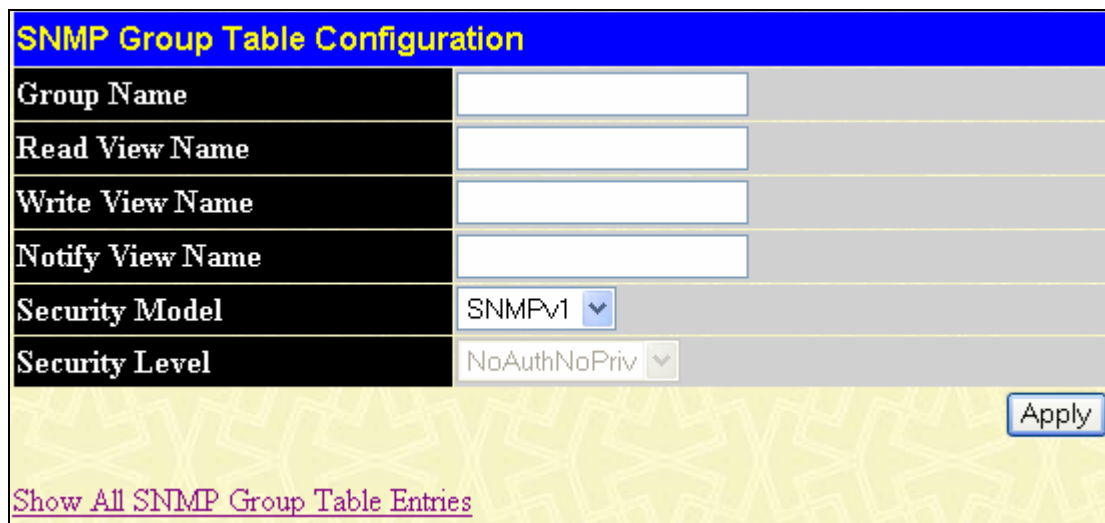To view the **SNMP Host Table** window click **Administration** > **SNMP Manager > SNMP Host Table**
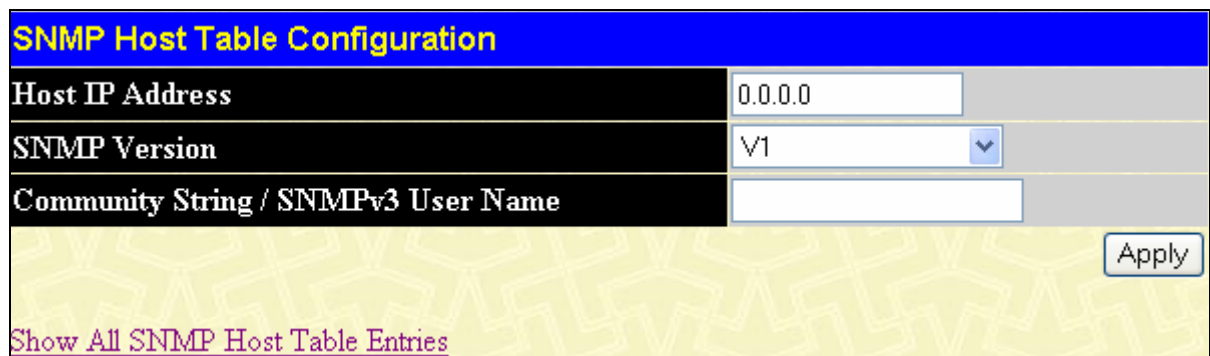
Figure 6- 30. SNMP Host Table

To delete an existing **SNMP Host Table** entry, click the corresponding ⊠ button under the **Delete** heading.
To add a new entry to the Switch's **SNMP Host Table**, click the **Add** button in the upper left-hand corner of
the page. This will open the **SNMP Host Table Configuration** page, as shown below.

Figure 6- 30. SNMP Host Table Configuration window

The following parameters can set:

Parameter	Description
Host IP Address	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
SNMP Version	*V1* - To specifies that SNMP version 1 will be used.
	V2 - To specify that SNMP version 2 will be used.
	V3-NoAuth-NoPriv - To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level.
	V3-Auth-NoPriv - To specify that the SNMP version 3 will be used, with 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, click **Administration** > **SNMP Manager > SNMP Engine ID**

Figure 6- 31. SNMP Engine ID Configuration window

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

IP-MAC-Port Binding (IMPB)

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. 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, this means a user can enable or disable the function on the individual port.

IP-MAC-Port Binding (IMPB)

The IP-MAC Ports Settings menu is used to enable IP-MAC binding on a per port basis. Ports that are enabled will apply the IP-MAC check to ingress packets for the port. The IP-MAC database used for the check must be set up with the **IP-MAC-Port Binding Table** (see below).
This table is used to enable or disable IP-MAC binding on specific ports. Select a port or a range of ports with the **From** and **To** fields. Enable or disable the port with the **State** field.
The **Zero IP** field is used to allow ARP packets entrance to the Switch when these packets have an IP address of 0.0.0.0, regardless of whether or not the 0.0.0.0 IP address is set in the IP-MAC Binding table. When the **Zero IP** field is set to *Disabled*, ARP packets containing the 0.0.0.0 IP address are dropped. Click **Apply** to save changes.
To view this table, click **Administration** > **IP-MAC Binding** > **IP-MAC Binding Port**

IP-MAC Binding Ports Setting

From	To	State	Zero IP	Apply
Port 1	Port 1	Disabled	Disabled	Apply

IP-MAC Binding Port State Table

Port	State	Zero IP
1	Disabled	Disabled
2	Disabled	Disabled
3	Disabled	Disabled
4	Disabled	Disabled
5	Disabled	Disabled
6	Disabled	Disabled
7	Disabled	Disabled
8	Disabled	Disabled
9	Disabled	Disabled
10	Disabled	Disabled
11	Disabled	Disabled
12	Disabled	Disabled
13	Disabled	Disabled
14	Disabled	Disabled
15	Disabled	Disabled
16	Disabled	Disabled
17	Disabled	Disabled
18	Disabled	Disabled
19	Disabled	Disabled
20	Disabled	Disabled
21	Disabled	Disabled
22	Disabled	Disabled
23	Disabled	Disabled
24	Disabled	Disabled
25	Disabled	Disabled
26	Disabled	Disabled

Figure 6- 32. IP-MAC Binding Ports window

When IP-MAC Binding Ports are enabled, use the IP-MAC Binding menu to configure the IP-MAC binding as applied to the enabled ports.

IP-MAC Binding Table

The IP-MAC Binding Table can be used to create IP-MAC binding entries. Enter the IP and MAC addresses of the authorized users in the appropriate fields and click **Add**. To use IP-MAC binding to check on specific

ports, the ports must first be enabled in the **IP-MAC Binding Ports** menu (see above). The ports are specified in the **Port** field as a range of integers (for example "1-3") or select the **All** option to apply to all ports.

To view this table, click **Administration** > **IP-MAC Binding** > **IP-MAC Binding Table**

Figure 6- 33. IP-MAC Binding Table menu

The **Address Binding Trap Log Settings** 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.

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**.

IP-MAC Binding Blocked

To view unauthorized devices that have been blocked by IP-MAC binding restrictions open the **IP-MAC Binding Blocked** window shown below. To view this table click **Administration** > **IP-MAC Binding** > **IP-MAC Binding Blocked**

Figure 6- 34. 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 ✕ next to the entry's MAC address. To delete all the entries in the **IP-MAC Binding Blocked Table** click **Delete All**.

D-Link Single IP Management

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 SIM. The **Commander Switch (CS)**, which is the master switch of the group, **Member Switch (MS)**, which is a switch that is recognized by the CS a member of a SIM group, and a **Candidate Switch (CaS)**, which is a Switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.

- A SIM group can only have one Commander Switch (CS).

- All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.

- A SIM group accepts up to 33 switches (numbered 0-32), including the Commander Switch (numbered 0).

There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.

If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.

SIM allows intermediate devices that do not support SIM. This enables the user to manage switches that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. SIM switches 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 commander 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 Single 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 a 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

After configuring one switch to operate as the CS of a SIM group, additional switches may join the group through a direct connection to the Commander switch. Only the Commander switch will allow entry to the candidate switch enabled for SIM. 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 an MS, it automatically becomes a member of the first SNMP community (include read/write and read only) to which the CS belongs. However, if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

SIM Using the Web Interface

All 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, click **Administration > Single IP Settings > SIM Settings**

Figure 6- 35. 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- 36. SIM Settings window (Enabled)

The following parameters can be set:

Parameters	Description
SIM State	Use the pull down menu to either enable or disable the SIM state on the Switch. *Disabled* will render all SIM functions on the Switch inoperable.
Role State	Use the pull down menu to change the SIM role of the Switch. The two choices are: • *Candidate* - A Candidate Switch (CaS) is not the member of a SIM group but is connected to a Commander Switch. This is the default setting for the SIM role. • *Commander* - Choosing this parameter will make the Switch a Commander Switch (CS). The user may join other switches to this Switch, over Ethernet, to be part of its SIM group. Choosing this option will also enable the Switch to be configured for SIM.
Discovery Interval	The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to a Commander Switch will include information about other switches connected to it. (Ex. MS, CaS). The user may set the **Discovery Interval** from 30 to 90 seconds.

Holdtime	This parameter may be set for the time, in seconds the Switch will hold information sent to it from other switches, utilizing the **Discovery Interval**. The user may set the hold time from 100 to 255 seconds.

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

After enabling the Switch to be a Commander Switch (CS), the **Single IP Management** folder will then contain three added links to aid the user in configuring SIM through the web, including **Topology**, **Firmware Upgrade** and **Configuration Backup/Restore**.

Topology

The **Topology** window will be used to configure and manage the Switch within the SIM group and requires Java script to function properly on your computer.

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

Figure 6- 37. 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 Name** is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
Local Port	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.

Speed	Displays the connection speed between the CS and the MS or CaS.
Remote Port	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
MAC Address	Displays the **MAC Address** of the corresponding Switch.
Model Name	Displays the full **Model Name** of the corresponding Switch.

To view the **Topology Map**, click the View menu in the toolbar and then Topology, which will produce the following screen. The **Topology View** will refresh itself periodically (20 seconds by default).
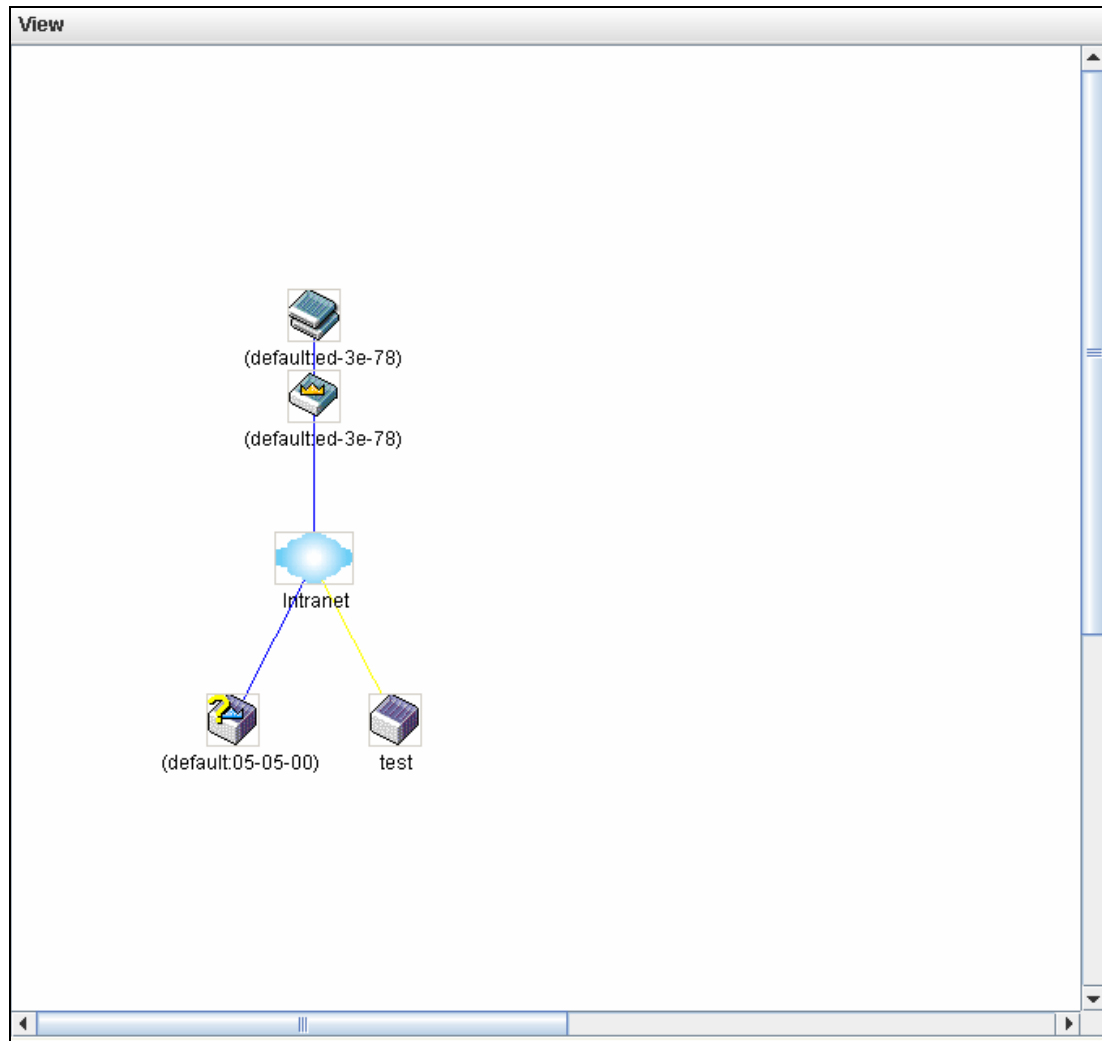
Figure 6- 38. Topology view

This screen will display how the devices within the Single IP Management Group are connected to other groups and devices. Possible icons in this screen are as follows:

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.
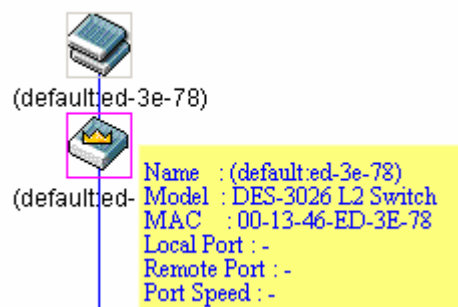
Figure 6- 39. Device Information Utilizing the Tool Tip

Setting the mouse cursor over a line between two devices will display the connection speed between the two devices, as shown below.
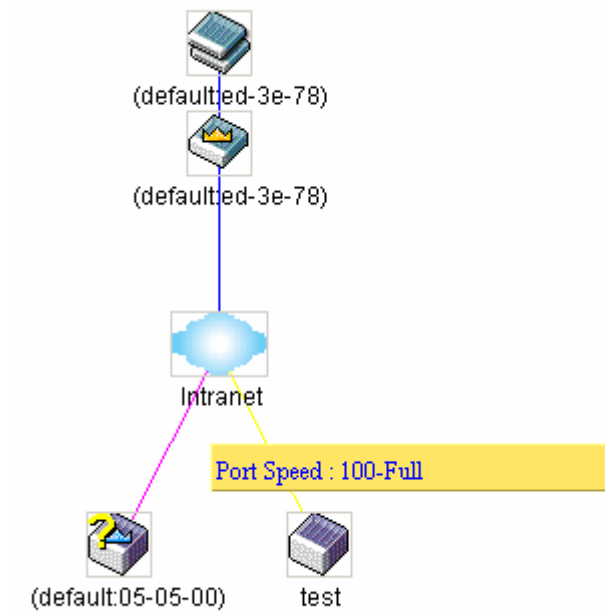
Figure 6- 40. Port Speed Utilizing the Tool Tip

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
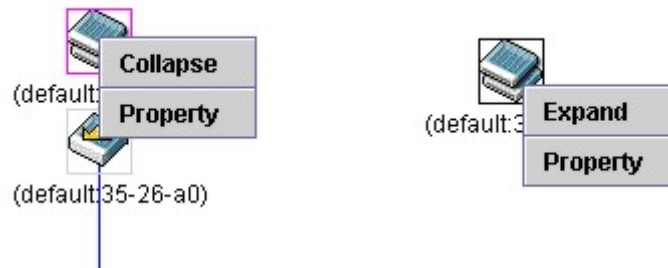
Figure 6- 41. Right Clicking a Group Icon

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.
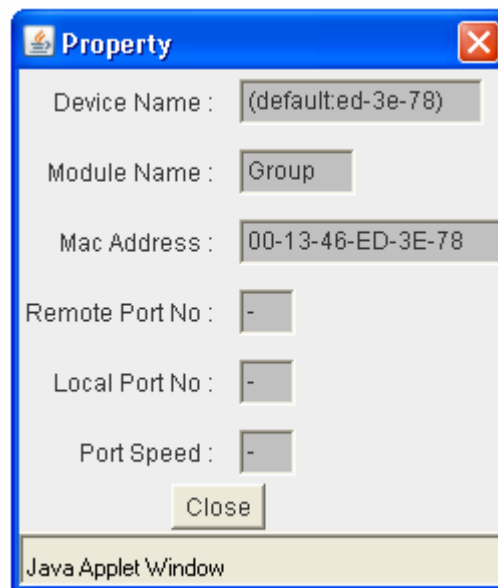
Figure 6- 42. Property window

Commander Switch Icon
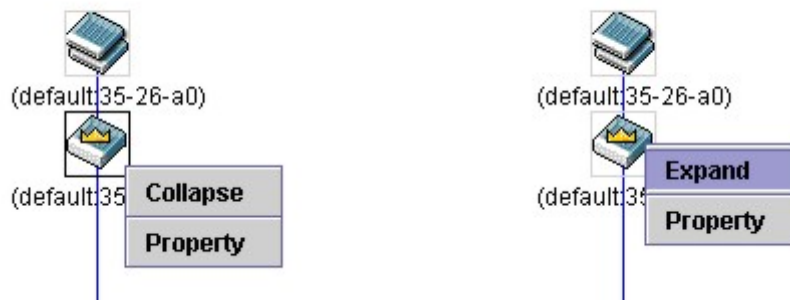
Figure 6- 43. Right Clicking a Commander Icon

The following options may appear for the user to configure:

- **Collapse** - to collapse the group that will be represented by a single icon.
- **Expand** - to expand the SIM group, in detail.
- **Property** - to pop up a window to display the group information.
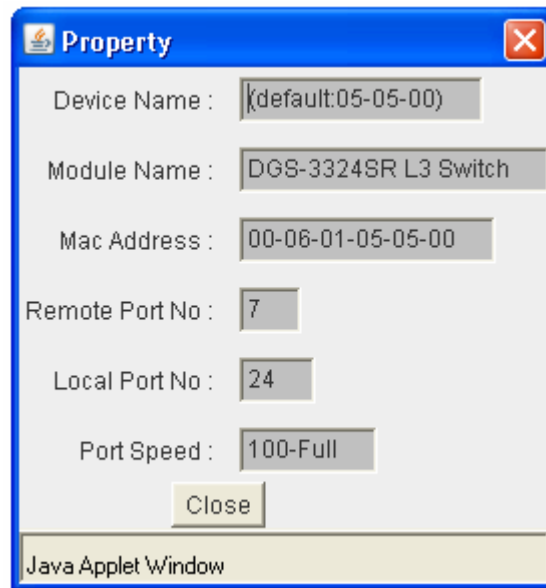
Figure 6- 44. Property window

Member Switch Icon
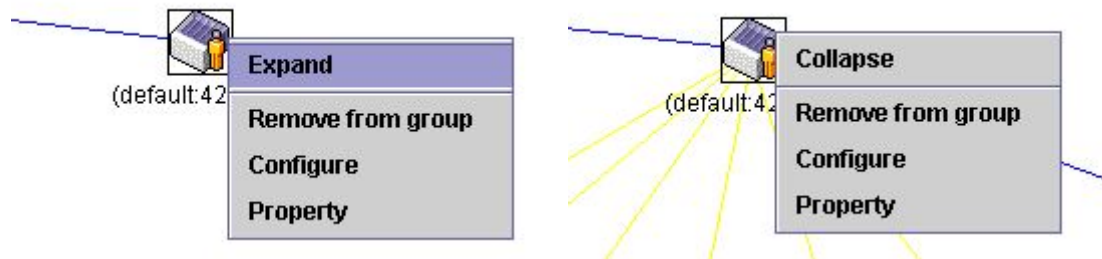
Figure 6- 45. Right Clicking a Member icon

The following options may appear for the user to configure:

- **Collapse** - to collapse the group that will be represented by a single icon.
- **Expand** - to expand the SIM group, in detail.
- **Remove from group** - remove a member from a group.
- **Configure** - launch the web management to configure the Switch.
- **Property** - to pop up a window to display the device information.
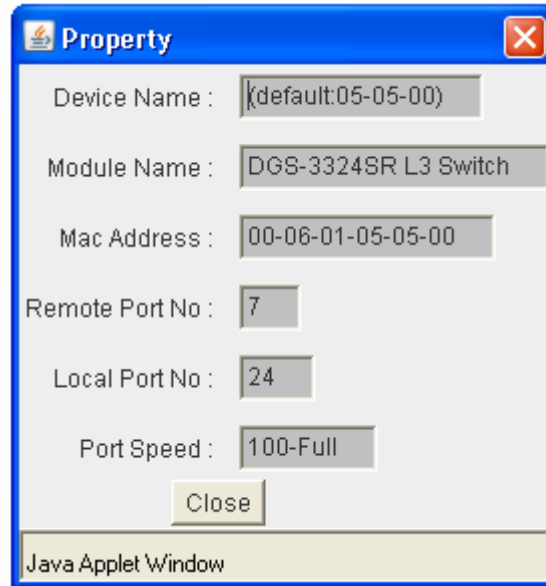
Figure 6- 46. Property window

Candidate Switch Icon
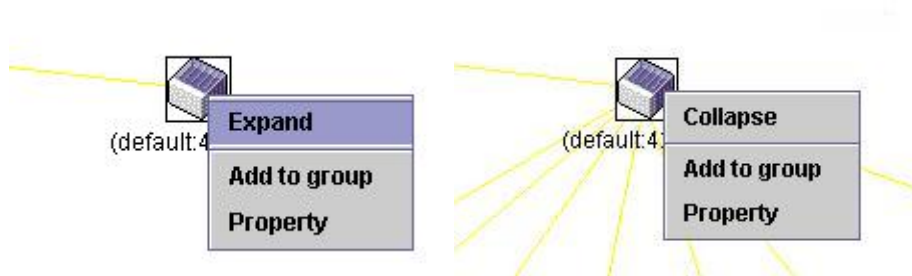
Figure 6- 47. Right Clicking a Candidate icon

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.
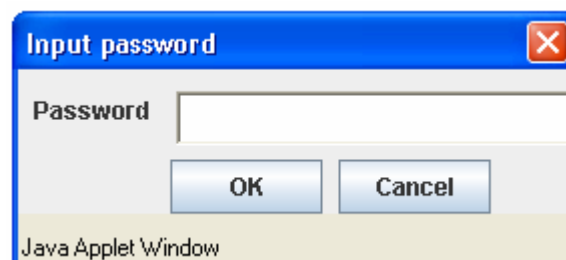
Figure 6- 48. Input password window.

- **Property** - to pop up a window to display the device information, as shown below.
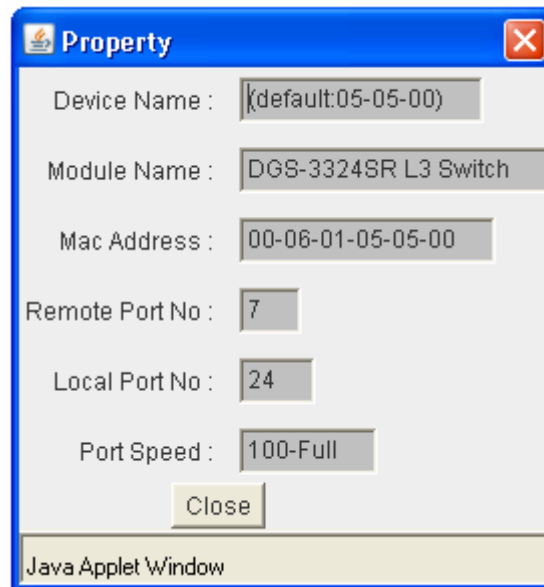
Figure 6- 49. Device Property window.

This window holds the following information:

Parameter	Description
Device Name	This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
Module Name	Displays the full module name of the switch that was right-clicked.
MAC Address	Displays the MAC Address of the corresponding Switch.
Remote Port No.	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
Local Port No.	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
Port Speed	Displays the connection speed between the CS and the MS or CaS

Click **Close** to close the **Property** window.

Menu Bar

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

Figure 6- 50. 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.
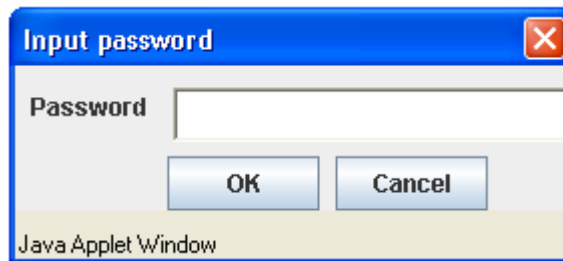
Figure 6- 51. Input password window.

- **Remove from Group** - remove an MS from the group.

Device

- **Configure** - will open the web manager for the specific device.

View

- **Refresh** - update the views with the latest status.
- **Topology** - display the Topology view.

Help

- **About** - Will display the SIM information, including the current SIM version.
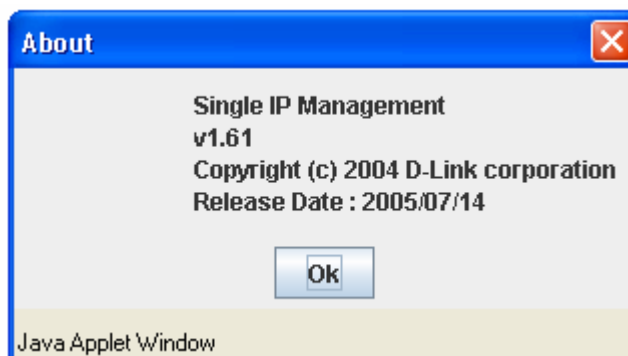
Figure 6- 52. About window.

NOTE: Upon this firmware release, some functions of the SIM can only be configured through the Command Line Interface. See the *DES-30XX CLI Manual* for more information on SIM and its configurations.

Firmware Upgrade

This screen is used to upgrade firmware from the Commander Switch to the Member Switch. Member Switches will be listed in the table and will be specified by **Port** (port on the CS where the MS resides), **MAC Address**, **Model Name** and **Version**. To specify a certain Switch for firmware download, click its corresponding check box under the **Port** heading. To update the firmware, enter the **Server IP Address** where the firmware resides and enter the **Path/Filename** of the firmware. Click **Download** to initiate the file transfer. To access the following window, click **Administration > Single IP Setting> Firmware Upgrade**

Figure 6- 53. Firmware Upgrade window

Configuration File Backup/Restore

This screen is used to upgrade configuration files from the Commander Switch to the Member Switch using a TFTP server. Member Switches will be listed in the table and will be specified by **Port** (port on the CS where the MS resides), **MAC Address**, **Model Name** and **Version**. To specify a certain Switch for upgrading configuration files, click its corresponding radio button under the **Port** heading. To update the configuration file, enter the **Server IP Address** where the file resides and enter the **Path/Filename** of the configuration file. Click **Download** to initiate the file transfer from a TFTP server to the Switch. Click **Upload** to backup the configuration file to a TFTP server. To access the following window, click **Administration > Single IP Setting> Configuration File Backup/Restore**

Figure 6- 54. Configuration File Backup/Restore window

Upload Log File

The following window is used to upload log files from SIM member switches to a specified PC. To upload a log file, enter the IP address of the SIM member switch and then enter a path on your PC where you wish to save this file. Click **Upload** to initiate the file transfer. To view this window click **Administration > Single IP Setting > Upload Log File**

Figure 6- 55. Upload Log File window

Forwarding & Filtering

Unicast Forwarding

To view or configure the Unicast Forwarding window click, **Administration > Forwarding & Filtering > Unicast Forwarding**

Figure 6- 56. Setup Static Unicast Forwarding Table and 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.
Port	Allows the selection of the port number on which the MAC address entered above resides.

Click **Apply** to implement the changes made. Current entries can be found in the **Static Unicast Forwarding Table** as shown in the bottom half of the figure above. To delete an entry in the **Static Unicast Forwarding Table**, click the corresponding ✖ under the **Delete** heading.

Multicast Forwarding

The following figure and table describes how to set up **Multicast Forwarding** on the Switch. To view this window click **Administration** > **Forwarding & Filtering** > **Multicast Forwarding**

Figure 6- 57. Static Multicast Forwarding Settings and Current Multicast Forwarding Entries window

The **Static Multicast Forwarding Settings** page 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**, as shown below:

Figure 6- 58. Setup Static Multicast Forwarding Table - Add

The following parameters can be set:

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

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

Multicast Filtering Mode

Use the **Multicast Filtering Mode Setting** menu to select one of two filtering options for multicast packets:

- **Forward unregistered groups** – This default setting will forward all multicast streams.
- **Filter unregistered groups** – This setting will only forward multicasts to registered multicast groups. Multicasts to unregistered groups are blocked.

To view this window, click **Administration** > **Forwarding & Filtering** > **Multicast Filtering Mode**

Figure 6- 59. Configure Multicast Filtering Mode

Select the desired Multicast Filtering Mode setting and click **Apply** to effect the change.

SMTP Service

SMTP or Simple Mail Transfer Protocol is a function of the Switch that will send switch events to mail recipients based on e-mail addresses entered using the commands below. The Switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the Switch, place the appropriate information into an e-mail and deliver it to recipients configured on the Switch. This can benefit the Switch administrator by simplifying the management of small workgroups or wiring closets, increasing the speed of handling emergency Switch events and enhancing security by recording questionable events occurring on the Switch.

The Switch plays four important roles as a client in the functioning of SMTP:

- The server and server virtual port must be correctly configured for this function to work properly. This is accomplished in the **SMTP Service Settings** window by properly configuring the *SMTP Server Address* and *SMTP Server Port* fields.

- Mail recipients must be configured on the Switch. This information is sent to the server which then processes the information and then e-mails Switch information to these recipients. Up to 8 e-mail recipients can be configured on the Switch using the **SMTP Service Settings** window by configuring the *Mail Receiver Address* field.

- The administrator can configure the source mail address from which messages are delivered to configured recipients. This can offer more information to the administrator about Switch functions and problems. The personal e-mail can be configured using the **SMTP Service Settings** window and setting the *Self Mail Address* field.

- The Switch can be configured to send out test mail to first ensure that the recipient will receive e-mails from the SMTP server regarding the Switch. To configure this test mail, the SMTP function must first be enabled by configuring the SMTP State in the **SMTP Service Settings** window and then by sending an email using the **SMTP Service** window. All recipients configured for SMTP will receive a sample test message from the SMTP server, ensuring the reliability of this function.

The Switch will send out e-mail to recipients when one or more of the following events occur:

- When a cold start occurs on the Switch.
- When a port enters a link down status.
- When a port enters a link up status.
- When SNMP authentication has been denied by the Switch.
- When a switch configuration entry has been saved to the NVRAM by the Switch.
- When an abnormality occurs on TFTP during a firmware download event. This includes *in-process*, *invalid-file*, *violation*, *file-not-found*, *complete* and *time-out* messages from the TFTP server.
- When a system reset occurs on the Switch.

Information within the e-mail from the SMTP server regarding switch events includes:

- The source device name and IP address.
- A timestamp denoting the identity of the SMTP server and the client that sent the message, as well as the time and date of the message received from the Switch. Messages that have been relayed will have timestamps for each relay.
- The event that occurred on the Switch, prompting the e-mail message to be sent.
- When an event is processed by a user, such as save or firmware upgrade, the IP address, MAC address and User Name of the user completing the task will be sent along with the system message of the event occurred.
- When the same event occurs more than once, the second mail message and every repeating mail message following will have the system's error message placed in the subject line of the mail message.

The following details events occurring during the Delivery Process.

- Urgent mail will have high priority and be immediately dispatched to recipients while normal mail will be placed in a queue for future transmission.

- The maximum number of untransmitted mail messages placed in the queue cannot exceed 30 messages. Any new messages will be discarded if the queue is full.
- If the initial message sent to a mail recipient is not delivered, it will be placed in the waiting queue until its place in the queue has been reached, and then another attempt to transmit the message is made.
- There is a maximum of three attempts to deliver mail to recipients. Mail message delivery attempts will be tried every five minutes until the maximum number of attempts is reached. Once reached and the message has not been successfully delivered, the message will be dropped and not received by the mail recipient.

If the Switch shuts down or reboots, mail messages in the waiting queue will be lost.

SMTP Server Settings

The following window is used to configure the fields to set up the SMTP server for the switch, along with setting e-mail addresses to which switch log files can be sent when a problem arises on the Switch. To open the following window, click **Administration** > **SMTP Service > SMTP Server Settings**

Figure 6- 60. SMTP Service Settings and Mail Receiver Address Table window

The following parameters can be set:

Parameter	Description
SMTP State	Use the pull-down menu to enable or disable the SMTP service on this device.
SMTP Server Address	Enter the IP address of the SMTP server on a remote device. This will be the device that sends out the mail for you.
SMTP Server Port	Enter the virtual port number that the Switch will connect with on the SMTP server. The common port number for SMTP is 25, yet a value between 1 and 65535 can be chosen.
Self Mail Address	Enter the e-mail address from which mail messages will be sent. This address will be the "from" address on the e-mail message sent to a recipient. Only one self mail address can be configured for this Switch. This string can be no more that 64 alphanumeric characters.
Mail Receiver Address	Enter a list of e-mail addresses so recipients can receive e-mail messages regarding Switch functions. Up to 8 e-mail addresses can be added per Switch. Do delete these addresses from the Switch, click it's corresponding ✕ under the Delete heading in the Mail Receiver Address Table.

Click **Apply** to implement changes made.

SMTP Service

The following window is used to send test messages to all mail recipients configured on the Switch, thus testing the configurations set and the reliability of the SMTP server. To access the following window, click **Administration** > **SMTP Service > SMTP Service**

Figure 6- 61. SMTP Mail Service

The following parameters can be set:

Parameter	Description
Subject	Enter the subject of the test e-mail.
Content	Enter the content of the test e-mail.

Once your message is ready, click **Send** to send this mail to all recipients configured on the Switch for SMTP.

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- 62. DHCP/ BOOTP Relay Global Settings window

The following fields can be set:

Parameter	Description
BOOTP 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*
BOOTP 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*.
BOOTP 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 Vendor class Identifier option 60 State	Allows the user to *Enable* or *Disable* the DHCP relay option 60 on the Switch. The default is *Disabled*. *Enabled* – Allows the relay servers priority based on option 60. If the relay servers are determined based on option 60 then the IPIF configured servers will be ignored. *Disabled* – If the relay server is not determined then the IPIF configured servers will be used to determine the relay servers.
DHCP Client identifier option 61 State	Allows the user to *Enable* or *Disable* the DHCP relay option 61 state on the Switch. The default is *Disabled*.

	Enabled – When option 61 is enabled, if the packets do not have option 61 then the relay servers cannot be determined based on option 61. If the relay servers are determined based on option 61 then the IPIF configured servers will be ignored.
	Disabled – If the relay server is not determined then the IPIF configured servers will be used to determine the relay servers.
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 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, you might configure a client with the option-82 field. In this situation, you should disable the information-check feature so that the switch does not remove the option-82 field from the packet. You can 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 on the Switch.

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- 63. Circuit ID and Remote ID Sub-option Format

DHCP/BOOTP Relay Interface Settings

This window allows the user to set up a server, by IP address, for relaying DHCP/ BOOTP information to the Switch. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP/BOOTP server using the following window. Properly configured settings will be displayed in the **DHCP/BOOTP Relay Interface Table** at the bottom of the following window. The user may add up to four server IP's per IP interface on the Switch. To enable and configure **DHCP/BOOTP Relay Global Settings** on the Switch, click **Administration > DHCP/BOOTP Relay** > **DHCP/BOOTP Relay Interface Settings**

DHCP/BOOTP Relay Interface Settings

Interface	Server IP	Apply
System	0.0.0.0	Add

DHCP/BOOTP Relay Interface Table

Interface	Server 1	Server 2	Server 3	Server 4

Figure 6- 64. DHCP/BOOTP Relay Interface Settings and DHCP/BOOTP Relay Interface 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

DHCP Relay Option 60 Default Settings

This function allows the user to set up the **DHCP Relay Option 60 Default Settings**. When there are no servers found that are suitable for the packet based on option 60, the relay servers will be determined by the default relay server setting. To view this window, click **Administration** > **DHCP/BOOTP Relay** > **DHCP Relay Option 60 Default Settings**

DHCP Relay Option 60 Default Settings

Relay IP Address	0.0.0.0	Add
Mode	Drop	Apply

DHCP Relay Option 60 Default RelayTable

Server 1	Server 2	Server 3	Server 4

Figure 6- 65. DHCP Relay Option 60 Default Settings window

The following parameters may be configured or viewed.

Parameter	Description
Relay IP Address	Enter the ip address that the
Mode	*Drop* – When drop is specified, the packet with no matching rules found will be dropped without further process. *Relay* – When relay is specified the packet will be processed further based on option 61. The final relay servers will unite option 60 default relay servers and the relay servers determined by option 61.

DHCP Relay Option 60 Settings

This window allows the user to choose whether DHCP relay will process the DHCP option or not. When Option 60 is enabled, if the packet doesn't already have option 60 then the relay servers cannot be determined based on option 60. The relay servers will be determined based on either option 61 or IPIF configured servers. If the relay servers are determined based on option 60 or option 61 then the IPIF configured servers will be ignored. If the relay servers are not determined by option 60 or option 61, then the IPIF will be used to determine the relay servers.

To view this window, click **Administration** > **DHCP/BOOTP Relay** > **DHCP Relay Option 60 Settings**

Figure 6- 66. DHCP Relay Option 60 Settings window

To find an entry, enter the String or IP address and click **Search**, to view all entries click **ViewAll** to delete an entry click **Delete**.
To add a new entry click **Add**, the following window will appear for the user to configure.

Figure 6- 67. DHCP Relay Option 60 Settings window - Add

The following parameters may be configured.

Parameter	Description
String	Enter a string for the new entry up to a maximum of 255 characters.
Server IP	Enter a Server IP address.
Match Type	Use the drop down menu to choose *Exact Match* or *Partial Match*.

Click **Apply** to implement changes made. To return to the DHCP Relay Option 60 Table, click the Show DHCP Relay Option 60 Table link.

DHCP Relay Option 61 Default Settings

This window allows the user to set the default Server IP address. This setting can be used to determine the rule to process the packets that have no option 61 matching rules. The default is **Drop**.

To view this window, click **Administration** > **DHCP/BOOTP Relay** > **DHCP Relay Option 61 Default Settings**

Figure 6- 68. DHCP Relay Option 61 Default Settings window

DHCP Relay Option 61 Settings

This window allows the user to view the DHCP Relay Option 61 Table.

To view this window, click **Administration** > **DHCP/BOOTP Relay** > **DHCP Relay Option 61 Settings**

Figure 6- 69. DHCP Relay Option 61 Settings window

To delete an entry, enter the appropriate information and click **Delete**, to remove all entries click **Clear All**. To add a new entry click **Add,** the following screen will appear for the user to configure.

Figure 6- 70. DHCP Relay Option 61 Settings window – (Add)

The following parameters may be set.

Parameter	Description
Client ID	The client may be identified by either the **MAC Address** or by the user specified **String**. Choose the desired method and enter the appropriate information for the **Client ID**.

Relay Rule	The relay rule is specified to determine that the relay server is based on option 61. When option_61 is enabled, if the packet does not have option 61, then the relay servers cannot be determined based on option 61. If relay servers are determined based on option 60, and one relay server is determined based on option 61, the final relay servers will be the union of these two sets of servers. If the relay servers are determined based on option 60 or option 61, then per IPIF configured servers will be ignored. If the relay servers are not determined either by option 60 or option 61, then per IPIF configured servers will be used to determine the relay servers.
	Drop – When drop is specified, the packet with no matching rules found will be dropped without further process.
	Relay – When relay is specified the packet will be processed further based on option 61.

Click **Apply** to implement changes made. To return to the DHCP Relay Option 61 Table, click the Show DHCP Relay Option 61 Table link.

L2 Features

Static VLAN Entry

VLAN Trunking Settings

Trunking

IGMP Snooping

Spanning Tree

Loopback Detection

VLANs

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 Switch

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 Switch supports IEEE 802.1Q 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 of which the receiving port is a member.

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.
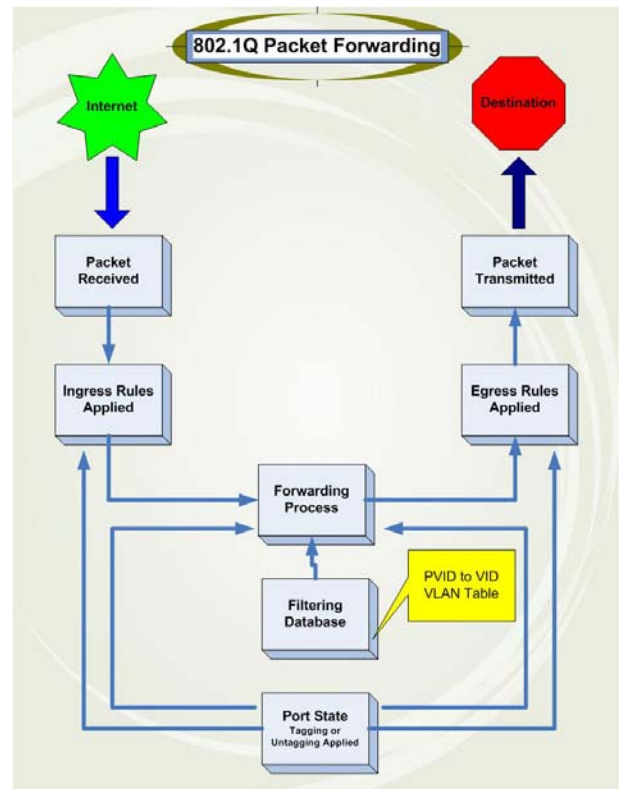
Figure 7- 1. IEEE 802.1Q Packet Forwarding

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.
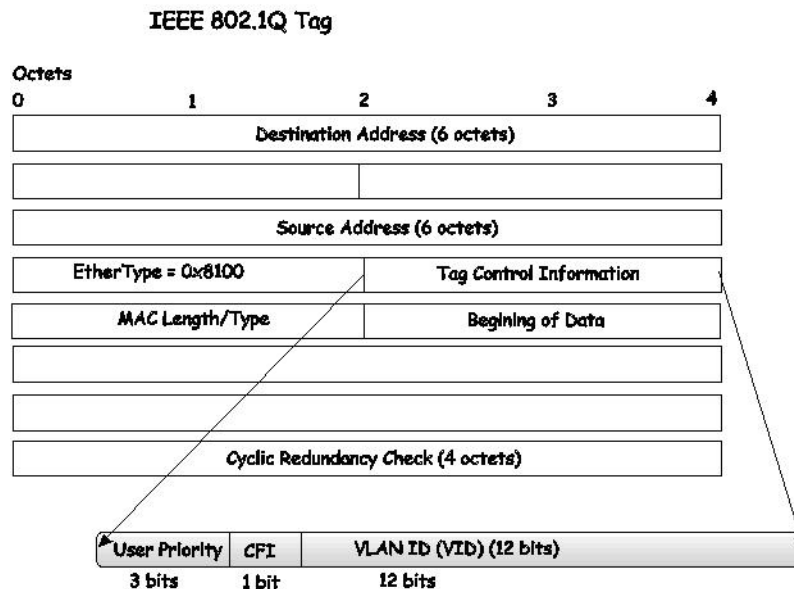
Figure 7- 2. IEEE 802.1Q Tag

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.
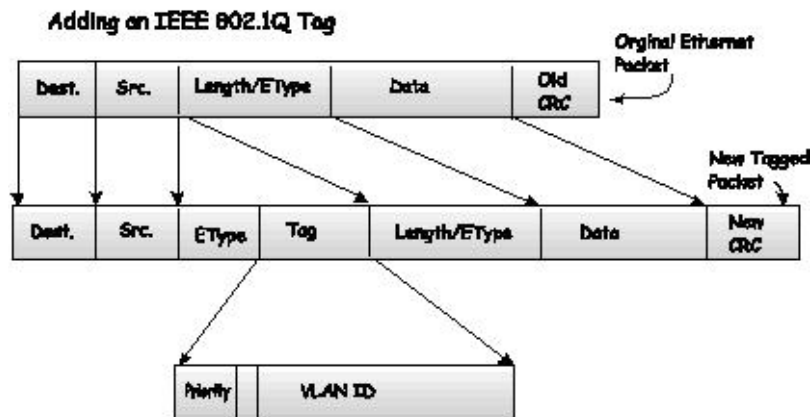
Figure 7- 3. Adding an IEEE 802.1Q Tag

Tagging and Untagging

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

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

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

Ingress Filtering

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

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the Switch then determines if the destination port is a member of the 802.1Q VLAN. If it

is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

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

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

Default VLANs

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

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

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

An example is presented below:

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

Table 7- 1. VLAN Example - Assigned Ports

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.

Static VLAN Entry

The **Static VLAN Entry** table allows the user to configure the Static VLAN entries for the switch. To view this window click **L2 Features** > **VLAN** > **Static VLAN Entry**

Figure 7- 4. 802.1Q Static VLANs window

The **802.1Q Static VLANs** menu lists all previously configured VLANs by **VLAN ID** and **VLAN Name**.

To delete an existing 802.1Q VLAN, click the corresponding ![X] button under the **Delete** heading. To edit an entry click the corresponding **Modify** button.

To create a new 802.1Q VLAN, click the **Add** button in the **802.1Q Static VLANs** menu. A new menu 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 menu.

Figure 7- 5. 802.1Q Static VLANs – (Add)

To return to the **Current 802.1Q Static VLANs Entries** window, click the <u>Show All Static VLAN Entries</u> link. To change an existing 802.1Q VLAN entry, click the **Modify** button of the corresponding entry you wish 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.

Figure 7- 6. 802.1Q Static VLANs – (Modify)

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

Parameter	Description
VID	Allows the entry of a VLAN ID in the Add dialog box, or displays the VLAN ID of an existing VLAN in the Modify dialog box. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allows the entry of a name for the new VLAN in the Add dialog box, or for editing the VLAN name in the Modify dialog box.
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.

Click **Apply** to implement changes made. Click the Show All Static VLAN Entries link to return to the **802.1Q Static VLANs** window.

Link Aggregation

Understanding Port Trunk Groups

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

The Switch supports up to three port trunk groups with 2 to 8 ports in each group. A potential bit rate of 8000 Mbps can be achieved.
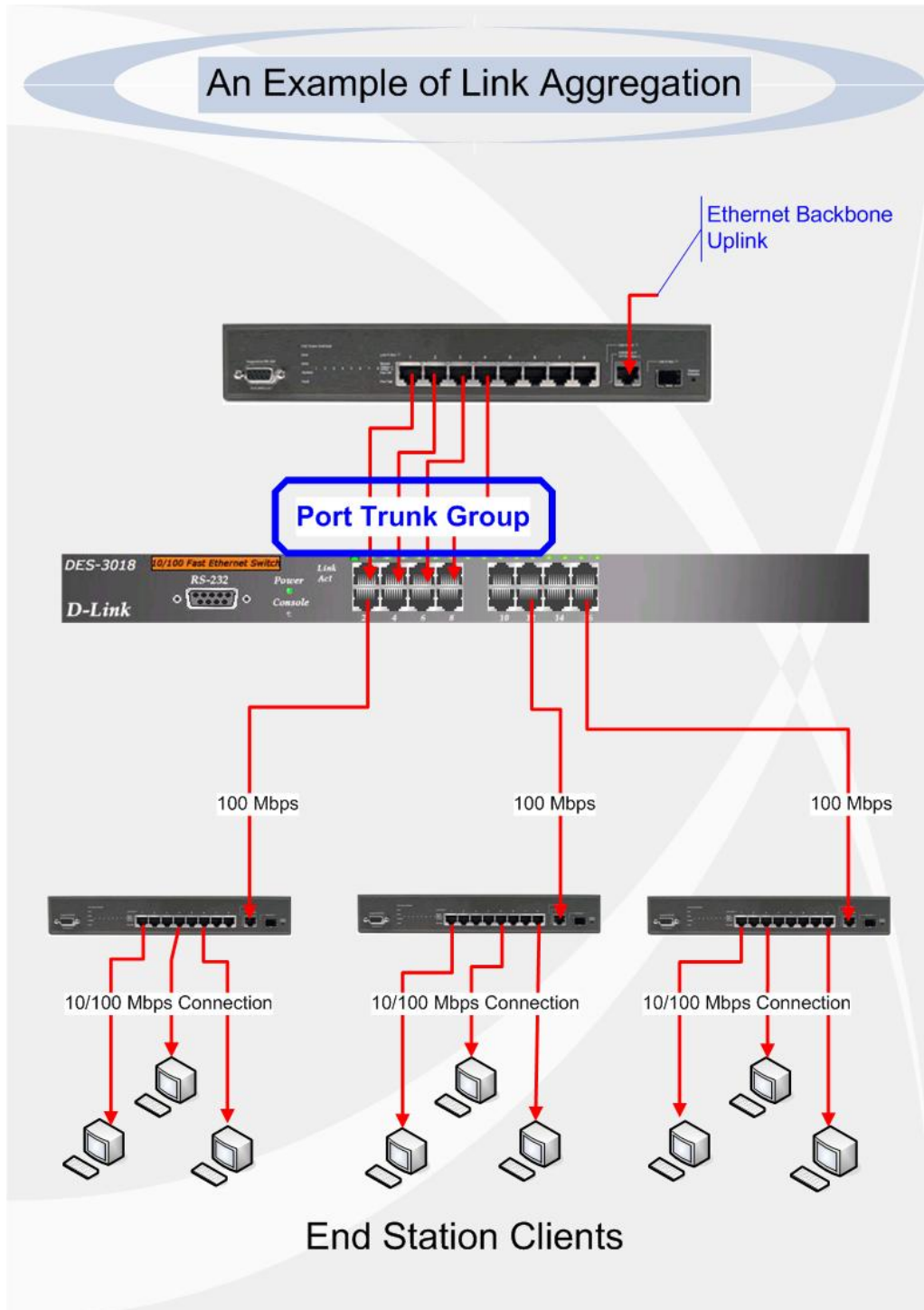
Figure 7- 7. Example of Port Trunk Group

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

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

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

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

The Switch allows the creation of up to 3 link aggregation groups, each group consisting of 2 to 4 links (ports). All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control, traffic segmentation and 802.1p default priority configurations must be identical. Port locking, port mirroring and 802.1X must not be enabled on the trunk group. Further, the aggregated links must all be of the same speed and should be configured as full-duplex.

The Master Port of the group is to be configured by the user, and all configuration options, including the VLAN configuration that can be applied to the Master Port, are applied to the entire link aggregation group.

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

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

VLAN Trunk Settings

The **VLAN Trunk Settings** table allows the user to configure a port or range of ports as VLAN trunk ports, by default none of the ports on the Switch are VLAN trunk ports unless configured. To view this window click **L2 Features** > **VLAN Trunk Settings**

Figure 7- 8. VLAN Trunk Settings window

The following parameters can be set:

Parameter	Description
VLAN Trunk Status	Use the pull down menu to *Enable* or *Disable* the VLAN trunk global settings on the Switch. If enabled the VLAN trunk ports shall be ale to forward all tagged frames with any VID.
From…To	Enter the port or range of ports you wish to configure for VLAN trunk port settings.
Status	Use the pull down menu to *Enable* or *Disable* the VLAN trunk settings for a port or range of ports on the Switch.

Link Aggregation

To configure a port trunking group or view the current trunking group entries, click **L2 Features > Trunking > Link Aggregation**

Figure 7- 9. Port Trunking Group window

To configure port trunk groups, click the **Add** button to add a new trunk group and use the **Port Trunking Configuration** menu (see example below) to set up trunk groups. To modify a port trunk group, click the hyperlinked group number corresponding to the entry you wish to alter. To delete a port trunk group, click the corresponding ⊠ under the **Delete** heading in the **Current Trunking Group Entries** table.

Figure 7- 10. Link Aggregation Group Configuration window – Add

To return to the Port Trunking Group Entries Table, click the hyperlinked Show All Port Trunking Group Entries.

LACP Port Settings

This window allows the user 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 (Link Aggregation Control Protocol) control frames. To view the LACP Settings window click **L2 Features** > **Trunking** > **LACP Port Settings**

Figure 7- 11. LACP Settings window

The following fields can be set:

Parameter	Description
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).

Click **Apply** to implement changes made.

IGMP Snooping

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

In order to use IGMP Snooping it must first be enabled for the entire Switch (see **Advanced Settings**). You may then fine-tune the settings for each VLAN using the **IGMP Snooping** link in the **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. Use the **IGMP Snooping Group Entry Table** to view the IGMP Snooping status. To modify the settings, click the **Modify** button for the VLAN Name entry you want to change.

To view this window click **L2 Features** > **IGMP Snooping** > **IGMP Snooping**

Figure 7- 12. Current IGMP Snooping Group Entries

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

Figure 7- 13. IGMP Snooping Settings-Edit window

97

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 **IGMP Snooping Settings**.
VLAN Name	This is the **VLAN Name** that, along with the **VLAN ID**, identifies the VLAN for which to modify the **IGMP Snooping Settings**.
Query Interval (1-65535)	The **Query Interval** field is used to set the time (in seconds) between transmitting IGMP queries. Entries between 1 and 65535 seconds are allowed. Default = 125.
Max Response Time (1-25)	This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The **Max Response Time** field allows an entry between 1 and 25 (seconds). Default = 10.
Robustness Value (1-255)	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the **Robustness 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 (1-25)	This field specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. Default = 1.
Host Timeout (1-16711450)	This is the maximum amount of time in seconds allowed for a host to continue membership in a multicast group without the Switch receiving a host membership report. Default = 260.
Router Timeout (1-16711450)	This is the maximum amount of time in seconds a route is kept in the forwarding table without receiving a membership report. Default = 260.
Leave Timer (1-16711450)	This specifies the maximum amount of time in seconds between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. If no response to the membership query is received before the **Leave Timer** expires, the (multicast) forwarding entry for that host is deleted.
Querier State	Choose *Enabled* to enable transmitting IGMP Query packets or *Disabled* to disable. The default is *Disabled*.
Querier Router Behavior	This read-only field describes the behavior of the router for sending query packets. *Querier* will denote that the router is sending out IGMP query packets. *Non-Querier* will denote that the router is not sending out IGMP query packets. This field will only read *Querier* when the **Querier State** and the **State** fields have been Enabled.
State	Select *Enabled* to implement IGMP Snooping. This field is *Disabled* by default.
Multicast fast leave	This parameter allows the user to enable the *Fast Leave* function. Enabled, this function will allow members of a multicast group to leave the group immediately (without the implementation of the Last Member Query Timer) when an IGMP Leave Report Packet is received by the Switch. The default is *Disabled*.

Click **Apply** to implement the new settings. Click the Show All IGMP Group Entries link to return to the **Current IGMP Snooping Group Entrie**s window.

> **NOTE:** The Fast Leave function is intended for IGMPv2 users wishing to leave a multicast group and is best implemented on VLANs that have only one host connected to each port. When one host of a group of hosts uses the Fast Leave function, it may cause the inadvertent fast leave of other hosts of the group.

Static Router Ports 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.

To view this window click, **L2 Features** > **IGMP Snooping > Static Router Ports Settings**

Figure 7- 14. Static Router Ports Settings window

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

Figure 7- 15. Static Router Ports Settings - Modify window

The following parameters can be set:

Parameter	Description
VID	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	These are the ports on the Switch that will have a multicast router attached to them.

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

IGMP Access Control Settings

This window is used to enable the IGMP access control settings on the switch. When the access control settings are enabled the switch will receive an IGMP join message, the switch will then send the access request to the radius server to complete the authentication process. To view this window click, **L2 Features** > **IGMP Snooping > IGMP Access Control Settings**

IGMP Access Control Settings			
From	**To**	**Status**	**Apply**
Port 1 ⌄	Port 1 ⌄	Disabled ⌄	Apply

IGMP Access Control Table	
Port	**Status**
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled

Figure 7- 16. IGMP Access Control Settings

The following parameters can be set:

Parameter	Description
From…To	Enter a port or group of ports that may be configured for IGMP Access Control settings.
Status	This function is used to *Enable* or *Disable* the IGMP Access Control Settings.

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

NOTE: To use IGMP Access Control, the user must first configure the multicast filtering mode so that it can filter unregistered groups.

Spanning Tree

This Switch supports two versions of the Spanning Tree Protocol; 802.1D STP and 802.1w Rapid STP. 802.1D STP will be familiar to most networking professionals. However, since 802.1w RSTP has been recently introduced to D-Link managed Ethernet switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1D STP and 802.1w RSTP.

802.1w Rapid Spanning Tree

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

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 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 two 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. RSTP combines the transition states disabled, blocking and listening used in 802.1D and creates a single state Discarding. In either case, ports do not forward packets. In the STP port transition states disabled, blocking or listening or in the RSTP port state discarding, there is no functional difference, the port is not active in the network topology. Table 6-2 below compares how the two protocols differ regarding the port state transition.

All two 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.

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

Table 6- 1. Comparing Port States

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

Edge Port

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

P2P Port

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

802.1D and 802.1w Compatibility

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

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, click **L2 features** > **Spanning Tree** > **STP Bridge Global Settings**

Figure 7- 17. STP Bridge Global Settings

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)

The following parameters can be set:

Parameter	Description
Spanning Tree Protocol	Use the pull-down menu to enable or disable STP globally on the Switch. The default is *Disabled*.

Bridge 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.
Bridge 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.
Bridge 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.
Bridge Priority (0-61440)	A Priority for the Switch can be set from *0* to *61440.* This number is used in the voting process between Switches on the network to determine which Switch will be the root Switch. A low number indicates a high priority, and a high probability that this Switch will be elected as the root Switch.
Default Path Cost	This read-only field displays the protocol used in determining the default path cost per port. **802.1t** will calculate this 32-bit cost value through the use of a specific formula based on the port bandwidth.
STP Version	Use the pull-down menu to choose the desired version of STP to be implemented on the Switch. There are two choices: *STPCompatibility* - 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.
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.

Click **Apply** to implement changes made.

STP Port Settings

STP can be set up on a port per port basis.
To view the following window click **L2 Features > Spanning Tree > STP Port Settings**

STP Port Settings

From	To	State	Cost(0=Auto)	Priority	Migration	Edge	P2P	BPDU
Port 1	Port 1	Enabled	0	128	No	False	Auto	Disabled

Apply

The STP Port Information

Port	Connection	State	Cost	Priority	Edge	P2P	STP Status	Role	Port Forward BPDU
1	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
2	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
3	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
4	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
5	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
6	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
7	100M/Full/None	Yes	*2000000	128	No	Yes	Forwarding	NonStp	Enabled
8	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
9	100M/Full/None	Yes	*2000000	128	No	Yes	Forwarding	NonStp	Enabled
10	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
11	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
12	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
13	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
14	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
15	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
16	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
17	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
18	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
19	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
20	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
21	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
22	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
23	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
24	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
25	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled
26	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled

Figure 7- 18. STP Port Settings and Table window

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

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

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

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

The following fields can be set:

Parameter	Description
From/To	A consecutive group of ports may be configured starting with the selected port.
State	Used to *Enable* or *Disable* the STP port state settings on the Switch.
Cost (0 = Auto)*	**External Cost** - This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto). • *0 (auto)* - Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. • *value 1-2000000* - Define a value between 1 and 2000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.
Priority	A Port Priority can be from *0* to *240*. The lower the number, the greater the probability the port will be chosen as the Root Port.
Migration	Setting this parameter as "*yes*" will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting If the Switch is configured for RSTP, the port will be capable to migrate from 802.1D STP to 802.1w RSTP. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP on all or some portion of the segment.
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.*
BPDU	Choosing Enabled will allow the forwarding of BPDU packets in the specified ports from other network devices. This will go into effect only if STP is globally disabled AND Forwarding BPDU is globally enabled (See STP Bridge Global Settings above). The default setting Disabled, does not forward BPDU packets when STP is disabled.

Click **Apply** to implement changes made.

NOTE: To enable Forwarding BPDU on a per port basis, the following settings must first be in effect: 1. STP must be globally disabled and 2. Forwarding BPDU must be globally enabled. These are the default settings configurable in the **STP Bridge Global Settings** menu discussed previously.

Loopback Detection

The Loopback Detection function is used to identify loops occurring between the Switch and a device that is directly connected to it. This process is accomplished by the use of a Configuration Testing Protocol (CTP) packet that is generated by the switch. Users may set the dispatching time interval of the CTP packet and once a CTP packet has returned to the port from where it originated, the Loopback Detection function will disable this port until the anomaly has ceased, and the loopback occurrence will be noted in the Switch's log. Once the loopback problem has stopped, this port will be automatically recovered in a time period that can also be specified by the user.

To configure the settings for the Loopback Detection feature, click **L2 Features** > **Loopback Detection**

Figure 7- 19. Loopback Detection window

The following fields may be configured:

Parameter	Description
Loopdetect Status	Choose whether to globally enable or disable the Loopback Detection function by using this pull down menu.
Interval	Enter a time interval, between 1 and 32767 seconds, that CTP packets will be dispatched from Loopback Detection enabled ports. If this packet is returned, the port will be disabled. The default setting is 10 seconds.

Recover Time	Enter a time, in seconds that a port will have to wait before being recovered from a Loopback Detection shutdown. The user may set a time between 60 and 1000000 seconds with a default setting of 60 seconds. The user may also enter a time of 0 which means that the port can only be recovered manually by the user. This is done by going to the **Port Configuration** folder located in the **Administration** folder and manually enabling these ports using the **Port Settings** window.
From… To	Choose a port or group of ports that are to be enabled for the Loopback Detection function.
State	Use the pull-down menu to enable or disable the Loopback function for the selected ports.

Click **Apply** to implement changes made.

<div align="right">
Section 8
</div>

CoS

CoS

The Switch supports 802.1p and other priority protocols. The following section discusses the implementation 802.1p priority queuing and the Class of Service or CoS mapping on the Switch.

IEEE 802.1p Priority

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

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

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

The Switch allows you to further tailor how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows you to specify its relative priority to suit the needs of your network. There may be circumstances where it would be advantageous to group two or more differently tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 3, be reserved for data packets with a priority value of 7. Packets that have not been given any priority value are placed in Queue 0 and thus given the lowest priority for delivery.

A weighted round robin system is employed on the Switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 3, 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.

The Advantages of CoS

CoS 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 Switch implements basic 802.1p priority queuing.
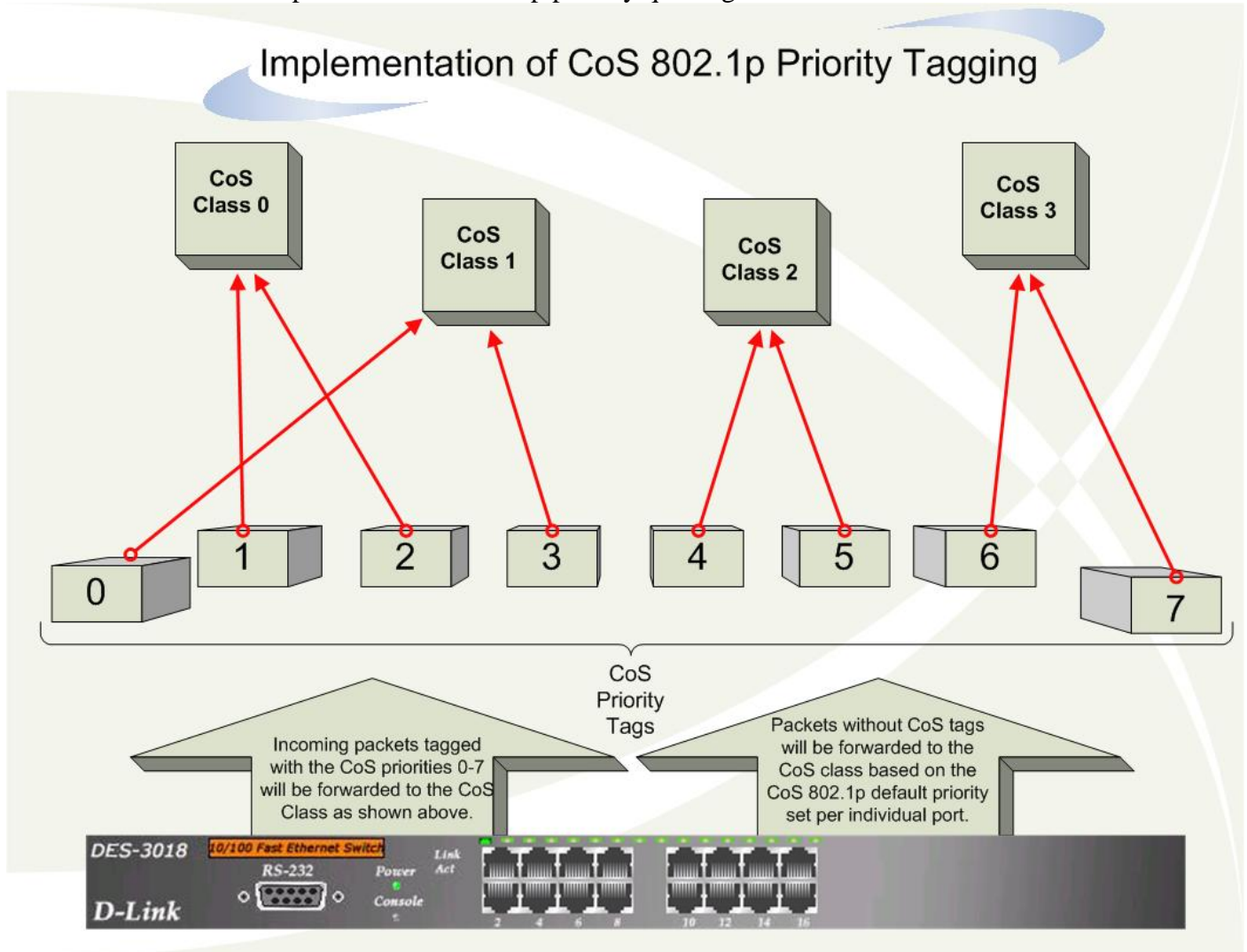
Figure 8- 1. An Example of the Default CoS Mapping on the Switch

The picture above shows the default priority setting for the Switch. Class-3 has the highest priority of the four priority classes of service on the Switch. In order to implement CoS, 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, if 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 CoS

The DES-3000 series switch supports 802.1p priority queuing. The DES-3000 series has 4 priority classes of service. These priority classes of service are numbered from 3 (Class 3) — the highest priority class of service — to 0 (Class 0) — the lowest priority class of service. The eight priority queues specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority classes of service as follows:

- Priority 0 is assigned to the Switch's Q1 class.
- Priority 1 is assigned to the Switch's Q0 class.
- Priority 2 is assigned to the Switch's Q0 class.
- Priority 3 is assigned to the Switch's Q1 class.
- Priority 4 is assigned to the Switch's Q2 class.
- Priority 5 is assigned to the Switch's Q2 class.
- Priority 6 is assigned to the Switch's Q3 class.
- Priority 7 is assigned to the Switch's Q3 class.

Priority scheduling is implemented using two types of methods, strict priority and round-robin priority. If no changes are made to the CoS priority scheduling settings the method used is strict priority.

For strict priority-based scheduling, packets residing in the highest priority class of service are transmitted first. Once a strict scheduling is implemented for CoS, the highest class will work in strict mode and the other classes will remain in a weight fair scheduling mode. Higher priority packets always receive preference regardless of the amount of lower priority packets in the buffer and regardless of the time elapsed since any lower priority packets have been transmitted. By default, the Switch is configured to empty the buffer using strict priority.

NOTICE: The default CoS scheduling arrangement is a strict priority schedule which means the switch will consider the highest class of service to have strict scheduling only, while the other queues empty in a round-robin method. See the **config scheduling_mechanism** command in this section for more information regarding this subject.

To use implement round-robin (weighted) priority, the Switch's four priority classes of service can be configured to reduce the buffer in a round-robin fashion - beginning with the highest priority class of service, and proceeding to the lowest priority class of service before returning to the highest priority classes of service.

The weighted-priority based scheduling alleviates the main disadvantage of strict priority-based scheduling – in that lower priority class of service get starved of bandwidth – by providing a minimum bandwidth to all classes of service for transmission. This is accomplished by configuring the maximum number of packets allowed to be transmitted from a given priority class of service and the maximum amount of time a given priority class of service will have to wait before being allowed to transmit its accumulated packets. This establishes a Class of Service (CoS) for each of the Switch's four hardware priority classes of service.

The possible **weight** value range is: 1 to 55 packets.

In networking environments that use alternative priority protocols, the Switch's CoS can be mapped to accommodate DSCP priority and Type of Service (ToS) priority. CoS can also be mapped to specified destination MAC addresses or ports on the Switch.

Port Bandwidth

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port. To view this table, click **CoS > Port Bandwidth**

Bandwidth Settings

From	To	Type	no_limit	Rate	Apply
Port 1	Port 1	Both	Disabled	64	Apply

Port Bandwidth Table

Port	RX Rate (Kbit/sec)	TX Rate (Kbit/sec)	Effective RX (Kbit/sec)	Effective TX (Kbit/sec)
1	no_limit	no_limit	no_limit	no_limit
2	no_limit	no_limit	no_limit	no_limit
3	no_limit	no_limit	no_limit	no_limit
4	no_limit	no_limit	no_limit	no_limit
5	no_limit	no_limit	no_limit	no_limit
6	no_limit	no_limit	no_limit	no_limit
7	no_limit	no_limit	no_limit	no_limit
8	no_limit	no_limit	no_limit	no_limit
9	no_limit	no_limit	no_limit	no_limit
10	no_limit	no_limit	no_limit	no_limit
11	no_limit	no_limit	no_limit	no_limit
12	no_limit	no_limit	no_limit	no_limit
13	no_limit	no_limit	no_limit	no_limit
14	no_limit	no_limit	no_limit	no_limit
15	no_limit	no_limit	no_limit	no_limit
16	no_limit	no_limit	no_limit	no_limit
17	no_limit	no_limit	no_limit	no_limit
18	no_limit	no_limit	no_limit	no_limit
19	no_limit	no_limit	no_limit	no_limit
20	no_limit	no_limit	no_limit	no_limit
21	no_limit	no_limit	no_limit	no_limit
22	no_limit	no_limit	no_limit	no_limit
23	no_limit	no_limit	no_limit	no_limit
24	no_limit	no_limit	no_limit	no_limit
25	no_limit	no_limit	no_limit	no_limit
26	no_limit	no_limit	no_limit	no_limit

Note: To perform precise bandwidth control, it is required to enable the flow control to mitigate the retransmission of TCP traffic.

Figure 8- 2. Bandwidth Settings and Port Bandwidth Table window

The following parameters can be set or are displayed:

Parameter	Description
From/To	A consecutive group of ports may be configured starting with the selected port.
Type	This drop-down menu allows you to select between *RX* (receive,) *TX* (transmit,) and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
No Limit	This drop-down menu allows you to specify that the selected port will have no bandwidth limit. *Enabled* disables the limit.
Rate	This field allows you to enter the data rate, in Kbit/s, that will be the limit for the selected port. The user may choose a rate between 64 and 1024000 Kbit/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**.

802.1p Default Priority

The Switch allows the assignment of a default 802.1p priority to each port on the Switch.
To view this table click, **CoS > 802.1p Default Priority**

Figure 8- 3. 802.1p Default Priority and the 802.1p Default Priority window

This page allows you 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 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 your settings.

802.1p User Priority

The Switch allows the assignment of a class of service to each of the 802.1p priorities. To view this window click, **CoS** > **802.1p User Priority**

Figure 8- 4. 802.1p User Priority window

Once you have assigned a priority to the port groups on the Switch, you can then assign this Class to each of the four levels of 802.1p priorities. Click **Apply** to set your changes.

CoS Scheduling Mechanism

This drop-down menu allows you to select between a **Weight Fair** and a **Strict** mechanism for emptying the priority classes. To view this window click **CoS > CoS Scheduling Mechanism**

Figure 8- 5. CoS Scheduling Mechanism and CoS Scheduling Mechanism Table window

NOTICE: The default CoS scheduling arrangement is a strict priority schedule for the highest class (Class-3) which means the Switch will consider the highest class of service to have strict scheduling only, while the other queues empty in a round-robin method.

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

Parameter	Description
Strict	Denoting a Strict scheduling will set the highest queue to be emptied first while the other

	queues will follow the weighted round-robin scheduling scheme.
Weight fair	Use the weighted round-robin (*WRR*) algorithm to handle packets in an even distribution in priority classes of service.

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

CoS Output Scheduling

CoS can be customized by changing the output scheduling used for the hardware classes of service in the Switch. As with any changes to CoS 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 you choose to customize this setting, it is important to monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the CoS settings are not suitable. To view this window click **CoS** > **CoS Output Scheduling**

Figure 8- 6. CoS Output Scheduling Configuration window

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

Parameter	Description
Weights	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 1 and 55 can be specified.

Click **Apply** to implement changes made.

Priority Settings

The Priority Setting window will allow users to configure the CoS priority settings on a port per port basis. When CoS tagged packets arrive on the switch, they are mapped to the settings configured here. For example, if a port has been assigned a MAC priority, the packet that has the CoS priority assigned to a MAC address will be sent to the CoS queue configured for that MAC address. Once the configuration has been completed, users may see the results in the Priority Settings Table seen here. After configuring the port priorities, users may adjust the individual CoS settings on the other windows located in the CoS folder of the Switch. To view the following window, click **CoS > Priority Settings**

Priority Setting

From	To	MainSelect	Apply
Port 1	Port 1	none	Apply

Priority Setting Table

Port	Port Priority	Ethernet Priority	IP Priority
1	off	802.1p_priority	off
2	off	802.1p_priority	off
3	off	802.1p_priority	off
4	off	802.1p_priority	off
5	off	802.1p_priority	off
6	off	802.1p_priority	off
7	off	802.1p_priority	off
8	off	802.1p_priority	off
9	off	802.1p_priority	off
10	off	802.1p_priority	off
11	off	802.1p_priority	off
12	off	802.1p_priority	off
13	off	802.1p_priority	off
14	off	802.1p_priority	off
15	off	802.1p_priority	off
16	off	802.1p_priority	off
17	off	802.1p_priority	off
18	off	802.1p_priority	off
19	off	802.1p_priority	off
20	off	802.1p_priority	off
21	off	802.1p_priority	off
22	off	802.1p_priority	off
23	off	802.1p_priority	off
24	off	802.1p_priority	off

Figure 8- 7. Priority Setting

Configure the following Priority Setting parameters:

Parameter	Description
From/To	Users may select a port or group of ports to assign ToS priority settings, based on the following Main Select field.
MainSelect	Select the general priority settings for the ports previously stated using the pull-down menu. Priority option include: **none** – Choosing this option will clear the selected ports form having CoS priority settings. **port_priority** – Choosing this option will assign ports to map CoS priorities to individual ports. **802.1p_priority** - Choosing this option will assign ports to map CoS priorities to 802.1p priorities. **MAC**-**Base -** Choosing this option will assign ports to map CoS priorities to MAC addresses. **tos** - Choosing this option will assign ports to map CoS priorities to ToS priorities. **dscp**- Choosing this option will assign ports to map CoS priorities to DSCP priorities.

Click **Apply** to implement changes made.

TOS Priority Settings

Use the **TOS Priority Settings** menu to configure ToS priority mapping for Class of Service on the Switch. When a packet is received containing this ToS tag, it will be mapped to the CoS queue configured here. These settings will only take effect if the priority settings per port are configured for ToS. To view this table click, **CoS** > **TOS Priority Settings**

Figure 8- 8. TOS Priority Setting

Select the **TOS** value from the pull-down menu and the **Class ID** of the priority level mapped to and click the **Apply** button. The new mapping is displayed in the **Port Priority Table** below.

DSCP Priority Settings

Use the **DSCP Priority Settings** menu to configure DSCP priority mapping for Class of Service on the Switch. When a packet is received containing this DSCP tag, it will be mapped to the CoS queue configured here. These settings will only take effect if at least one of the priority settings per port is configured for DSCP.

Type the **DSCP** bit level and the **Class ID** priority from the pull-down menu mapped to and click the **Apply** button. The new mapping is displayed in the **DSCP Priority Table** below.

To view this table click, **CoS** > **DSCP Priority Settings**

DSCP Priority Settings		
DSCP	Class ID	Apply
	3	Apply

DSCP Priority Table	
DSCP	Class ID
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	0
25	0
26	0
27	0
28	0
29	0
30	0
31	0
32	0
33	0
34	0
35	0
36	0
37	0
38	0
39	0
40	0
41	0
42	0
43	0
44	0
45	0
46	0
47	0
48	0
49	0
50	0
51	0
52	0
53	0
54	0
55	0
56	0
57	0
58	0
59	0
60	0
61	0
62	0
63	0

Figure 8- 9. DSCP Priority Setting

Port Mapping Priority Settings

Use the **Port Mapping Priority Settings** menu to configure priority mapping for Class of Service on the Switch. **Port Mapping Priority CoS** can only be used if it has been previously configured for the selected ports in the **Priority Setting** menu. There are two Class of Service levels available. To view this table click, **CoS** > **Port Mapping Priority Settings**

Figure 8- 10. Port Mapping Priority CoS

Use the **From/To** menu to select the ports being configured, the selected ports must first be configured for port-based priority in the Priority Setting menu. Select the **Class** level for the port(s), there are two levels 3 for high priority and 0 for low priority.

MAC Priority Settings

When using the MAC Priority mechanism, the packet is classified based on the MAC address field priority in the MAC priority table entries.

To configure a destination MAC address for a CoS queue, users must adhere to the following steps:

1. Users must first enter a static destination MAC address into the Forwarding Database (FDB) of the switch. To accomplish this, go to the Unicast Forwarding table in the **Forwarding Filtering** folder under the **Configuration** menu and click on the **Unicast Forwarding** link, which will display a window for users to enter this information.
2. Once a destination MAC has been added to the FDB, users must then configure the appropriate queue to be mapped to this destination MAC address, using the following window.
3. Once the previous parameters are set, users should go to the **Priority Settings** window located in this folder and set the egress ports on the switch to **MAC Priority**. These ports must only be set for MAC Priority and not for any other priority choice. Please be advised that the default priority setting is for 802.1p and users must change the priority to MAC Priority for this function to work properly. Be sure that the device with this destination MAC address is connected to the port for which this priority is configured.

To view this table, click **CoS > MAC Priority**

Figure 8- 11. MAC Priority Setting

Type in the **MAC Address**, select the **Class ID** priority level and click the **Apply** button.

| Section 9 |

CPU Interface Filtering

CPU Interface Filtering State

CPU Interface Filtering Table

CPU Interface Filtering

Due to needed extra switch security, the DES-3000 switch series 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. 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 DES-3000 switch series 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. Choose **Enabled** to enable CPU packets to be scrutinized by the Switch and **Disabled** to disallow this scrutiny. To access this window, click **CPU Interface Filtering > CPU Interface Filtering State**

Figure 9- 1. 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 individual entry, click the hyperlinked **Profile ID** number. To view this table click, **CPU Interface Filtering** > **CPU Interface Filtering Table**

Figure 9- 2. CPU Interface Filtering Table

To add an entry to the **CPU Interface Filtering Table**, click the **Add** button. This will open the **CPU Interface Filtering 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 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 9- 3. CPU Interface Filtering Configuration window – Ethernet

Parameter	Description
Profile ID (1-3)	Type in a unique identifier number for this profile set. This value can be set from 1 - 3.
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	Selecting this option instructs the Switch to examine the 802.1p type value in each frame's

	header.
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.

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

Figure 9- 4. CPU Interface Filtering Configuration window- IP

Parameter	Description
Profile ID (1-3)	Type in a unique identifier number for this profile set. This value can be set from 1 - 3.
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 that you specify a source port mask and/or a destination port mask. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between **urg** (urgent), **ack** (acknowledgement), **psh** (push), **rst** (reset), **syn** (synchronize), **fin** (finish).
	• **src port mask** - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter.
	• **dest 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).
	• **dest 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 0x0-0xffffffff).

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

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

Figure 9- 5. CPU Interface Filtering Configuration window- Packet Content
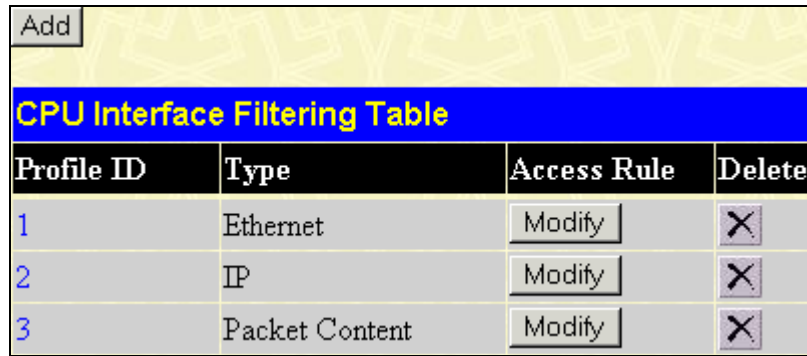
This screen will aid the user in configuring the Switch to mask packet headers beginning with the offset value specified. The following fields are used to configure the **Packet Content Mask**:

Parameter	Description
Profile ID (1-3)	Type in a unique identifier number for this profile set. This value can be set from 1 - 3.
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 establish the rule for a previously created CPU Access Profile:
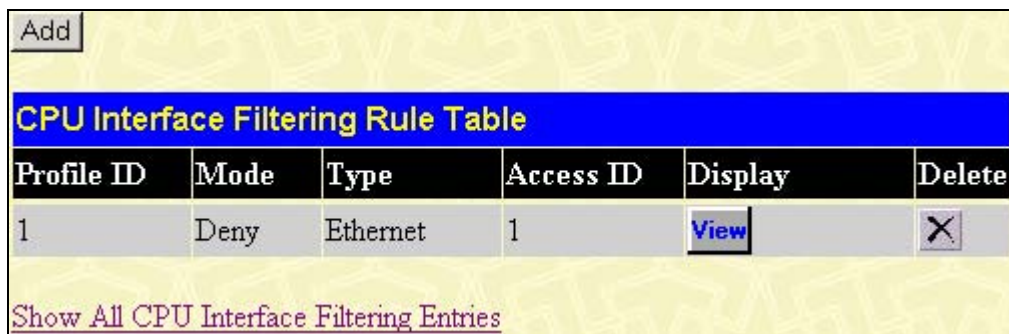
In the **CPU interface** folder, click the **CPU Interface Filtering State** link to open the **CPU Interface Filtering Table**.

Figure 9- 6. 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** and **Packet Content**. Each entry will open a new and unique window, as shown in the examples below.
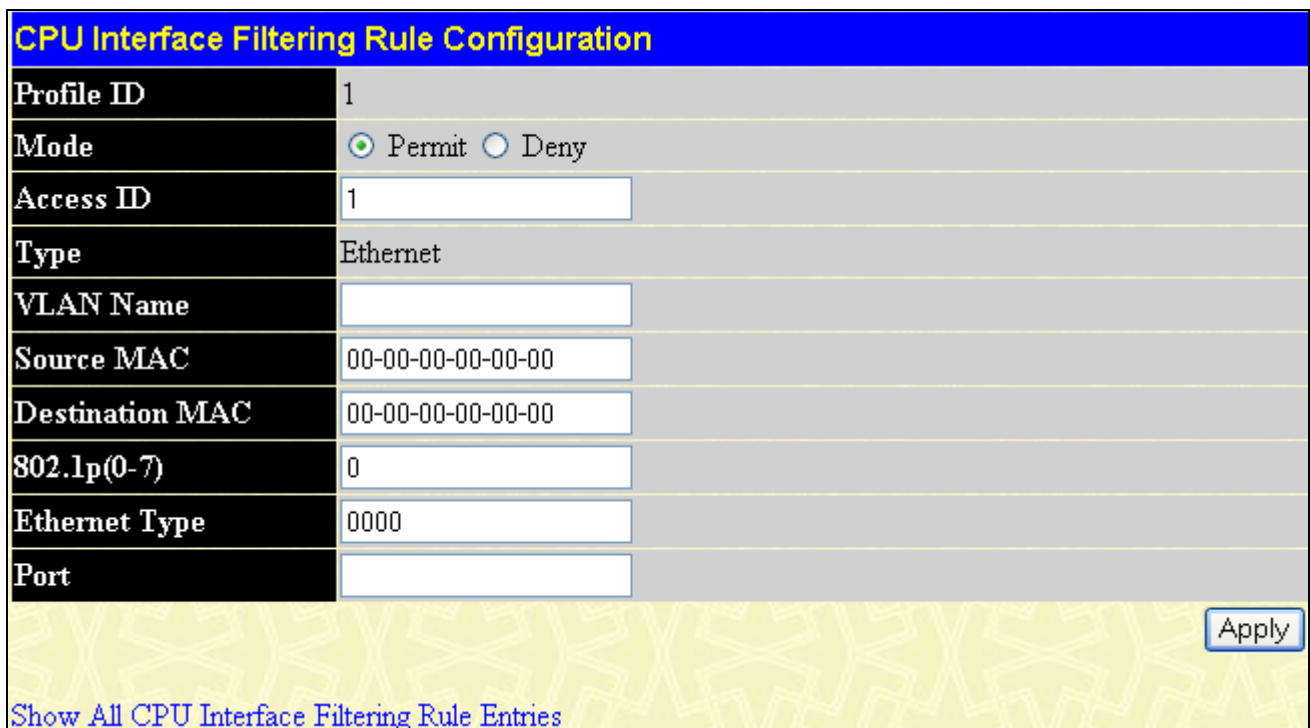
Figure 9- 7. CPU Interface Filtering Table – Ethernet

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

Figure 9- 8. CPU Interface Filtering Rule Configuration – Ethernet

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

Parameters	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select *Permit* to specify that 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 and priority. This value can be set from 1 - 5.
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	Specifies that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type	Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value (hex 0x0-0xffff) in the packet header. The Ethernet type value may be set in the form: hex 0x0-0xffff, which means the user may choose any combination of letters and numbers ranging from a-f and from 0-9999.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the Switch into this field. Entering *all* will denote all ports on the Switch.

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

Figure 9- 9. CPU Interface Filtering Rule Display – Ethernet

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

Figure 9- 10. CPU Interface Filtering Rule Table – IP

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

Figure 9- 11. 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 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 - 5.
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)	Enter the DSCP bit for which to identify incoming packets. The user may choose a DSCP bit between 0-63.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the Switch into this field. Entering *all* will denote all ports 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 9- 12. CPU Interface Filtering Rule Display - IP

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

Figure 9- 13. 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** button:

Figure 9- 14. CPU Interface Filtering Rule Configuration - Packet Content

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

Parameters	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that 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 - 5.
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.*

131

	• *value (32-47)* - Enter a value in hex form to mask the packet from byte 32 to byte 47.
	• *value (48-63)* - Enter a value in hex form to mask the packet from byte 48 to byte 63.
	• *value (64-79)* - Enter a value in hex form to mask the packet from byte 64 to byte 79.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the Switch into this field. Entering *all* will denote all ports 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:

CPU Interface Filtering Rule Display

Profile ID	3
Access ID	1
Mode	Permit
Type	Packet Content
Offset 0-15	0x00000000 0x00000000 0x00000000 0x00000000
Offset 16-31	---------
Offset 32-47	---------
Offset 48-63	---------
Offset 64-79	---------
Port	2

Show All CPU Interface Filtering Rule Entries

Figure 9- 15. CPU Interface Filtering Rule Display – Packet Content

| Section 10 |

Security

Traffic Control

Port Security

Port Lock Entries

802.1X

Trusted Host

Traffic Segmentation

SSH

The following section will aid the user in configuring security functions for the Switch. The Switch includes various functions for security, including ***Traffic Control, Port Security, Port Lock Entries, 802.1X, Trusted Host, Traffic Segmentation*** and *SSH* all discussed in detail in the following section.

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 end station 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.

Traffic Trap Configuration

Traffic Trap	None ▾	Apply

Traffic Control Settings

From	To	Broadcast Storm	Multicast Storm	Unicast Storm	Threshold	Action	Count Down	Interval	Apply
Port 1 ▾	Port 1 ▾	Disabled ▾	Disabled ▾	Disabled ▾	128	Drop ▾	5	5	Apply

Traffic Control Table

Port	Broadcast Storm	Multicast Storm	Unicast Storm	Threshold (Kbit/sec)	Action	Count Down	Interval	Forever
1	Disabled	Disabled	Disabled	64	Drop	0	5	
2	Disabled	Disabled	Disabled	64	Drop	0	5	
3	Disabled	Disabled	Disabled	64	Drop	0	5	
4	Disabled	Disabled	Disabled	64	Drop	0	5	
5	Disabled	Disabled	Disabled	64	Drop	0	5	
6	Disabled	Disabled	Disabled	64	Drop	0	5	
7	Disabled	Disabled	Disabled	64	Drop	0	5	
8	Disabled	Disabled	Disabled	64	Drop	0	5	
9	Disabled	Disabled	Disabled	64	Drop	0	5	
10	Disabled	Disabled	Disabled	64	Drop	0	5	
11	Disabled	Disabled	Disabled	64	Drop	0	5	
12	Disabled	Disabled	Disabled	64	Drop	0	5	
13	Disabled	Disabled	Disabled	64	Drop	0	5	
14	Disabled	Disabled	Disabled	64	Drop	0	5	
15	Disabled	Disabled	Disabled	64	Drop	0	5	
16	Disabled	Disabled	Disabled	64	Drop	0	5	
17	Disabled	Disabled	Disabled	64	Drop	0	5	
18	Disabled	Disabled	Disabled	64	Drop	0	5	
19	Disabled	Disabled	Disabled	64	Drop	0	5	
20	Disabled	Disabled	Disabled	64	Drop	0	5	
21	Disabled	Disabled	Disabled	64	Drop	0	5	
22	Disabled	Disabled	Disabled	64	Drop	0	5	
23	Disabled	Disabled	Disabled	64	Drop	0	5	
24	Disabled	Disabled	Disabled	64	Drop	0	5	
25	Disabled	Disabled	Disabled	64	Drop	0	5	
26	Disabled	Disabled	Disabled	64	Drop	0	5	

Figure 10- 1. Traffic Control Settings window

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 **Count Down** field. Although the Count Down field can be specified, users are advised to disable this feature and assess the situation before recovering the port. The Count Down field may be disabled by entering a value of 0 (zero).

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 user may recover the affected ports by using the Traffic Control Recover section of the previous window and recover the ports shutdown forever. 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 any unknown storms. To view the window above, click **Security > Traffic Control**:

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

Parameter	Description
Traffic Control Recover	
From… To	Select the ports to be recovered from being "Shutdown Forever" by the shutdown action of this feature.
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 Storm	Enables or disable Broadcast Storm Control.
Multicast Strom	Enables or disables Multicast Storm Control.
Unicast Storm	Enables or disables Unknown Unicast storm control.
Threshold	Specifies the number of broadcast/multicast/unicast packets, in Kbps (Kilo bit per seconds), received by the Switch that will trigger the Traffic Control function to commence. The configurable threshold range is from 64-1024000 with a default setting of 64.
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. *Shut Down* – 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.
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. 5 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 ports' (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**

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

Port Security Table			
Port	**Admin State**	**Max.Learning Addr**	**Lock Address Mode**
1	Disabled	1	DeleteOnTimeout
2	Disabled	1	DeleteOnTimeout
3	Disabled	1	DeleteOnTimeout
4	Disabled	1	DeleteOnTimeout
5	Disabled	1	DeleteOnTimeout
6	Disabled	1	DeleteOnTimeout
7	Disabled	1	DeleteOnTimeout
8	Disabled	1	DeleteOnTimeout
9	Disabled	1	DeleteOnTimeout
10	Disabled	1	DeleteOnTimeout
11	Disabled	1	DeleteOnTimeout
12	Disabled	1	DeleteOnTimeout
13	Disabled	1	DeleteOnTimeout
14	Disabled	1	DeleteOnTimeout
15	Disabled	1	DeleteOnTimeout
16	Disabled	1	DeleteOnTimeout
17	Disabled	1	DeleteOnTimeout
18	Disabled	1	DeleteOnTimeout
19	Disabled	1	DeleteOnTimeout
20	Disabled	1	DeleteOnTimeout
21	Disabled	1	DeleteOnTimeout
22	Disabled	1	DeleteOnTimeout
23	Disabled	1	DeleteOnTimeout
24	Disabled	1	DeleteOnTimeout

Figure 10- 2. Port Security Settings and Table window

The following parameters can be set:

Parameter	Description
From/To	A consecutive group of ports may be configured starting with the selected port.

Admin State	This pull-down menu allows you to enable or disable Port Security (locked MAC address table for the selected ports).
Max. Addr(0-10)	The number of MAC addresses that will be in the MAC address forwarding table for the selected switch and group of ports.
Lock Address Mode	This pull-down menu allows you to select how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are: • *Permanent* – The locked addresses will not age out after the aging timer expires. • *DeleteOnTimeout* – The locked addresses will age out after the aging timer expires. • *DeleteOnReset* – The locked addresses will not age out until the Switch has been reset.

Click **Apply** to implement changes made.

NOTE: The uplink module ports (DES-3010F/FL/G ports 9-10, DES-3018 ports 17-18, DES-3026 ports 25-26) do not support the port security function.

Port Lock 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 the following window, click **Security > Port Lock Entries**

Figure 10- 3. Port Lock Entries Table

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

Parameter	Description
VID	The VLAN ID of the entry in the forwarding database table that has been 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 *Secured_Permanent* can be deleted.
Delete	Click the ⊠ in this field to delete the corresponding MAC address that was permanently learned by the Switch.

802.1X

802.1X Port-Based and MAC-Based Access Control

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server. The following figure represents a basic EAPOL packet:
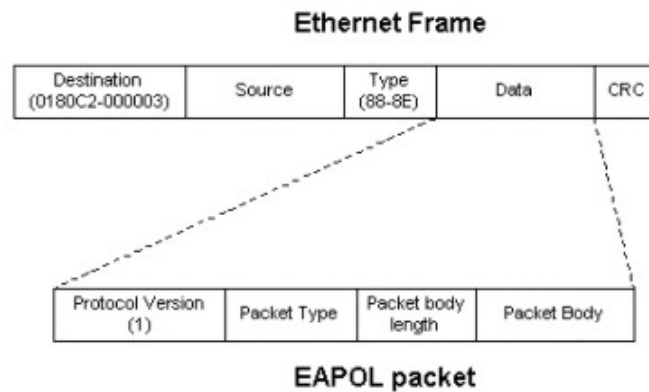
Figure 10- 4. The EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X Access Control method has three roles, each of which are vital to creating and maintaining a stable and working Access Control security method.
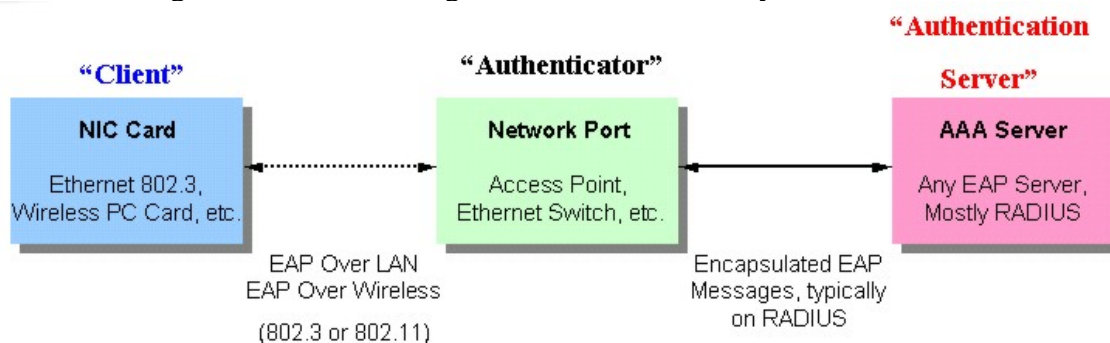
Figure 10- 5. The three roles of 802.1X

The following section will explain the three roles of Client, Authenticator and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or switches services.
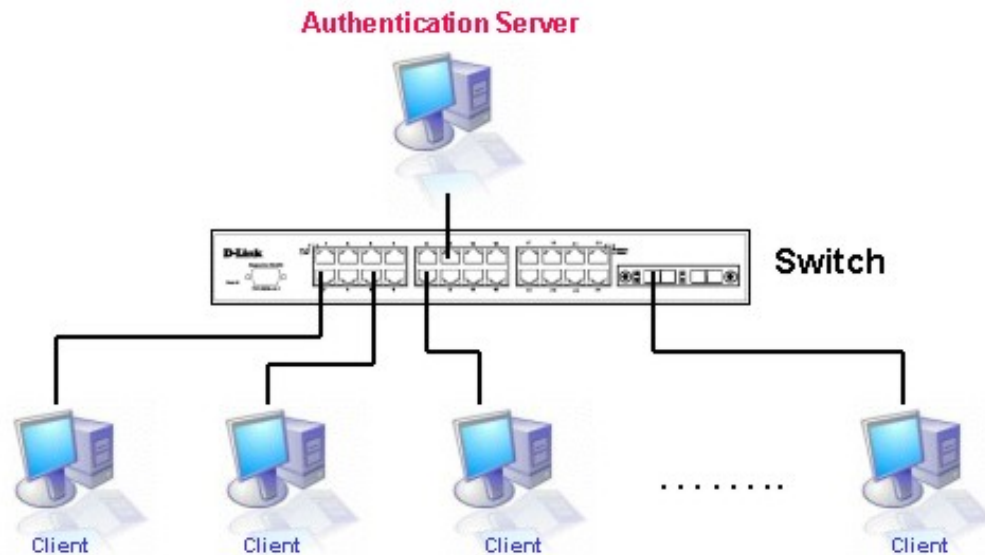
Figure 10- 6. The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator server has two purposes when utilizing 802.1X. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

Three steps must be implemented on the Switch to properly configure the Authenticator.

1. The 802.1X State must be *Enabled*.

2. The 802.1X settings must be implemented by port.

3. A RADIUS server must be configured on the Switch.
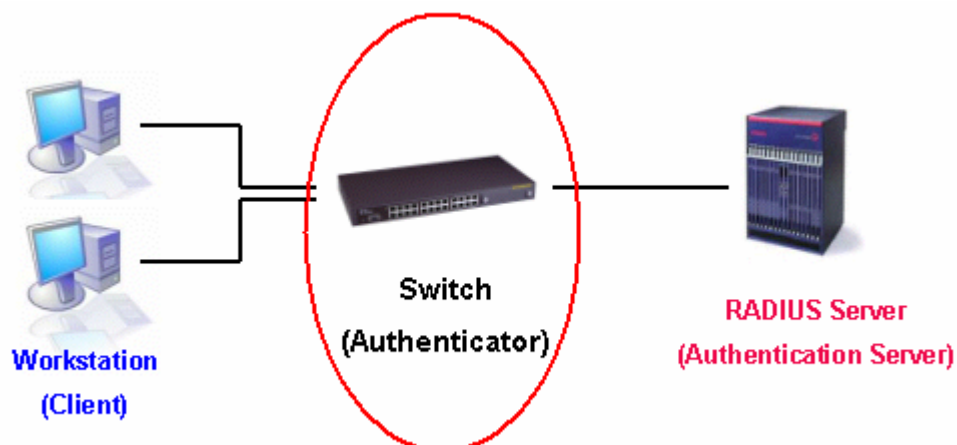
Figure 10- 7. The Authenticator

Client

The Client is simply the end station that wishes to gain access to the LAN or switch services. All end stations must be running software that is compliant with the 802.1X protocol. For users running Windows XP, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.
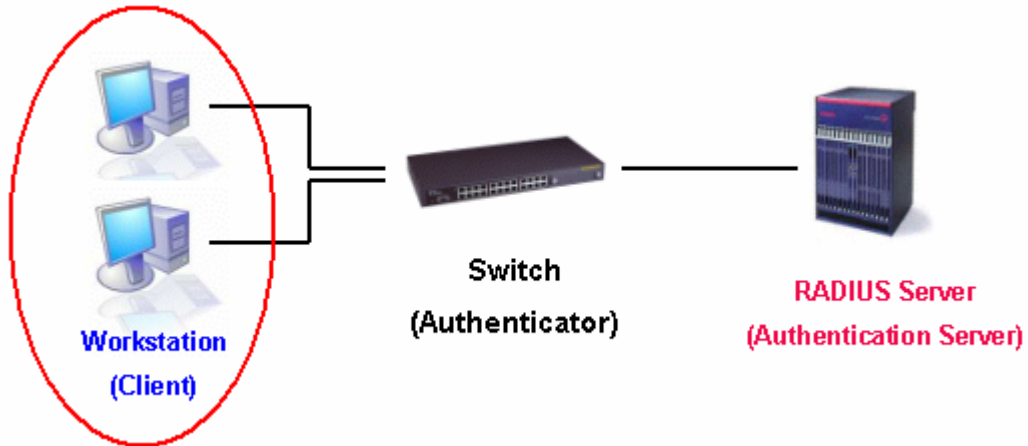
Figure 10- 8. The Client

Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is "locked" until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully "unlocks" the port. Once the port is unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.

Figure 10- 9. The 802.1X Authentication Process

The D-Link implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:
1. Port-Based Access Control – This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
2. MAC-Based Access Control – Using this method, the Switch will automatically learn up to eight MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1X Port-based and MAC-based Network Access Control

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

Port-Based Network Access Control
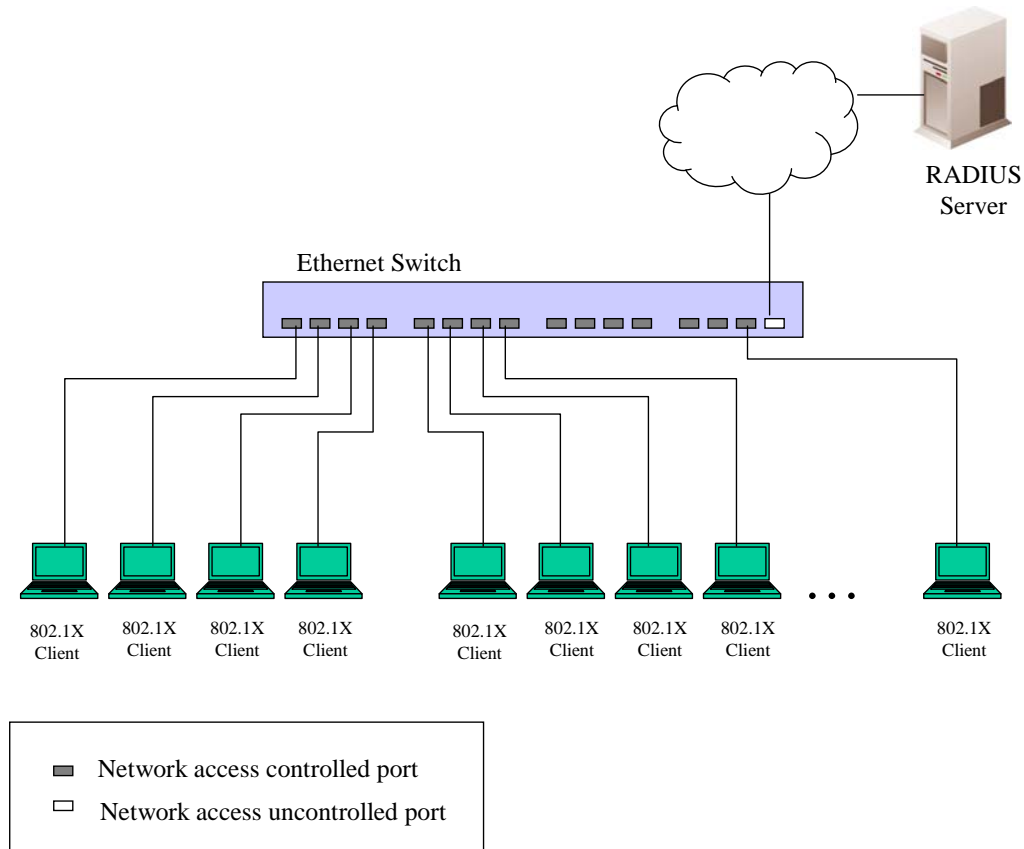
Figure 10- 10. Example of Typical Port-Based Configuration

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

MAC-Based Network Access Control
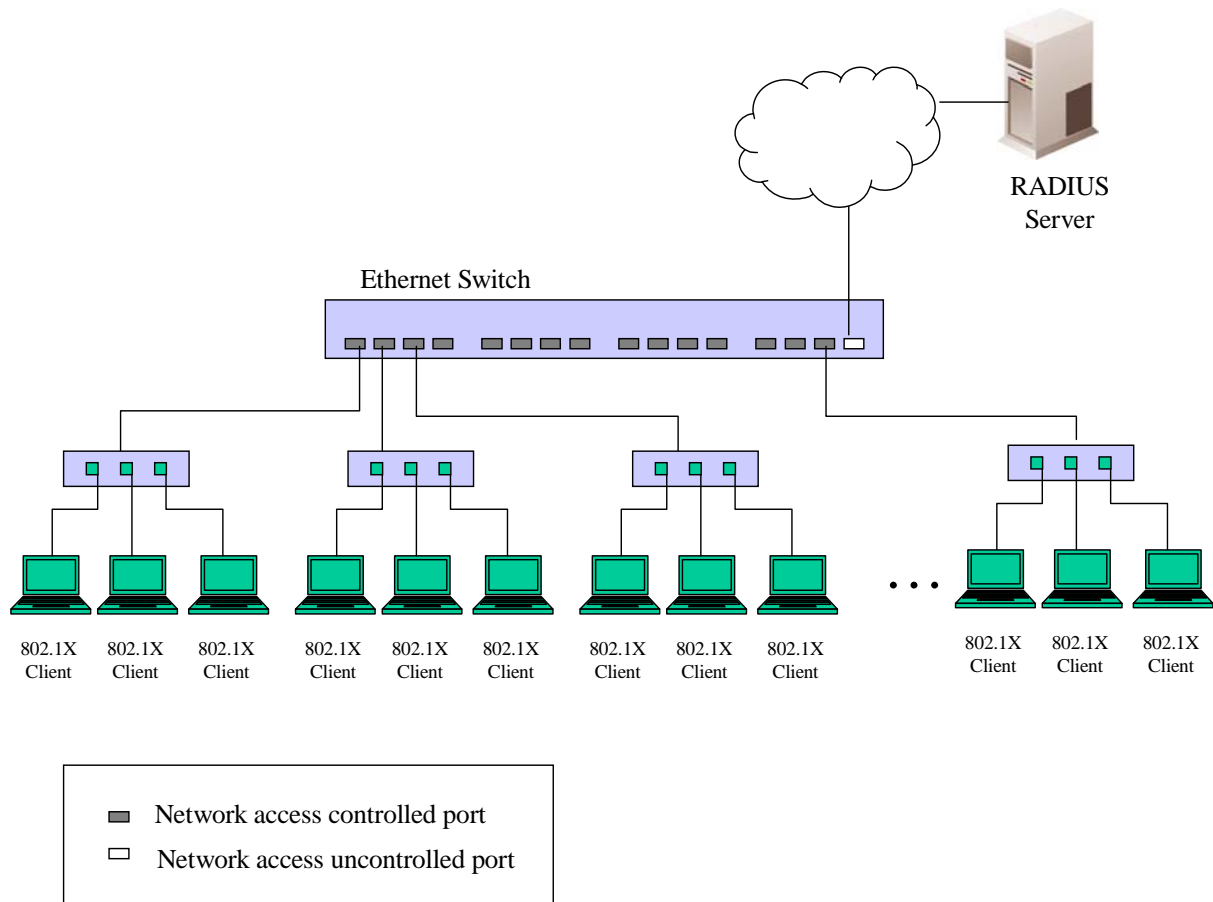
Figure 10- 11. Example of Typical MAC-Based Configuration

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

802.1X Authenticator Settings

To configure the 802.1X authenticator settings, click **Security > 802.1X > 802.1X Authenticator Settings**

Port	AdmDir	Ctrl Stat	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled	Forward EAPOL PDU
1	both	auto	30	60	30	30	2	3600	no	Disabled
2	both	auto	30	60	30	30	2	3600	no	Disabled
3	both	auto	30	60	30	30	2	3600	no	Disabled
4	both	auto	30	60	30	30	2	3600	no	Disabled
5	both	auto	30	60	30	30	2	3600	no	Disabled
6	both	auto	30	60	30	30	2	3600	no	Disabled
7	both	auto	30	60	30	30	2	3600	no	Disabled
8	both	auto	30	60	30	30	2	3600	no	Disabled
9	both	auto	30	60	30	30	2	3600	no	Disabled
10	both	auto	30	60	30	30	2	3600	no	Disabled
11	both	auto	30	60	30	30	2	3600	no	Disabled
12	both	auto	30	60	30	30	2	3600	no	Disabled
13	both	auto	30	60	30	30	2	3600	no	Disabled
14	both	auto	30	60	30	30	2	3600	no	Disabled
15	both	auto	30	60	30	30	2	3600	no	Disabled
16	both	auto	30	60	30	30	2	3600	no	Disabled
17	both	auto	30	60	30	30	2	3600	no	Disabled
18	both	auto	30	60	30	30	2	3600	no	Disabled
19	both	auto	30	60	30	30	2	3600	no	Disabled
20	both	auto	30	60	30	30	2	3600	no	Disabled
21	both	auto	30	60	30	30	2	3600	no	Disabled
22	both	auto	30	60	30	30	2	3600	no	Disabled
23	both	auto	30	60	30	30	2	3600	no	Disabled
24	both	auto	30	60	30	30	2	3600	no	Disabled

Figure 10- 12. 802.1X Authenticator Settings window

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

Figure 10- 13. 802.1X Authenticator Settings – Modify window

This screen allows you to set the following parameters:

Parameter	Description
From……To	Use the drop down menu to enter the port or ports to be set.
AdmDir	Sets the administrative-controlled direction to either *in* or *both*. If *in* is selected, control is only exerted over incoming traffic through the port you selected in the first field. If *both* is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.
PortControl	This allows you to control the port authorization state. Select *forceAuthorized* to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client. If *forceUnauthorized* is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface. If *Auto* is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The default setting is *Auto*.
TxPeriod	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 you to set the number of seconds that the Switch remains in the quiet

147

	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 re-authentication of the client. The default setting is 3600 seconds.
ReAuth	Determines whether regular re-authentication will take place on this port. The default setting is *Disabled*.
Forward EAPOL PDU Both	This function allows the user to *Enable* or *Disable* the EAPOL PDU received by the port.

Click **Apply** to implement your configuration changes. To view configurations for the **802.1X Authenticator Settings** on a port-by-port basis, click the link Show Authenticators Setting.

Local Users

To configure Local Users for 802.1X, click **Security > 802.1X > Local Users.** This window will allow the user to set different 802.1X local users on the Switch.

Figure 10- 14. 802.1X Local User Table Configuration and 802.1X Local User Table window

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

802.1X Capability Settings

Click **Security > 802.1X > 802.1X Capability Settings** to view the following window:

Figure 10- 15. 802.1X Capability Settings and Table window

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

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

150

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 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 802.1X Guest VLANs. These VLANs should have limited access rights and features separate from other VLANs on the network.

To implement 802.1X Guest 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 possesses 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.
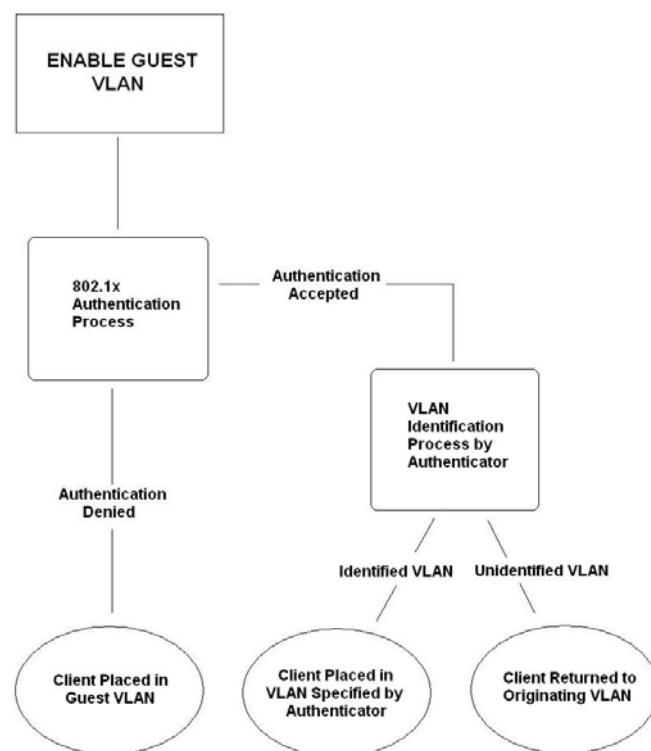
Figure 10- 16. Guest VLAN Authentication Process

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.

Configure 802.1X Guest VLAN

To set a Guest 802.1X VLAN, the user must first configure a normal VLAN which can be enabled here for Guest VLAN status. To view this window, click **Security** > **802.1X** > **Configure 802.1X Guest VLAN**, which will display the following window for the user to configure.

Figure 10- 17. 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. Click the Delete check box to remove the selected VLAN from being an 802.1X Guest VLAN.
Operation	The user has three 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.
	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.

Initializing Ports for Port Based 802.1X

Existing 802.1X port and MAC settings are displayed and can be configured using the window below.
To view the following window, click **Security > 802.1X > Initialize Port(s)**

Figure 10- 18. Initialize Port window

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

Parameter	Description
From and To	Select ports to be initialized.
Port	A read only field indicating a port on the Switch.
MAC Address	The MAC address of the Switch connected to the corresponding port, if any.
Auth PAE State	The Authenticator PAE State will display one of the following: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth* or *ForceUnauth*.
Backend_State	The Backend Authentication State will display one of the following: *Request, Response, Success, Fail, Timeout, Idle* or *Initialize.*
Open Dir	The Operational Controlled Directions are *both* and *in*.
PortStatus	The status of the controlled port can be *Authorized* or *Unauthorized.*

Initializing Ports for MAC Based 802.1X

To initialize ports for the MAC side of 802.1X, the user must first enable 802.1X by MAC address in the **Advanced Settings** window. To view the following window, click **Security > 802.1X > Initialize Port(s)**

Figure 10- 19. Initialize Ports (MAC based 802.1X)

To initialize ports, first choose the range of ports in the **From** and **To** field. Then the user must specify the MAC address to be initialized by entering it into the **MAC Address** field and checking the corresponding check box. To begin the initialization, click **Apply**.

NOTE: The user must first globally enable 802.1X in the **DES-3026 Web Management Tool** window before reauthenticating ports. Information in the **Initialize Ports Table** cannot be viewed before enabling 802.1X.

NOTE: The uplink module ports (DES-3010F/FL/G ports 9-10, DES-3018 ports 17-18, DES-3026 ports 25-26) do not support the 802.1X function.

Reauthenticate Port(s) for Port Based 802.1X

This window allows you to reauthenticate a port or group of ports by choosing a port or group of ports by using the pull down menus **From** and **To** and clicking **Apply**. The **Reauthenticate Port Table** displays the current status of the reauthenticated port(s) once you have clicked **Apply.**
To view the following window, click **Security > 802.1X > Reauthenticate Port(s)**

Figure 10- 20. Reauthenticate Port and Reauthenticate Port Table window

This window displays the following information:

Parameter	Description
Port	The port number of the reauthenticated port.
Auth State	The Authenticator State will display one of the following: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth* or *ForceUnauth.*
BackendState	The Backend State will display one of the following: *Request, Response, Success, Fail, Timeout, Idle* or *Initialize.*
OpenDir	The Operational Controlled Directions are *both* and *in.*
PortStatus	The status of the controlled port can be *Authorized* or *Unauthorized.*

NOTE: The user must first globally enable 802.1X in the **DES-3026 Web Management Tool** window before reauthenticating ports. Information in the **Reauthenticate Ports Table** cannot be viewed before enabling 802.1X.

NOTE: The uplink module ports (DES-3010F/G ports 9-10, DES-3018 ports 17-18, DES-3026 ports 25-26) do not support the 802.1X function.

Reauthenticate Port(s) for MAC-based 802.1X

To reauthenticate ports for the MAC side of 802.1X, the user must first enable 802.1X by MAC address in the **Advanced Settings** window. To view the following window, click **Security > 802.1X > Reauthenticate Port(s)**

Figure 10- 21. Reauthenticate Ports – MAC based 802.1X

To reauthenticate ports, first choose the range of ports in the **From** and **To** field. Then the user must specify the MAC address to be reauthenticated by entering it into the **MAC Address** field and checking the corresponding check box. To begin the reauthentication, click **Apply**.

RADIUS Server

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

To view the following window, click **Security > 802.1X > RADIUS Server**

Figure 10- 22. 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.
Timeout (1-255 secs)	This value determines timeout conditions of the RADIUS Server. The default setting is *5* seconds.
Retransmit (1-255)	Set the Retransmit of the RADIUS Server. The default value is *2*.
Key	Set the key the same as that of the RADIUS server.
Confirm Key	Confirm the shared key is the same as that of the RADIUS server.
Status	This allows you to set the RADIUS Server as *Valid* (Enabled) or *Invalid* (Disabled).

Click **Apply** to implement changes made.

Trusted Host

To view the Trusted Host table, click **Security** > **Trusted Host**

Figure 10- 23. Security IP Management menu

Use the **Security IP Management** to permit remote stations to manage the Switch. If you choose to define one or more designated management stations, only the chosen stations, as defined by IP address and Subnet Mask, will be allowed management privilege through the web manager or Telnet session. To define a management station IP setting, type in the IP address and click the **Apply** button. Click **Del All** to remove all IP addresses configured from being Trusted Hosts.

Traffic Segmentation

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

To view this window, click **Security** > **Traffic Segmentation**

Port	Configuration	Setup
Port 1 ▾	View	Setup

Current Traffic Segmentation Table

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

Figure 10- 24. Current Traffic Segmentation Table

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

Figure 10- 25. Setup Forwarding Ports window

This page allows you to determine which port on a given switch in a switch stack will be allowed to forward packets to other ports on that switch. Configuring traffic segmentation on the Switch is accomplished in two parts. First, you specify a port from that switch, using the **Port** pull-down menu. Then specify the different ports that you want to be able to receive packets from the port you specified in the first part.

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

The **Port** drop-down menu allows you to select a port from that switch. This is the port that will be transmitting packets.

The **Forward Port** click boxes allow you to select which of the ports on the selected switch will be able to forward packets. These ports will be allowed to receive packets from the port specified above.

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

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

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 Server Configuration

The following window is used to configure and view settings for the SSH server and can be opened by clicking **Security > SSH > SSH Server Configuration**

Figure 10- 26. SSH Server Configuration and SSH Server Configuration Settings window

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

Parameter	Description
SSH Server Status	Use the pull-down menu to enable or disable SSH on the Switch. The default is *Disabled*.
Max Session (1-8)	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*.
Listened Port Number	Enter the virtual port number to be used with this feature. The common port number for SSH is 22.

SSH Authentication Mode and Algorithm Settings

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 10- 27. SSH Server Authentication Mode and Algorithm Settings 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**

(Note:Maximum of 8 entries.)

SSH User Authentication Mode

User Name	Auth. Mode	Host Name	Host IP
RG	Password		

Figure 10- 28. SSH User Authentication Mode window

In the example screen above, the User Account "RG" has been previously set using the User Accounts window in the Administration 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.

User Account Add Table

User Name	
New Password	
Confirm New Password	
Access Right	Admin

Apply

Show All User Account Entries

Figure 10- 29. SSH User Configuration

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

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

(Note:Maximum of 8 entries.)

SSH User Authentication Mode

User Name	Auth. Mode	Host Name	Host IP
RG	Password		

Figure 10- 30. 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:

Figure 10- 31. SSH User Authentication - Edit window

The user may set the following parameters:

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

Click **Apply** to implement changes made.

Section 11

Monitoring

CPU Utilization

Port Utilization

Packets

Packet Errors

Packet Size

VLAN Status

MAC Address

Switch Log

Log Settings

IGMP Snooping Group

Browse Router Port

Browse ARP Table

Session Table

Port Access Control

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 this window click **Monitoring** > **CPU Utilization**

Figure 11- 1. CPU Utilization graph

To view the CPU utilization by port, use the real-time graphic of the Switch at the top of the web page by simply clicking on a port. Click **Apply** to implement the configured settings. Click **Clear** to automatically refresh with new updated statistics.

The information is described 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.
Show / Hide	Check whether or not to display CPU utilization for five seconds, one minute or five minutes.

Port Utilization

The **Port Utilization** page displays the percentage of the total available bandwidth being used on the port. To view the port utilization, click **Monitoring** > **Port Utilization**
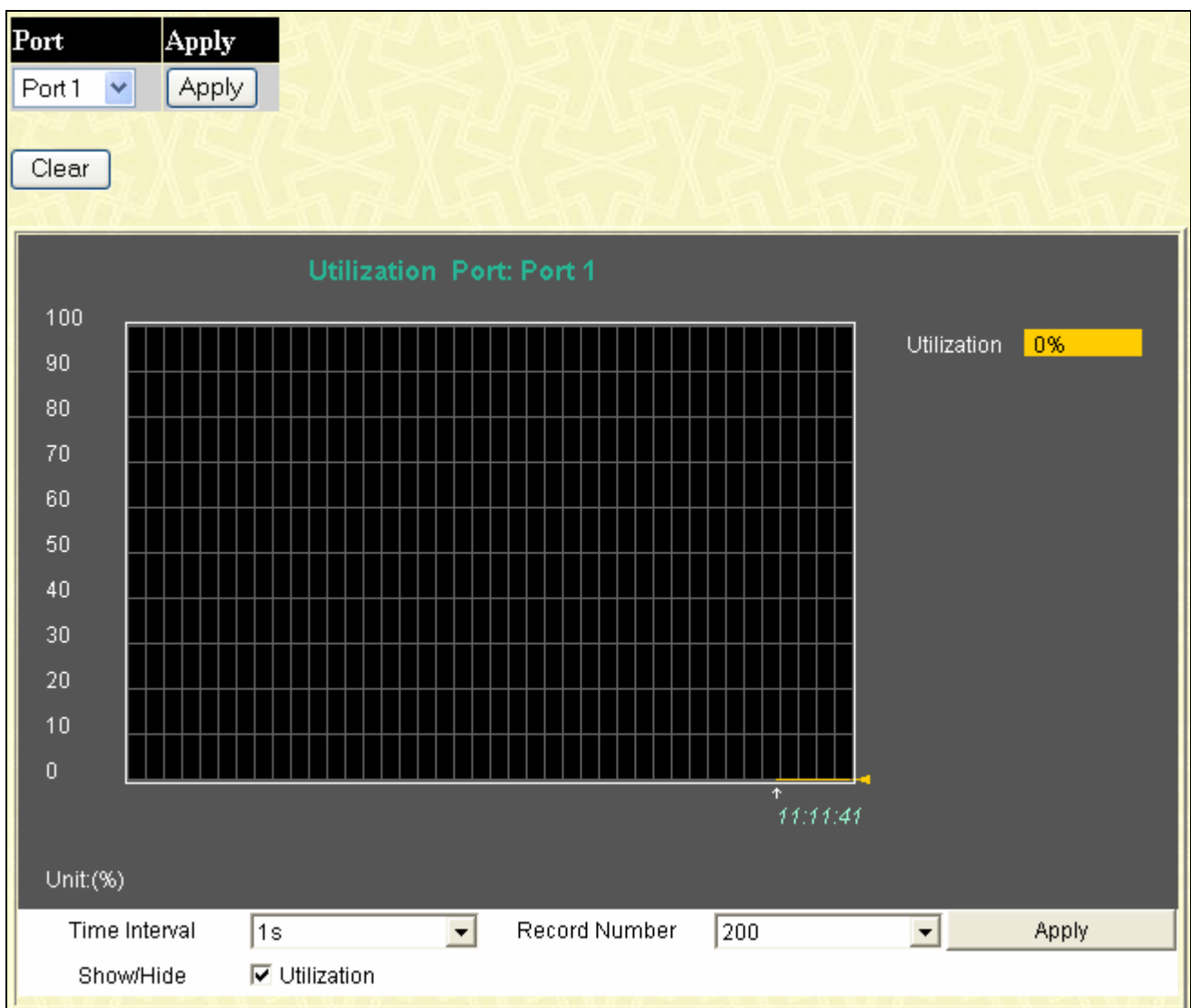
Figure 11- 2. Port Utilization window

The user may use the real-time graphic of the Switch at the top of the web page to view utilization statistics per port by clicking on a port. The following field can be set:

166

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

Click **Clear** to refresh the graph. Click **Apply** to implement changes made.

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)

This table is used to view the graph of packets received on the Switch. To select a port to view these statistics for, use the **Port** pull down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port. To view this window, click **Monitoring** > **Packets** > **Received (RX)**

Figure 11- 3. Rx Packets Analysis window (line graph for Bytes and Packets)

To view the **Received Packets Table**, click the link View Table, which will show the following table:
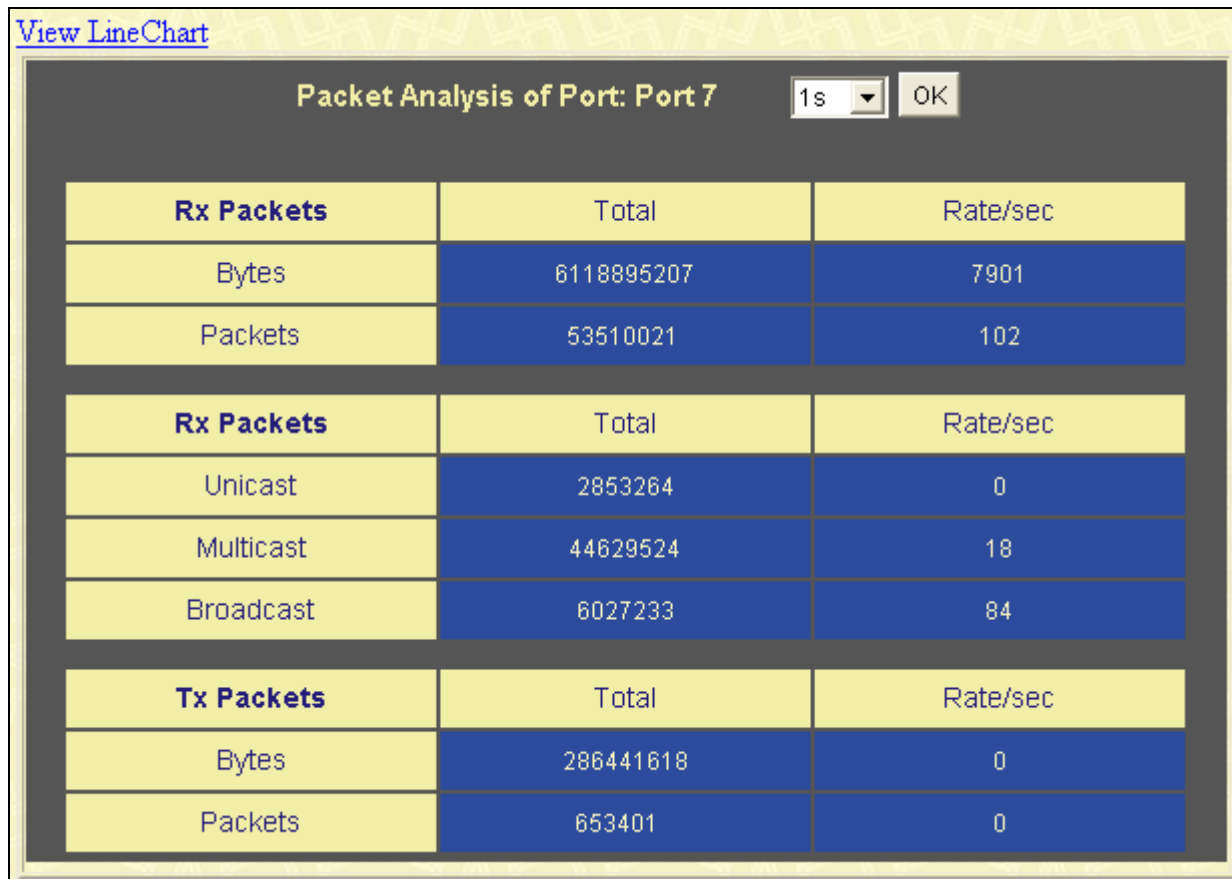
Figure 11- 4. Rx Packets Analysis Table

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)

The following graph displays the Unicast, Multicast and Broadcast packets received on the Switch. To select a port to view these statistics for, use the **Port** pull down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port. To view this graph, click **Monitoring** > **Packets** > **UMB Cast(RX)**

Figure 11- 5. Rx Packets Analysis window (line graph for Unicast, Multicast, and Broadcast Packets)

To view the **UMB Cast Table**, click the View Table link, which will show the following table:
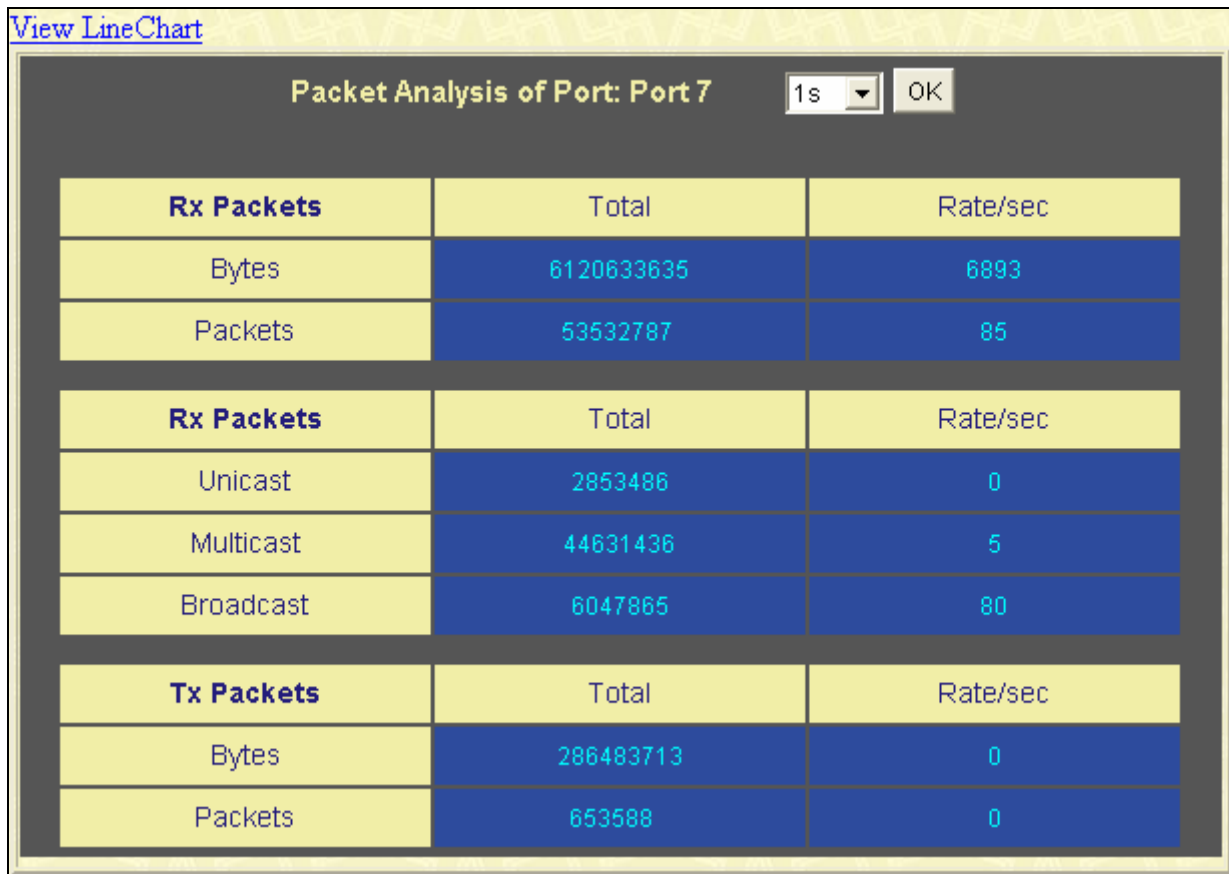
Figure 11- 6. Rx Packets Analysis window (table for Unicast, Multicast, and Broadcast Packets)

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)

Transmitted (TX) table allows the user to view the packets transmitted from the Switch. To view statistics for a specific port, use the **Port** pull down menu. The user may also use the real-time graphic, at the top of the web page by simply clicking on a port. To view this graph, click **Monitoring** > **Packets** > **Transmitted(TX)**
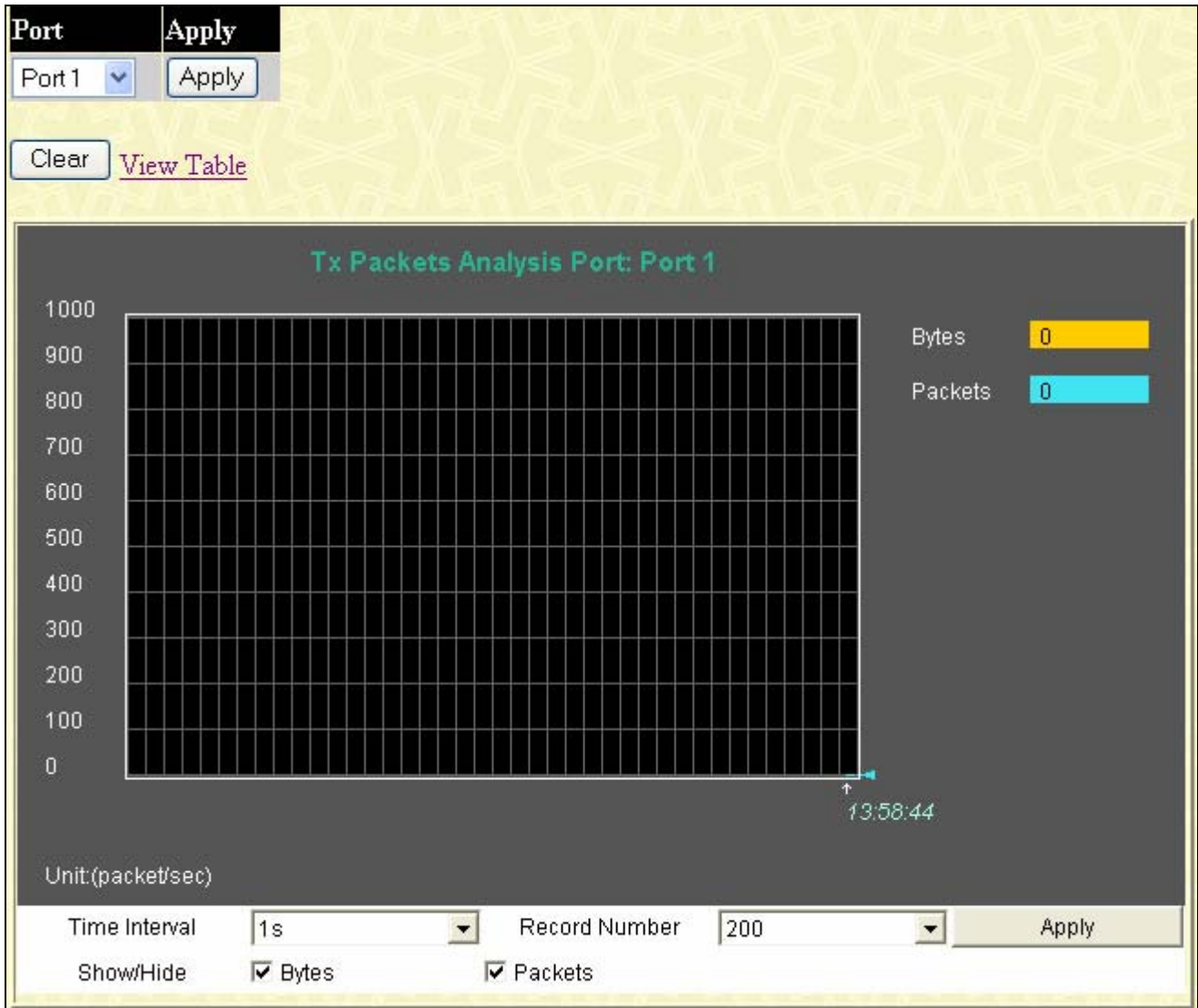
Figure 11- 7. Tx Packets Analysis window (line graph for Bytes and Packets)

To view the **Transmitted (TX) Table**, click the link View Table, which will show the following table:
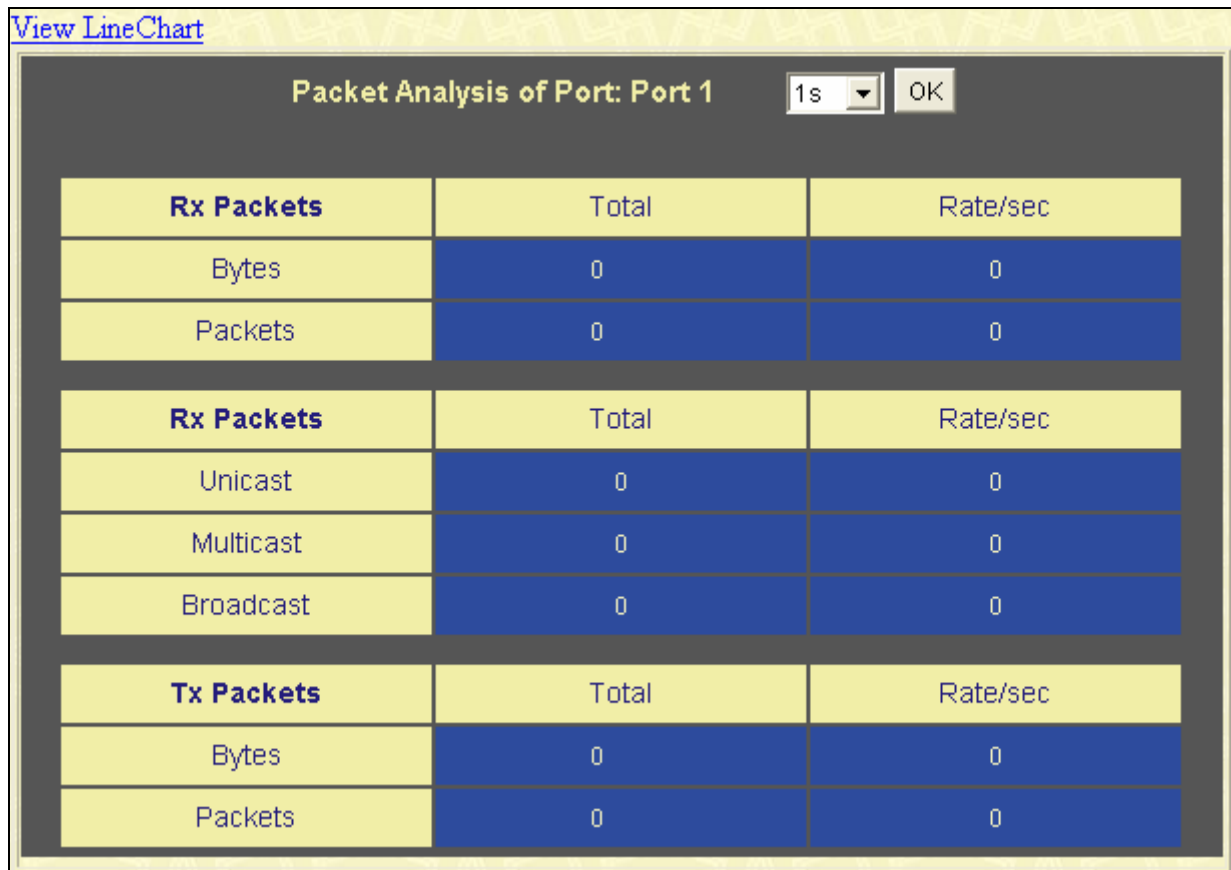
Figure 11- 8. Tx Packets Analysis window (table for Bytes and Packets)

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 from the port.
Packets	Counts the number of packets successfully sent on the port.
Unicast	Counts the total number of good packets that were transmitted by a unicast address.
Multicast	Counts the total number of good packets that were transmitted by a multicast address.
Broadcast	Counts the total number of good packets that were transmitted by a broadcast address.
Show/Hide	Check whether or not to display Bytes and Packets.
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 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)

The table displays the error packets received on the Switch. To view statistics for a specific port, select the port by using the **Port** pull down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port. To view this window, click **Monitoring** > **Packet Errors** > **Received (RX)**

Figure 11- 9. 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 11- 10. 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 packets received that were longer than 1518 octets, or if a VLAN frame is 1522 octets, and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	The number of packets with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522.
Drop	The number of packets that are dropped by this port since the last Switch reboot.
Show/Hide	Check whether or not to display Crc Error, Under Size, Over Size, Fragment, Jabber, and Drop errors.
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)

The following graph displays the error packets received on the Switch. To view statistics for a specific port, select the port by using the **Port** pull down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port. To view this window, click **Monitoring** > **Packet Errors** > **Transmitted(TX)**
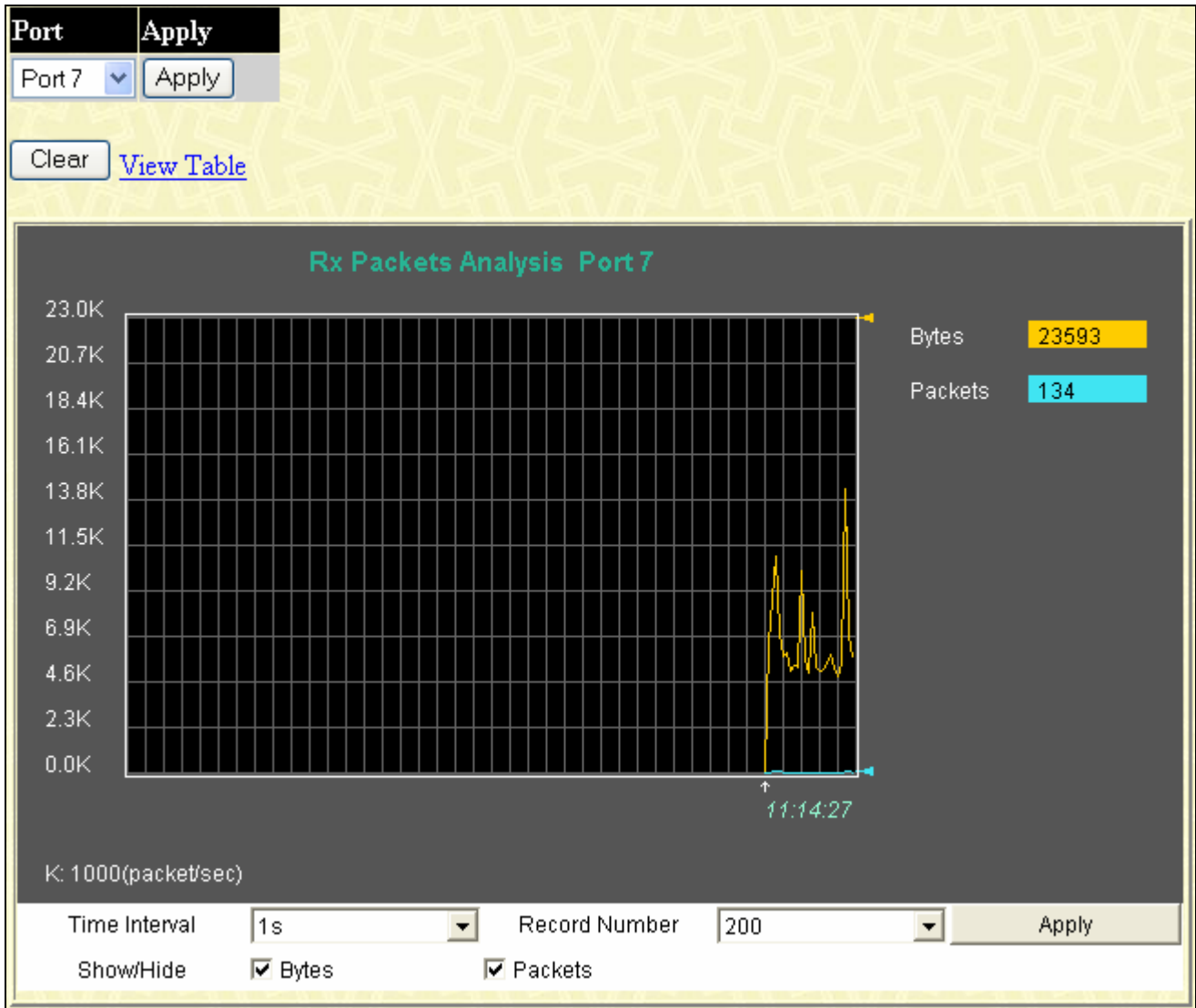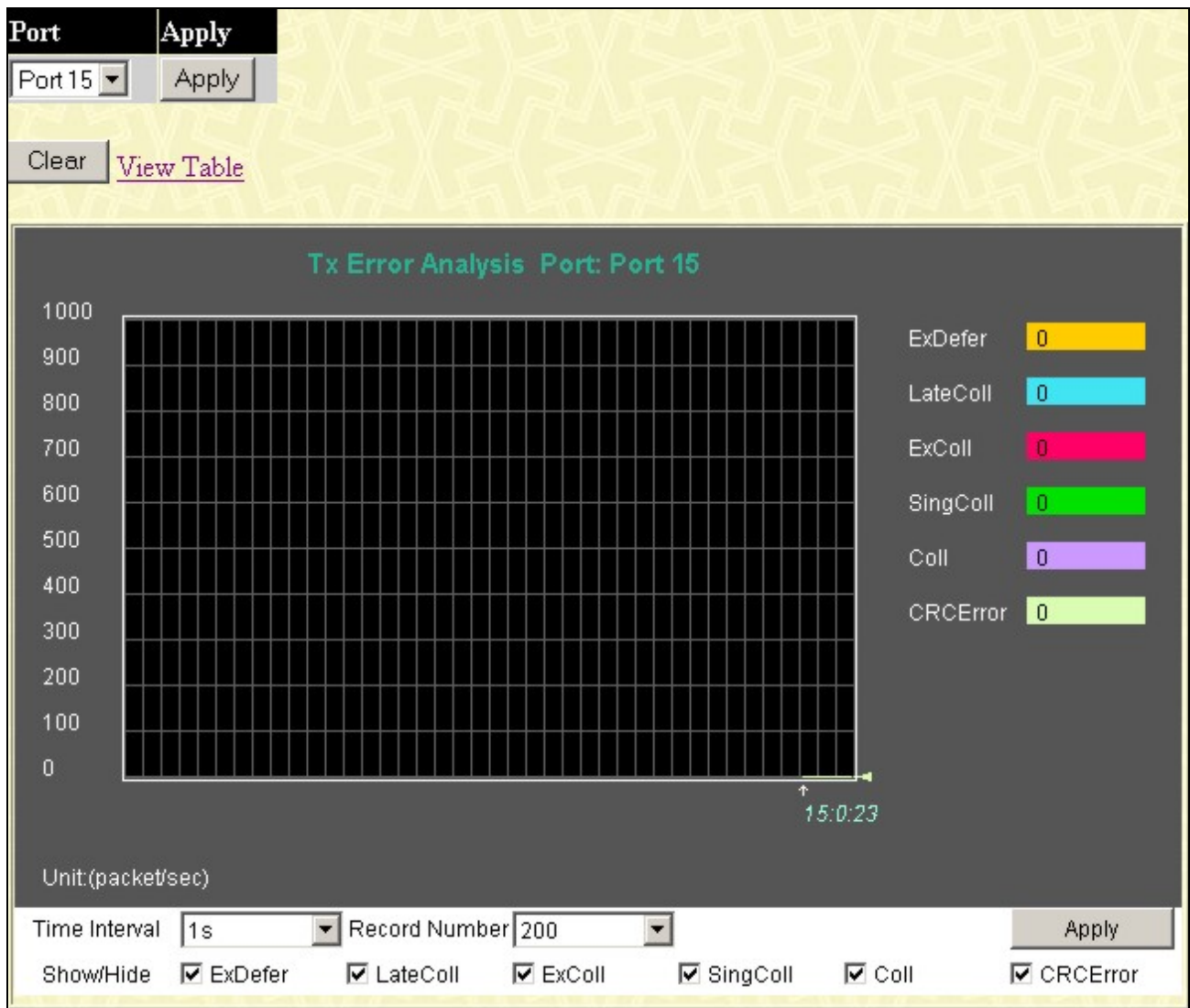

Figure 11- 11. Tx Error Analysis window (line graph)

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

View LineChart

Packet Analysis of Port: Port 1	1s ▼	OK

Tx Error	Total	Rate/sec
ExDefer	0	0
LateColl	0	0
ExColl	0	0
SingColl	0	0
Coll	0	0
CRCError	0	0
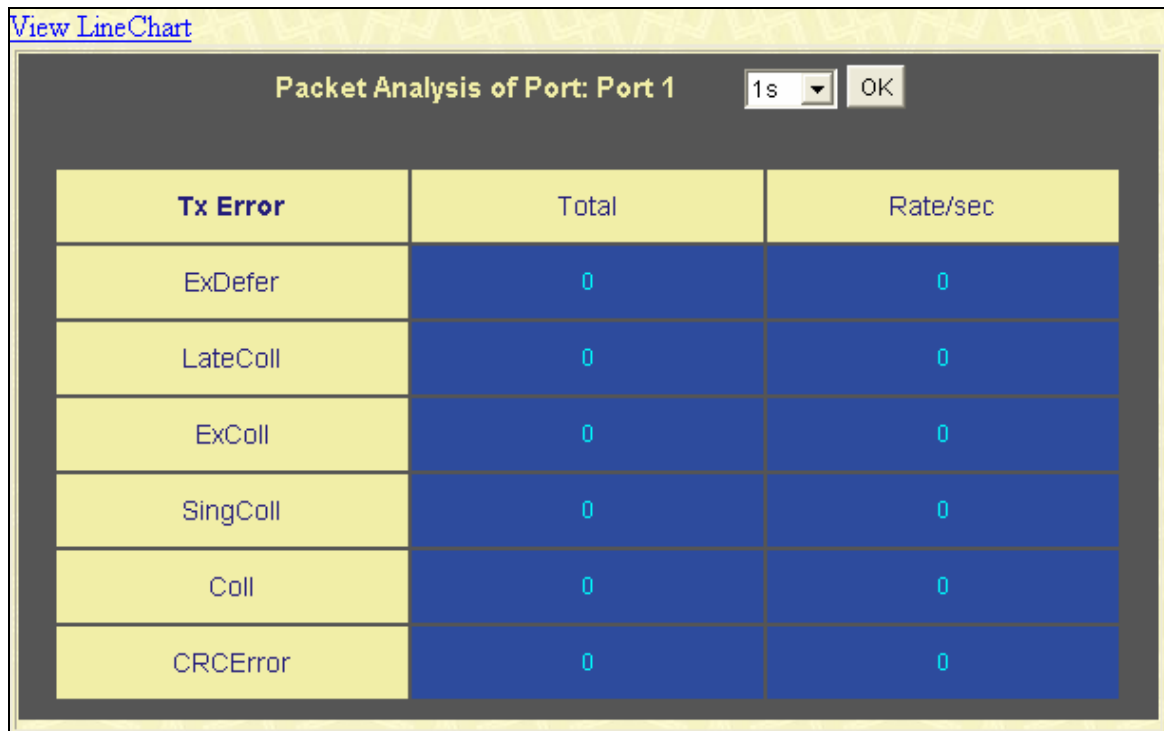
Figure 11- 12. Tx Error Analysis window (table)

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, select the port by using the **Port** pull down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port. To view this window, click **Monitoring** > **Packet Size**
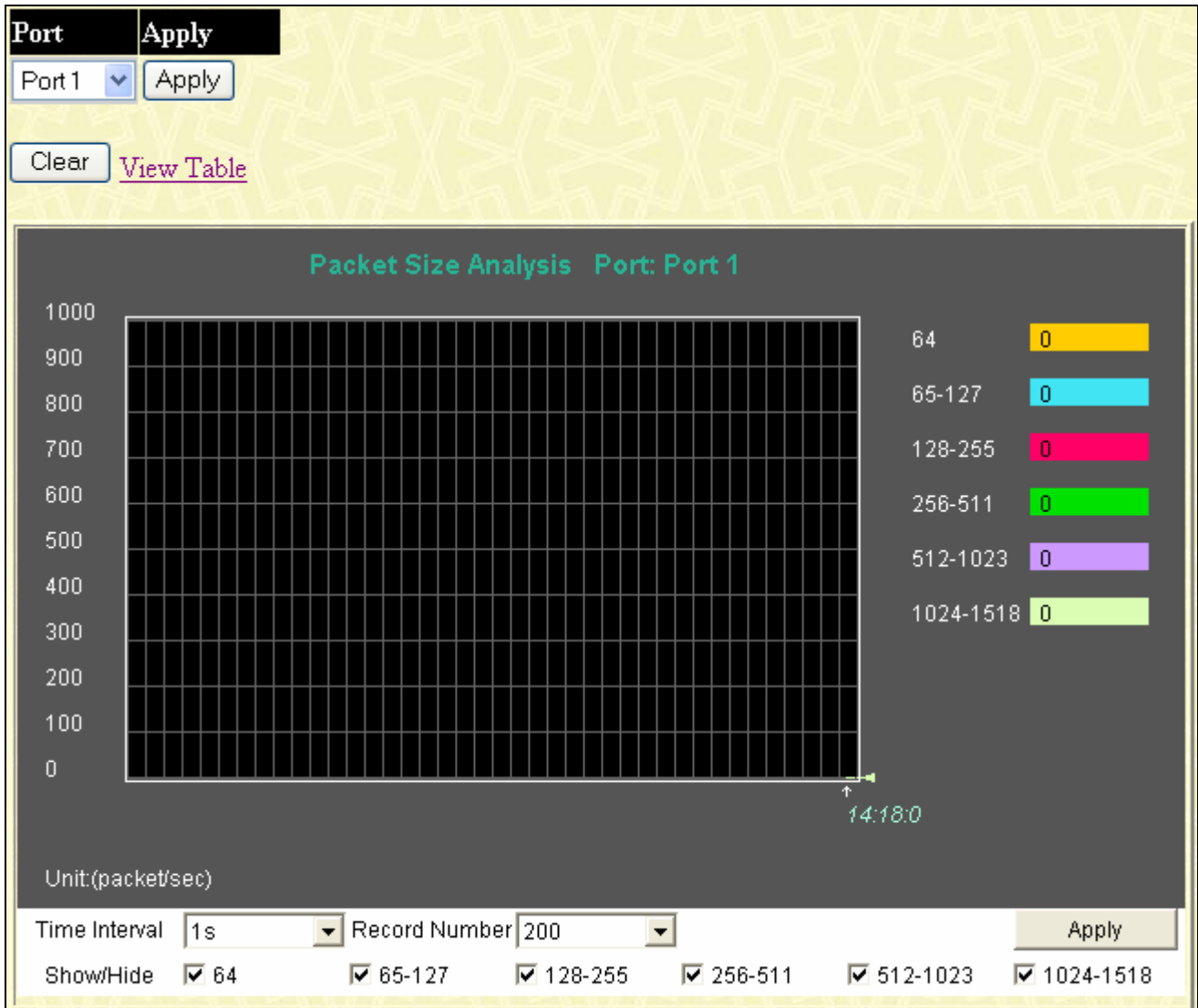
Figure 11- 13. Rx Size Analysis window (line graph)

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

Figure 11- 14. 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	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.

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, click **Monitoring** > **VLAN Status**

Figure 11- 15. VLAN Status window

Enter the **VLAN Name** and/or the **VID** and click **Find**, the information will be displayed in the table below.

MAC Address

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

To view the MAC Address forwarding table, click **Monitoring** > **MAC Address**

Figure 11- 16. MAC Address Table

The following fields can be viewed or set:

Parameter	Description
VLAN Name	Enter a VLAN Name by which to browse the forwarding table.
MAC Address	Enter a MAC address by which to browse the forwarding table.
Port	Select the port by using the corresponding pull-down menu.
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.
MAC Address	The MAC address entered into the address table.
Port	The 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.

181

Switch Log

The Web manager allows the Switch's history log, as compiled by the Switch's management agent, to be viewed. To view the Switch history log, click **Monitoring** > **Switch Log**

Sequence	Time	Log Text
17	0000-00-00,01:37:32	SSH server is enabled
16	0000-00-00,01:05:55	Successful login through Web (Username: Anonymous, IP:10.73.21.1, MAC:00-1B-FC-02-A6-03)
15	0000-00-00,00:24:39	Successful login through Web (Username: Anonymous, IP:10.73.21.1, MAC:00-1B-FC-02-A6-03)
14	0000-00-00,00:24:35	Logout through Web (Username: Anonymous, IP:10.73.21.1, MAC:00-1B-FC-02-A6-03)
13	0000-00-00,00:13:13	Successful login through Web (Username: Anonymous, IP:10.73.21.1, MAC:00-1B-FC-02-A6-03)
12	0000-00-00,00:00:31	Port 3 link up, 100Mbps FULL duplex
11	0000-00-00,00:00:29	Port 3 link down
10	0000-00-00,00:00:14	System started up
9	0000-00-00,00:00:10	Port 7 link up, 100Mbps FULL duplex
8	0000-00-00,00:00:10	Port 3 link up, 100Mbps FULL duplex
7	0000-00-00,00:04:10	Configuration saved to flash by console (Username: Anonymous)
6	0000-00-00,00:03:40	Firmware upgraded by console successfully (Username: Anonymous)
5	0000-00-00,00:03:01	Firmware upgrade by console was unsuccessful! (Username: Anonymous)
4	0000-00-00,00:00:58	Successful login through Console (Username: Anonymous)
3	0000-00-00,00:00:14	System started up
2	0000-00-00,00:00:10	Port 9 link up, 100Mbps FULL duplex
1	0000-00-00,00:00:10	Port 5 link up, 100Mbps FULL duplex

Clear

Figure 11- 17. 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. Clicking **Clear** will allow the user to clear the **Switch History Log**.
The information is described as follows:

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

Log Settings

Use the **Log Settings** menu to define the schedule or terms used for saving the Switch log. To view this table click, **Monitoring** > **Log Settings**

Figure 11- 18. Log Settings menu

Select the desired **Log Mode** and click the **Apply** button to put into effect.

Parameter	Description
Log Mode	Use the pull-down menu to select the desired method to save log files. The user has three options: **on_demand -** Specifies that logs are saved when requested by the host receiving the log. **log_trigger -** Specifies that logs are saved when previously configured triggers require the log to be saved to the Syslog host. Use the **config syslog host** command to determine what triggers are used. **time_interval** – Choose this option to save log files periodically, based on the time specified in the Time Interval field.
Time Interval	Specifies the minimum interval between saves in minutes.

Click **Apply** to implement changes made.

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 **Monitoring** > **IGMP Snooping Group**

Figure 11- 19. IGMP Snooping Group Table

The user may search the **IGMP Snooping Group Table** by VID by entering it in the top left hand corner and clicking **Search**.
The following field can be viewed:

Parameter	Description
VLAN ID	The VLAN ID 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 Map	These are the ports where the IGMP packets were snooped are displayed.

NOTE: To configure IGMP snooping for the Switch, go to the **L2 Features** folder and select **IGMP Snooping**. Configuration and other information concerning IGMP snooping may be found in Section 7 of this manual under **IGMP Snooping**.

Browse Router Port

This displays the Switch's ports that are currently configured as router ports. A router port configured by a user (using the console or Web-based management interface) is displayed as a static router port, designated by **S**. A router port that is dynamically configured by the Switch is designated by **D**. To view this table, click **Monitoring** > **Browse Router Port**

Figure 11- 20. Browse Router Port window

Browse ARP Table

This window will show all current ARP entries on the Switch. To clear the **ARP Table**, click **Clear All.** To view this table, click **Monitoring** > **Browse ARP Table**

Figure 11- 21. Browse ARP Table window

Session Table

The Session Table allows the user to view detailed information about the current configuration session of the Switch. Information such as the Session **ID** of the user, initial **Login Time**, **Live Time**, configuration connection **From** the Switch, **Level** and **Name** of the user are displayed. Click **Reload** to refresh this screen. To view this table, click **Monitoring** > **Session Table**

Figure 11- 22. Current Session Table

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 six screens to monitor.

> **NOTE:** The **Authenticator State**, **Authenticator Statistics**, Authenticator **Session Statistics** and **Authenticator Diagnostics** windows in this section cannot be viewed on the Switch unless 802.1X is enabled by port or by MAC address. To enable 802.1X, go to the **Switch 802.1X** entry in the **DES-3026 Web Management Tool**.

RADIUS Authentication

This table contains information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol. It has one row for each RADIUS authentication server that the client shares a secret with. To view the **RADIUS Authentication**, click **Monitoring > Port Access Control > RADIUS Authentication**

Figure 11- 23. RADIUS Authentication window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second. To clear the current statistics shown, click the *Clear* button in the top left hand corner.
The following fields can be viewed:

Parameter	Description
Server	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.

UDP Port	The UDP port the client is using to send requests to this server.
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.
Requests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
Accepts	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.
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.
AccessRetrans	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication 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.
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.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the authentication port
PacketsDropped	The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

RADIUS Accounting

This window shows managed objects used for managing RADIUS accounting clients, and the current statistics associated with them. It has one row for each RADIUS authentication server that the client shares a secret with. To view the **RADIUS Accounting**, click **Monitoring > Port Access Control > RADIUS Accounting**

Figure 11- 24. RADIUS Accounting window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second. To clear the current statistics shown, click the *Clear* button in the top left hand corner.

The following fields can be viewed:

Parameter	Description
Server IP Addr	The IP address assigned to each RADIUS Accounting server that the client shares a secret with.
UDP Port	The UDP port the client is using to send requests to this server.
Timeouts	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Responses	The number of RADIUS packets received on the accounting port from this server.
RoundTripTime	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
AccessRetrans	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
PendingRequests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
MalformedResponses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.

BadAuthenticators	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
PacketsDropped	The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.

Auth Diagnostics

This table contains the diagnostic information regarding the operation of the Authenticator associated with each port. An entry appears in this table for each port that supports the Authenticator function. To view the **Authenticator Diagnostics**, click **Monitoring > Port Access Control > Auth Diagnostics**

Port	EntersConnecting	EapLogoffsConnecting	EntersAuthenticating	SuccessAuthenticating	TimeoutsAuthenticating	FailAuthenticating
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0
19	0	0	0	0	0	0
20	0	0	0	0	0	0
21	0	0	0	0	0	0
22	0	0	0	0	0	0
23	0	0	0	0	0	0
24	0	0	Click to activate and use this control		0	0

Figure 11- 25. Authenticator Diagnostics window

The user may select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
EntersConnecting	Counts the number of times that the state machine transitions to the CONNECTING state from any other state.
EapLogOffsConnecting	Counts the number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
EntersAuthenticating	Counts the number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.
SuccessAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant (authSuccess = TRUE).
TimeoutsAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout (authTimeout = TRUE).
FailAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure (authFail = TRUE).
ReauthsAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).
EapStartsAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
EapLogOffAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
ReauthsAuthenticated	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a reauthentication request (reAuthenticate = TRUE).
EapStartsAuthenticated	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
EapLogOffAuthenticated	Counts the number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
Responses	Counts the number of times that the state machine sends an initial Access-Request packet to the Authentication server (i.e., executes sendRespToServer on entry to the RESPONSE state). Indicates that the Authenticator attempted communication with the Authentication Server.
AccessChallenges	Counts the number of times that the state machine receives an initial Access-Challenge packet from the Authentication server (i.e., aReq becomes TRUE, causing exit from the RESPONSE state). Indicates that the Authentication Server has communication with the Authenticator.
OtherReqToSupp	Counts the number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant

	(i.e., executes txReq on entry to the REQUEST state). Indicates that the Authenticator chose an EAP-method.
ResponsesFromSupplicant	Counts the number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK (i.e., rxResp becomes TRUE, causing the state machine to transition from REQUEST to RESPONSE, and the response is not an EAP-NAK). Indicates that the Supplicant can respond to the Authenticator's chosen EAP-method.
AuthSuccesses	Counts the number of times that the state machine receives an Accept message from the Authentication Server (i.e., aSuccess becomes TRUE, causing a transition from RESPONSE to SUCCESS). Indicates that the Supplicant has successfully authenticated to the Authentication Server.
AuthFails	Counts the number of times that the state machine receives a Reject message from the Authentication Server (i.e., aFail becomes TRUE, causing a transition from RESPONSE to FAIL). Indicates that the Supplicant has not authenticated to the Authentication Server.

Auth Session Statistics

This table contains the session statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function. To view the **Authenticator Session Statistics**, click **Monitoring > Port Access Control > Auth Session Statistics**

Port	Frames Rx	Frames Tx	UserName	Time	Terminate Cause
1	0	0		0	SupplicantLogoff
2	0	0		0	SupplicantLogoff
3	0	0		0	SupplicantLogoff
4	0	0		0	SupplicantLogoff
5	0	0		0	SupplicantLogoff
6	0	0		0	SupplicantLogoff
7	0	0		0	SupplicantLogoff
8	0	0		0	SupplicantLogoff
9	0	0		0	SupplicantLogoff
10	0	0		0	SupplicantLogoff
11	0	0		0	SupplicantLogoff
12	0	0		0	SupplicantLogoff
13	0	0		0	SupplicantLogoff
14	0	0		0	SupplicantLogoff
15	0	0		0	SupplicantLogoff
16	0	0		0	SupplicantLogoff
17	0	0		0	SupplicantLogoff
18	0	0		0	SupplicantLogoff
19	0	0		0	SupplicantLogoff
20	0	0		0	SupplicantLogoff
21	0	0		0	SupplicantLogoff
22	0	0		0	SupplicantLogoff
23	0	0		0	SupplicantLogoff
24	0	0		0	SupplicantLogoff

Authenticator Session Statistics   Time Interval 1s

Figure 11- 26. Authenticator Session Counter window

The user may select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Frames Rx	The number of user data frames received on this port during the session.
Frames Tx	The number of user data frames transmitted on this port during the session.
UserName	The User-Name representing the identity of the Supplicant PAE.
Time	The duration of the session in seconds.
Terminate Cause	The reason for the session termination. There are eight possible reasons for termination. 1) Supplicant Logoff 2) Port Failure 3) Supplicant Restart 4) Reauthentication Failure 5) AuthControlledPortControl set to ForceUnauthorized 6) Port re-initialization 7) Port Administratively Disabled 8) Not Terminated Yet
Octets Rx	The number of octets received in user data frames on this port during the session.
Octets Tx	The number of octets transmitted in user data frames on this port during the session.
ID	A unique identifier for the session, in the form of a printable ASCII string of at least three characters.
Authentic Method	The authentication method used to establish the session. Valid Authentic Methods include: (1) Remote Authentic Server - The Authentication Server is external to the Authenticator's System. (2) Local Authentic Server - The Authentication Server is located within the Authenticator's System.

Auth Statistics

This table contains the statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function. To view the Authenticator Statistics, click **Monitoring > Port Access Control > Auth Statistics**

Figure 11- 27. Authenticator Statistics window

The user may select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

The following fields can be viewed:

Parameter	Description
Port	The identification number assigned to the Port by the System in which the Port resides.
Frames Rx	The number of valid EAPOL frames that have been received by this Authenticator.
Frames Tx	The number of EAPOL frames that have been transmitted by this Authenticator.
Rx Start	The number of EAPOL Start frames that have been received by this Authenticator.
TxReqId	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
RxLogOff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Tx Req	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
Rx RespId	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx Resp	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.

Rx Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx Error	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Last Version	The protocol version number carried in the most recently received EAPOL frame.
Last Source	The source MAC address carried in the most recently received EAPOL frame.

Auth State

The following section describes the 802.1X Status on the Switch. To view the Authenticator State, click
Monitoring > Port Access Control > Auth State

Port	Auth_PAE_State	Backend_State	PortStatus
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized
13	ForceAuth	Success	Authorized
14	ForceAuth	Success	Authorized
15	ForceAuth	Success	Authorized
16	ForceAuth	Success	Authorized
17	ForceAuth	Success	Authorized
18	ForceAuth	Success	Authorized
19	ForceAuth	Success	Authorized
20	ForceAuth	Success	Authorized
21	ForceAuth	Success	Authorized
22	ForceAuth	Success	Authorized
23	ForceAuth	Success	Authorized
24	ForceAuth	Success	Authorized

Authenticator State   Time Interval 1s ▼ OK

Figure 11- 28. Authenticator State window – Port-based 802.1X

Figure 11- 29. Authenticator State window – MAC-Based 802.1X

This window displays the **Authenticator State** for individual ports on a selected device. A polling interval between *1* and *60* seconds can be set using the drop-down menu at the top of the window and clicking **OK**. The information on this window is described as follows:

Parameter	Description
MAC Address	Displays the Authenticator MAC address.
Auth PAE State	The **Authenticator PAE State** value can be: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force_Auth* or *Force_Unauth*.
Backend State	The **Backend Authentication State** can be *Request, Response, Success, Fail, Timeout, Idle* or *Initialize*.
Port Status	Controlled Port Status can be *Authorized* or *Unauthorized*.

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- 30. Factory Reset to Default Value window

Reboot System

The following menu is used to restart the Switch.
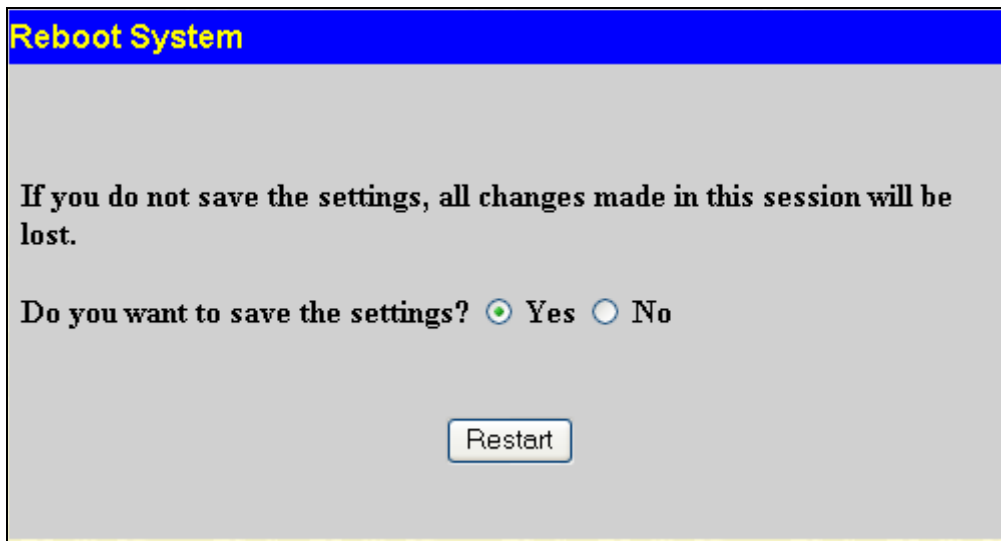
Figure 11- 31. Reboot System window

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

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

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

Save Changes

The Switch has two levels of memory, normal RAM and non-volatile or NV-RAM. Some settings, 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.

There are three Save Changes options:

- **Save Config** – Saves current configuration to NV-RAM. This configuration will be loaded upon rebooting.
- **Save Log** – Save history log.
- **Save All** – Save configuration and log.
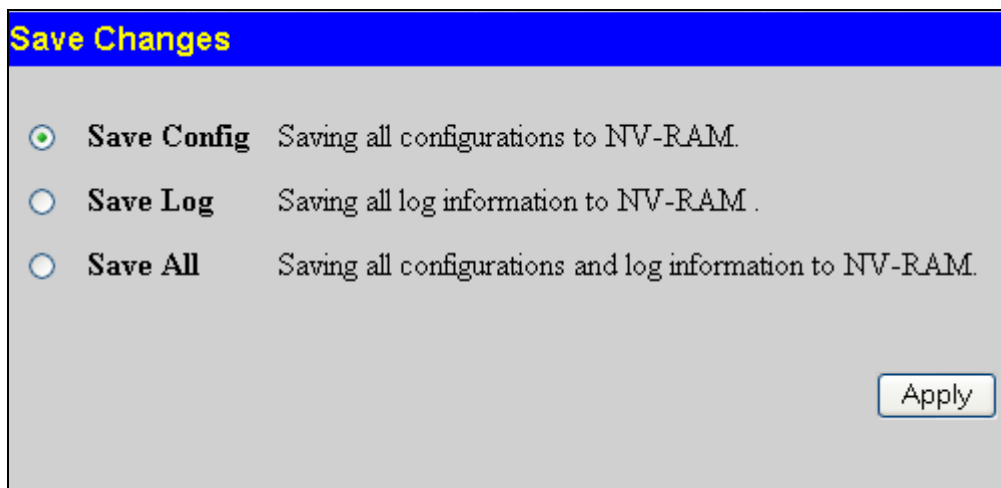
Figure 11- 32. Save Changes screen

Logout

The following window is used to logout of the Switch. Clicking the **Logout** button will return the user to the main login page.
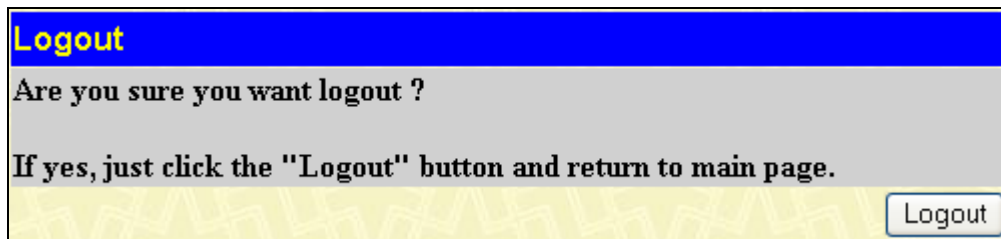
Figure 11- 33. Reboot System window

Appendix A

Physical and Environmental	
AC input	DES-3010F/FL: 110/220 VAC, 0.234A/0.145A, 60/50 Hz
	DES-3010G: 110/220 VAC, 0.231A/0.138A 60/50 Hz
	DES-3016: 100/240 VAC, 50/60 Hz
	DES-3018: 110/220 VAC, 0.249A/0.153A, 60/50 Hz
	DES-3026: 110/220 VAC, 0.276A/0.173A, 60/50 Hz
Power Consumption:	DES-3010FL – 14.8W
	DES-3010F – 15W
	DES-3010G – 14.8W
	DES-3016 – 11W
	DES-3018 – 15.2W
	DES-3026 – 17W
Operating Temperature:	0 to 40 degrees Celsius
Storage Temperature:	-40 to 70 degrees Celsius
Humidity:	Operating: 5% to 95% RH non-condensing;
	Storage: 0% to 95% RH non-condensing
Dimensions:	DES-3010F/FL – 280 mm x 180 mm x 44 mm (1U), 11 inch rack-mount width
	DES-3016/DES-3018/3026 – 441 mm x 207mm x 44 mm (1U), 19 inch rack-mount width
Weight:	DES-3010F/FL/G – 1.5kg
	DES-3016 – 2.2kg
	DES-3018 and DES-3026 - 2.1 kg
EMI:	FCC Class A, CE Class A, C-Tick Class A,VCCI Class A
Safety:	CSA International

General	
Standards:	IEEE 802.3 10BASE-T Ethernet
	IEEE 802.3u 100BASE-TX Fast Ethernet
	IEEE 802.3z 1000BASE-SX Gigabit Ethernet
	IEEE 802.3ab 1000BASE-T Gigabit Ethernet
	IEEE 802.1 D/w Spanning Tree
	IEEE 802.1X Port Based Network Access Control
	IEEE 802.1 p/Q VLAN
	IEEE 802.3x Full-duplex Flow Control
	IEEE 802.3 Nway auto-negotiation
Protocols:	CSMA/CD
Data Transfer Rates:	Half-duplex Full-duplex
Ethernet Fast Ethernet Gigabit Ethernet	10 Mbps 20Mbps 100Mbps 200Mbps n/a 2000Mbps
Network Cables: 10BASE-T	2-pair UTP Cat. 3,4,5 (100 m) EIA/TIA- 568 100-ohm STP (100 m)
100BASE-TX	2-pair UTP Cat. 5 (100 m) EIA/TIA-568 100-ohm STP (100 m)
Number of Ports	DES-3010F/FL – 8 x 10/100 Mbps NWay ports, 1 x 1000BASE-T Gigabit Port, 1 x 100BASE-FX Fiber Optic Port
	DES-3010G – 8 x 10/100 Mbps NWay ports, 1 x 1000BASE-T Gigabit Port, 1 x SFP Fiber Optic Port
	DES-3016 – 16 x 10/100 Mbps NWay ports
	DES-3018 – 16 x 10/100 Mbps NWay ports + 2 Optional Module Slots
	DES-3026 – 24 x 10/100 Mbps NWay ports + 2 Optional Module Slots
	DEM-301T (Optional Module) – 1 x 1000BASE-T Gigabit Port
	DEM-201F (Optional Module) – 1 x 100BASE-FX (Multi-Mode Fiber)Port
	DEM-201FL (Optional Module) – 1 x 100BASE-FX (Single-Mode Fiber)Port
	DEM-301G (Optional Module) – 1 SFP Gigabit Port

Performance	
Transmission Method	Store-and-forward
RAM Buffer	32M Bytes per device
Filtering Address Table:	8K MAC address per device
Packet Filtering / Forwarding Rate:	14,880 pps per 10Mbps 148,809 pps per 100Mbps 1,488,100 pps per 1000Mbps
MAC Address Learning:	Automatic update.

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.
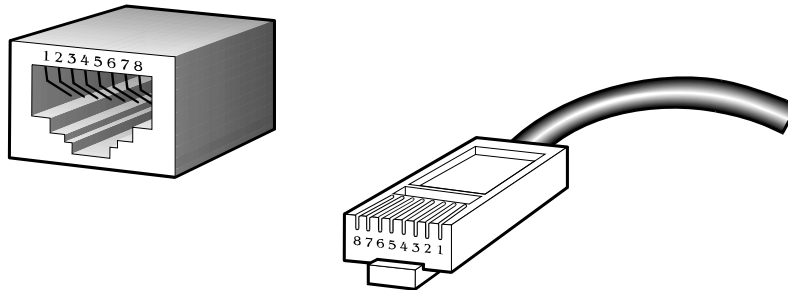
Appendix 1- 1. The standard RJ-45 port and connector

RJ-45 Pin Assignments		
Contact	MDI-X Port	MDI-II Port
1	BI-DB+	BI-DA+
2	BI-DB-	BI-DA-
3	BI-DA+	BI-DB+
4	BI-DD+	BI-DC+
5	BI-DD-	BI-DC-
6	BI-DA-	BI-DB-
7	BI-DC+	BI-DD+
8	BI-DC-	BI-DD+

Appendix 1- 2. The standard RJ-45 pin assignments

Appendix C

System Log Entries

Item	Cat.	Event Description	Log Information	Severity	Remark	Enhancement
1	system	System started up	Unit <unitID>, System started up	Critical	For all projects except DES-3526	
4		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.	V
5		System log saved to flash	Unit <unitID>, System log saved to flash by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	"by console""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.	V
6		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.	V
15	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	V
16		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	V
17		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	V
18		Configuration download was unsuccessful	Configuration download by console was unsuccessful! (Username:	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string,	V

			<username>, IP: <ipaddr>, MAC: <macaddr>)		which means if user login by console, will no IP and MAC information for logging	
19		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	V
20		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	V
21		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	V
22		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	V
23	Interface	Port link up	Port <unitID: portNum> link up, <link state>	Informational	link state, for ex., 100Mbps FULL duplex	
24		Port link down	Port <unitID: portNum> link down	Informational		
30	Console	Successful login through Console	Unit <unitID>, Successful login through Console (Username: <username>)	Informational	There are no IP and MAC if login by console.	
31		Login failed through Console	Unit <unitID>, Login failed through Console (Username: <username>)	Warning	There are no IP and MAC if login by console.	
32		Logout through Console	Unit <unitID>, Logout through Console (Username: <username>)	Informational	There are no IP and MAC if login by console.	
33		Console session timed out	Unit <unitID>, Console session timed out (Username: <username>)	Informational	There are no IP and MAC if login by console.	
34	Web	Successful login	Successful login through Web	Informational		V

		through Web	(Username: <username>, IP: <ipaddr>, MAC: <macaddr>)			
35		Login failed through Web	Login failed through Web (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning		V
36		Logout through Web	Logout through Web (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational		V
37		Web session timed out	Web session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational		V
42	Telnet	Successful login through Telnet	Successful login through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational		V
43		Login failed through Telnet	Login failed through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning		V
44		Logout through Telnet	Logout through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational		V
45		Telnet session timed out	Telnet session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational		V
46	SNMP	SNMP request received with invalid community string	SNMP request received from <ipAddress> with invalid community string!	Informational		
47	STP	Topology changed	Topology changed	Informational		
48		New Root selected	New Root selected	Informational		
50		Spanning Tree Protocol is enabled	Spanning Tree Protocol is enabled	Informational		
51		Spanning Tree Protocol is disabled	Spanning Tree Protocol is disabled	Informational		
124	Port security	Port security is exceeded to its maximum learning size and will not learn any new address	Port security violation (Port: <unitID: portNum>, MAC: <macaddr>)	Warning		

126	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		V
128	IP and Password Changed	IP Address change activity	Unit <unitID>, Management IP address was changed by (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational		V
129		Password change activity	Unit <unitID>, Password was changed by (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational		V
150	Packet Storm	Broadcast storm occurrence	Port <unitID: portNum> Broadcast storm is occurring	Warning		
151		Broadcast storm cleared	Port <unitID: portNum> Broadcast storm has cleared	Informational		
152		Multicast storm occurrence	Port <unitID: portNum> Multicast storm is occurring	Warning		
153		Multicast storm cleared	Port <unitID: portNum> Multicast storm has cleared	Informational		
154		Port shut down due to a packet storm	Port <unitID: portNum> is currently shut down due to a packet storm	Warning		
154	LBD	CTP detect port loop	Configuration Testing Protocol detects a loop in port <unitID: portNum>	Warning		
166	802.1X	VID assigned from radius server after radius client authenticated by radius server successfully. This VID will assign to the port and this port will be the vlan untagged port member.	Radius server <ipaddr> assigned vid :<vlanID> to port <[unitID:]portNum> (account :<username>)	Informational	This log will be generated when 802.1X authentication is successful and the target VLAN is assigned from the RADIUS server.	
167		Ingress bandwidth assigned from radius server after radius client authenticated by radius server successfully. This ingress bandwidth will be assigned to	RADIUS server <ipaddr> assigned ingress bandwith :<ingressBandwidth> to port <[unitID:]portNum> (account : <username>)	Informational	This log will be generated when the 802.1X authentication is successful and ingress bandwidth is assigned from the RADIUS server.	

		the port.				
168		Egress bandwidth assigned from radius server after radius client authenticated by radius server successfully. This egress bandwidth will assign to the port.	Radius server <ipaddr> assigned egress bandwidth: <egressBandwidth> to port <[unitID:]portNum> (account: <username>)	Informational	This log will be generated when 802.1X authentication is successful and egress bandwidth is assigned from the RADIUS server.	
169		802.1p default priority assigned from radius server after radius client authenticated by radius server successfully. This 802.1p default priority will assign to the port.	Radius server <ipaddr> assigned 802.1p deafult priority:<priority> to port <[unitID:]portNum> (account : <username>)	Informational	This log will be generated when 802.1X authentication is successful and the 802.1p default priority is assigned from the RADIUS server.	
170		802.1X Authentication failure	802.1X Authentication failure [for <reason>] from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr>)	Warning	This log will be generated when 802.1X authentication has finished and authentication has failed. The authentication failure reason will be one of the following: RADIUS server time-out 802.1X client session timeout	
171		802.1X Authentication success	802.1X Authentication success [for <reason>] from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr>)	Informational	This log will be generated when the 802.1X authentication has completed and authentication is successful.	

Appendix D

Cable Lengths

Use the following table to as a guide for the maximum cable lengths.

Standard	Media Type	Maximum Distance
Mini-GBIC	1000BASE-LX, Single-mode fiber module	10km
	1000BASE-SX, Multi-mode fiber module	550m
	1000BASE-LHX, Single-mode fiber module	40km
	1000BASE-ZX, Single-mode fiber module	80km
1000BASE-T	Category 5e UTP Cable	100m
	Category 5 UTP Cable (1000 Mbps)	
100BASE-TX	Category 5 UTP Cable (100 Mbps)	100m
10BASE-T	Category 3 UTP Cable (10 Mbps)	100m

Glossary

1000BASE-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 you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.

bridge: A device that interconnects local or remote networks no matter what higher level protocols are involved. Bridges form a single logical network, centralizing network administration.

broadcast: A message sent to all destination devices on the network.

broadcast storm: Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.

console port: The port on the Switch accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.

CSMA/CD: Channel access method used by Ethernet and IEEE 802.3 standards in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.

data center switching: The point of aggregation within a corporate network where a switch provides high-performance access to server farms, a high-speed backbone connection and a control point for network management and security.

Ethernet: A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.

Fast Ethernet: 100Mbps technology based on the Ethernet/CD network access method.

Flow Control: (IEEE 802.3z) A means of holding packets back at the transmit port of the connected end station. Prevents packet loss at a congested switch port.

forwarding: The process of sending a packet toward its destination by an internetworking device.

full duplex: A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

half duplex: A system that allows packets to be transmitted and received, but not at the same time. Contrast with full duplex.

IP address: Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.

IPX: Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.

LAN - Local Area Network: A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.

latency: The delay between the time a device receives a packet and the time the packet is forwarded out of the destination port.

line speed: See baud rate.

main port: The port in a resilient link that carries data traffic in normal operating conditions.

MDI - Medium Dependent Interface: An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.

MDI-X - Medium Dependent Interface Cross-over: An Ethernet port connection where the internal transmit and receive lines are crossed.

MIB - Management Information Base: Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.

multicast: Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.

protocol: A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

resilient link: A pair of ports that can be configured so that one will take over data transmission should the other fail. See also main port and standby port.

RJ-45: Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.

RMON: Remote Monitoring. A subset of SNMP MIB II that allows monitoring and management capabilities by addressing up to ten different groups of information.

RPS - Redundant Power System: A device that provides a backup source of power when connected to the Switch.

server farm: A cluster of servers in a centralized location serving a large user population.

SLIP - Serial Line Internet Protocol: A protocol which allows IP to run over a serial line connection.

SNMP - Simple Network Management Protocol: A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and end station operation.

Spanning Tree Protocol (STP): A bridge-based system for providing fault tolerance on networks. STP works by allowing you to implement parallel paths for network traffic, and ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.

stack: A group of network devices that are integrated to form a single logical device.

standby port: The port in a resilient link that will take over data transmission if the main port in the link fails.

switch: A device which filters, forwards and floods packets based on the packet's destination address. The switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.

TCP/IP: A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

telnet: A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.

TFTP - Trivial File Transfer Protocol: Allows you to transfer files (such as software upgrades) from a remote device using your switch's local management capabilities.

UDP - User Datagram Protocol: An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.

VLAN - Virtual LAN: A group of location- and topology-independent devices that communicate as if they are on a common physical LAN.

VLT - Virtual LAN Trunk: A Switch-to-Switch link which carries traffic for all the VLANs on each Switch.

VT100: A type of terminal that uses ASCII characters. VT100 screens have a text-based appearance.

Warranties and 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:

<u>Registration Card.</u> 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.

<u>Submitting A Claim.</u> 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 2008 D-Link Corporation. Contents subject to change without prior notice. D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. All other trademarks belong to their respective proprietors.

Copyright Statement
No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems Inc., as stipulated by the United States Copyright Act of 1976.

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.

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.

Limited Lifetime Warranty for the product is defined as follows:

- 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.

Product Registration

> ***Register your D-Link product online 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.**

Tech 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 within 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:
1-800-361-5265
Monday to Friday 7:30am to 9:00pm EST

D-Link Technical Support over the Internet:
http://support.dlink.com
email: support@dlink.ca

D-Link®
Building Networks for People

Technical Support

D-Link UK Technical Support over the Telephone:
0871 873 3000 (United Kingdom)
BT 10ppm (UK Pence per minute), other carriers may vary.
Times Mon-Fri 9.00am - 6.00pm Sat 10.00am - 2.00pm
+1890 886 899 (Ireland)
€0.05ppm peak, €0.045ppm off peak Times Mon-Fri 9.00am -
6.00pm Sat 10.00am - 2.00pm
D-Link UK & Ireland Technical Support over the Internet:
http://www.dlink.co.uk
ftp://ftp.dlink.co.uk

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.

Telefon: +49 (1805)2787
0,14€ pro Minute

Web: http://www.dlink.de
E-Mail: support@dlink.de

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.

Assistance technique D-Link par téléphone:
0 820 0803 03
0,12 €/min
Hours : Monday - Friday 9h to 13h and 14h to 19h
Saturday 9h to 13h and from 14h to 16h

Assistance technique D-Link sur internet :
Web: http://www.dlink.fr
E-mail: support@dlink.fr

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
0,067 €/min
Lunes a Viernes de 9:00 a 14:00 y de 15:00 a 18:00

Web: http://www.dlink.es
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 dal lunedì al venerdì dalle ore 9.00 alle ore
19.00 con orario continuato
Telefono: 199400057

Web: http://www.dlink.it/support

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.

Netherlands
0900 501 2007
€0.15ppm anytime
Web: www.dlink.nl

Belgium
070 66 06 40
€0.175ppm peak, €0.0875ppm off peak
Web: www.dlink.be

Luxemburg
+32 70 66 06 40
Web: 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:
0 801 022 021

Pomoc techniczna firmy D-Link świadczona przez Internet:
Web: http://www.dlink.pl
E-mail: dlink@fixit.pl

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

Telefon: 225 281 553
Land Line 1,78 CZK/min - Mobile 5.40 CZK/min
Telefonická podpora je v provozu: PO- PÁ od 09.00 do 17.00

Web: http://www.dlink.cz/suppport/
E-mail: support@dlink.cz

D-Link ®
Building Networks for People

Technikai Támogatás

Meghajtó programokat és frissítéseket a D-Link Magyarország weblapjáról tölthet le.

Tel: 06 1 461-3001
Fax: 06 1 461-3004
Land Line 14,99 HUG/min - Mobile 49.99,HUF/min

Web: http://www.dlink.hu
E-mail: support@dlink.hu

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.

D-Link Teknisk telefon Support:
800 10 610
(Hverdager 08:00-20:00)

D-Link Teknisk Support over Internett:
Web: 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
Åbningstider: kl. 08:00 – 20:00

D-Link teknisk support på Internettet:
Web: 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:

numerosta : 0800-114 677
Arkisin klo. 9 - 21

Internetin kautta:
Web: http://www.dlink.fi

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.

D-Link Teknisk Support via telefon:
0770-33 00 35
Vardagar 08.00-20.00

D-Link Teknisk Support via Internet:
Web: 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.

Assistência Técnica da D-Link na Internet:
Web: http://www.dlink.pt
E-mail: soporte@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

D-Link Hellas Support Center
Κεφαλληνίας 64, 11251 Αθήνα,
Τηλ: 210 86 11 114 (Δευτέρα- Παρασκευή 09:00-17:00)
Φαξ: 210 8611114

Web: http://www.dlink.gr/support

D-Link®
Building Networks for People

Tehnička podrška

Hvala vam na odabiru D-Link proizvoda. Za dodatne informacije, podršku i upute za korištenje uređaja, molimo vas da posjetite D-Link internetsku stranicu na www.dlink.eu

Web: www.dlink.biz/hr

D-Link®
Building Networks for People

Tehnična podpora

Zahvaljujemo se vam, ker ste izbrali D-Link proizvod. Za vse nadaljnje informacije, podporo ter navodila za uporabo prosimo obiščite D-Link - ovo spletno stran www.dlink.eu

Web: www.dlink.biz/sl

D-Link®

Building Networks for People

Suport tehnica

Vă mulțumim pentru alegerea produselor D-Link. Pentru mai multe informații, suport și manuale ale produselor vă rugăm să vizitați site-ul D-Link www.dlink.eu

Web: www.dlink.ro

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: +62-21-5731610   (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
Monday to Friday 9:00am to 6:00pm
http://www.d-link.co.kr
e-mail: lee@d-link.co.kr

New Zealand:

Tel: 0800-900-900
Monday to Friday 8:30am to 8:30pm
Saturday 9:00am to 5:00pm
http://www.dlink.co.nz
e-mail: support@dlink.co.nz

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

http://support.dlink-me.com

e-mail: support@dlink-me.com

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:

Teléfono: 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 Costa Rica:
Teléfono: 0800 0521478 Lunes a Viernes 06:00 am a 19:00 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 México:
Teléfono: 01800 1233201 Lunes a Viernes 06:00 am a 19:00
Soporte Técnico Help Desk Panamá:
Teléfono: 011 008000 525465 Lunes a Viernes 07:00 am a 20:00 pm
Soporte Técnico Help Desk Perú:
Teléfono: 0800-00968 Lunes a Viernes 07:00 am a 20:00 pm
Soporte Técnico Help Desk Venezuela:

Teléfono: 0800-1005767 Lunes a Viernes 07:30 am a 20:30 pm

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

E-mail:

e-mail: suporte@dlinkbrasil.com.br

D-Link®

Building Networks for People

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: +62-21-5731610

Dukungan Teknis D-Link melalui Internet:
Email : support@dlink.co.id
Website : http://support.dlink.co.id

技术支持

您可以在D-Link的官方網站找到產品的軟件升級和使用手冊

办公地址：北京市东城区北三环东路36号 环球贸易中心B座26F 02-05室 邮编: 100013

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：北京市东城区北三环东路36号 环球贸易中心B座26F 02-05室 邮编: 100013

维修中心电话：(010) 58257789

维修中心传真：(010) 58257790

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. Walicόw 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: 56-2-5838-950
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 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:_____
Fax:_____
Reseller's full address:_____
_____
_____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?
□Home □Office □Travel □Company Business □Home Business □Personal Use

2. How many employees work at installation site?
□1 employee □2-9 □10-49 □50-99 □100-499 □500-999 □1000 or more

3. What network protocol(s) does your organization use?
□XNS/IPX □TCP/IP □DECnet □Others_____

4. What network operating system(s) does your organization use?
□D-Link LANsmart □Novell NetWare □NetWare Lite □SCO Unix/Xenix □PC NFS □3Com 3+Open
□Banyan Vines □Windows NT □Windows ME □Windows 2000 □Windows XP
□Others_____

5. What network management program does your organization use?
□D-View □HP OpenView/Windows □HP OpenView/Unix □SunNet Manager □Novell NMS
□NetView 6000 □Others_____

6. What network medium/media does your organization use ?
□Fiber-optics □Thick coax Ethernet □Thin coax Ethernet □10BASE-T UTP/STP
□100BASE-TX □100BASE-T4 □100VGAnyLAN □Others_____

7. What applications are used on your network?
□Desktop publishing □Spreadsheet □Word processing □CAD/CAM
□Database management □Accounting □Others_____

8. What category best describes your company?
□Aerospace □Engineering □Education □Finance □Hospital □Legal □Insurance/Real Estate □Manufacturing
□Retail/Chainstore/Wholesale □Government □Transportation/Utilities/Communication □VAR
□System house/company □Other_____

9. Would you recommend your D-Link product to a friend?
□Yes □No □Don't know yet
10.Your comments on this product?_____

PLEASE
PLACE STAMP
HERE

TO:

D-Link®