D-Link ™ DES-3350SR

Standalone Layer 3 Switch

User's Guide

March 2005 P/N 651SR3350035

Table of Contents

Preface

The DES-3350SR *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, Unpacking and Setup- 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, Identifying External Components - Tells how you can connect the Switch to your Ethernet network.

Section 4, Connecting The Switch - This chapter describes how to connect the DES-3350SR to your Ethernet/Fast Ethernet/Gigabit Ethernet network.

 Section 5, Introduction to Switch Management- This chapter discusses many of the concepts and features used to manage the switch, as well as the concepts necessary for the user to understand the functioning of the switch.

Section 6, Web-Based Switch Management - Introduces basic Switch management features, including password protection, SNMP Settings, IP Address assignment and connecting devices to the Switch.

Section 7, Configuration - A detailed discussion about configuring some of the basic functions of the Switch, including accessing the Switch information, using the Switch's utilities and setting up network configurations, such as Quality of Service, Access Profile Table, Port Mirroring and configuring the Spanning Tree.

Section 8, Management – A detailed discussion regarding the Simple Network Management Protocol including description of features and a brief introduction to SNMP.

Section 9 Layer 3 IP Management - A detailed discussion of Layer3 features including IP Interface Settings, Layer 3 Global Settings, MD5 Key Table Settings, Route Redistribution Settings, Static/Default Route Settings, Static ARP Settings, RIP, OSPF, DHCP/Bootp Relay, DNS Relay, and IP Multicast Routing Protocol

Section 10, Monitoring - Features graphs and screens used in monitoring features and packets on the Switch.

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

Appendix A, Technical Specifications - The technical specifications of the Switch.

Appendix B, Understanding and Troubleshooting Spanning Tree Protocol - A detailed description of Spanning tree Protocol.

Intended Readers

The *DES-3350SR User's Guide* contains information for setup and management of the DES-3350SR switch. This guide is intended for network managers familiar with network management concepts and terminology.

Notes, Notices, and Cautions

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

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

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

Safety Instructions

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

⚠ **Safety Cautions**

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

Observe and follow service markings. Do not service any product except as explained in your system documentation. Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock. Only a trained service technician should service components inside these compartments.
If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:

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

- An object has fallen into the product.

- The product has been exposed to water.

- The product has been dropped or damaged.

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

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

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

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

- Use the product only with approved equipment.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Unplug the power cable before removing the power supply.

- If the system has multiple sources of power, disconnect power from the system by

- Unplug *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 and workbench pads and an antistatic grounding strap.

Section 1

Introduction

Fast Ethernet Technology
Gigabit Ethernet Technology
Switch Stacking
Performance Features
Ports

This section describes the functionality features of the DES-3350SR.

Fast Ethernet Technology

100Mbps Fast Ethernet (or 100BASE-T) 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 full duplex 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.

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.

Performance Features

Switch performance features include:

- 64 Byte system packet forwarding rate (up to 10.1 million packets per second)

- Full-wire speed (full-duplex) operation on all ports including Gigabit ports.

- 4 Priority Queues per port

- MAC Address Table supports 8K MAC addresses

- IP Address Table supports 2K IP entries

- Packet Buffer Memory supports 64 M bytes buffer memory per device

Software Features

Switch software features include:

CoS

- Classification based on 802.1P Priority
- Number of priority queues supported
- Based on TOS field on IP header
- DSCP
- Classification based on IP Destination and Source Addresses (Based on Layer 3 information)
- Classification based on TCP/UDP port number
- Classification based on MAC SA/DA

Spanning Tree

- 802.1D Spanning tree compatible
- 802.1w Rapid Spanning Tree support

VLAN

- 802.1Q support
- GARP/GVRP
- Number of VLANs supported per device

IP Multicast

- IGMP Snooping
- IGMP v2
- DVMRP
- PIM Dense mode support

Configuration

- Telnet Server
- TFTP Client
- BootP Client
- DHCP Client
- DHCP/BootP Relay
- DNS Relay support

Management

- Password enabled
- Web-based support
- SNMP v1 support
- SNMP v2c support
- SNMP v3 support
- TFTP upgrade
- Command Line Interface
- SNTP support
- Traffic Segmentation
- Bandwidth control
- Broadcast storm control

- Support Port Security function
- Support Cisco-like Port Security function
- Web GUI Traffic Monitoring
- Web MAC address browsing
- SNMP Trap on MAC Notification
- Delete individual IP address by dynamic learning (ARP table editing)
- Port Description
- CPU Utilization Monitoring
- Add 'Show Config' command
- Enlarge static ARP entries to 255

MIB Support

- RFC1213 MIB II
- RFC1493 Bridge
- RFC1757 RMON
- RFC 1643 Ether-like MIB
- Private MIB
- IGMP MIB
- 802.1p RFC2674
- RFC 2233 – Evolution of the Interfaces Group of MIB II (Receive Address Group is not supported)
- RIP MIB
- OSPF RFC1850
- CIDR MIB RFC2096

RMON

- 4 Groups of RMON (Statistics, History, Alarms, Events)

Port Configuration and Monitoring

- Auto-Negotiation Support
- Port Mirroring

Port Trunking

- Static mode trunking
- 802.3ad LACP

Routing Protocol

- RIP I/II
- OSPF support
- Floating static route

Security

- Supports 802.1X Port-based Access Control
- Supports 802.1X MAC-based Access Control
- Radius Client for 802.1x support

Access Control List support (ACL)

- Based on MAC address
- Based on VLAN

- Based on IP address
- Based on TCP/UDP port number
- Based on 802.1p priority
- Based on DSCP

<div style="border:1px solid black">

Section 2

</div>

Unpacking and Setup

Unpacking
Installation
Power On

This chapter provides unpacking and setup information for the Switch.

Unpacking

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

- One DES-3350SR Stackable layer 3 Switch

- Mounting kit: 2 mounting brackets and screws

- Four rubber feet with adhesive backing

- One AC power cord

- This User's Guide with Registration Card

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

Installation

Use the following guidelines when choosing a place to install the Switch:

- The surface must support at least 5 kg

- The power outlet should be within 1.82 meters (6 feet) of the device

- Visually inspect the power cord and see that it is secured to the AC power connector

- Make sure that there is proper heat dissipation from and adequate ventilation around the switch.

- Do not place heavy objects on the switch

Desktop or Shelf Installation

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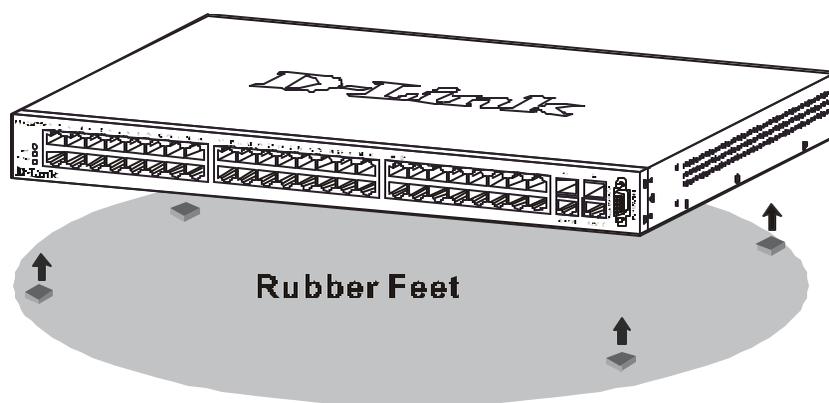
Figure 2 - 1.   Installing rubber feet for desktop installation

Rack Installation

The DES-3350SR can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets on the switch's side panels (one on each side) and secure them with the screws provided.
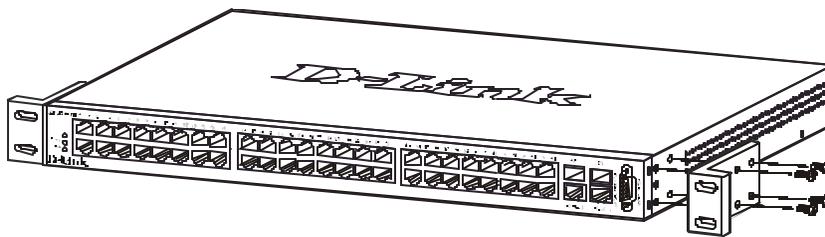
Figure 2 - 2.   Attaching the mounting brackets to the switch

Then, use the screws provided with the equipment rack to mount the switch on the rack.
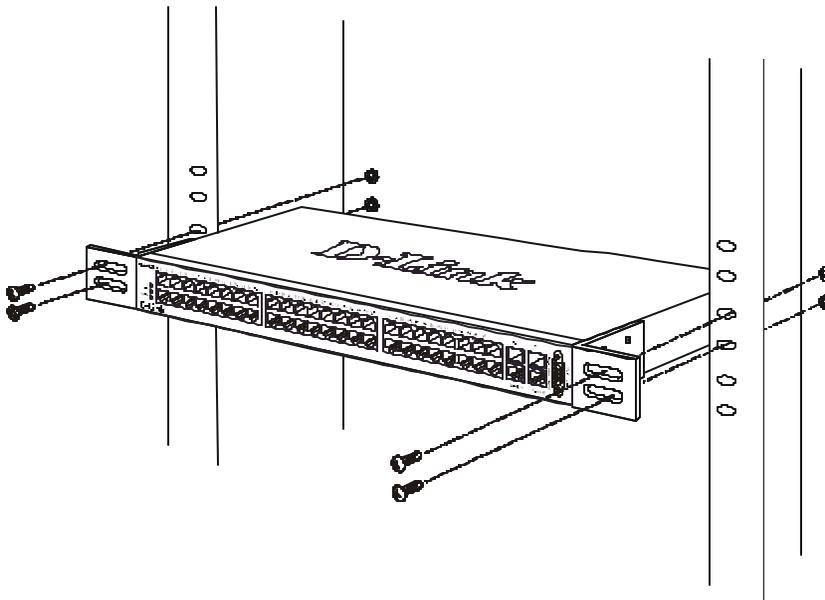
Figure 2 - 3.   Installing the switch on an equipment rack

Power on

The DES -3350SR switch can be used with AC power supply 100 - 240 VAC, 50 - 60 Hz. The power switch is located at the rear of the unit adjacent to the AC power connector and the system fan. The switch' s power supply will adjust to the local power source automatically and may be turned on without having any or all LAN segment cables connected.

After the power switch is turned on, the LED indicators should respond as follows:

- All LED indicators will momentarily blink. This blinking of the LED indicators represents a reset of the system

- The power LED indicator is always on after the power is turned ON

- The console LED indicator will blink while the Switch loads onboard software and performs a self-test. It will remain ON if there is a connection at the RS-232 port, otherwise this LED indicator is OFF

Power Failure

As a precaution in the event of a power failure, unplug the switch. When the power supply is restored, plug the switch back in.

<div style="border:1px solid black">

Section 3

</div>

Identifying External Components

Front Panel
Rear Panel
Side Panels
Gigabit Combo Ports
LED Indicators

This chapter describes the front panel, rear panel, side panels, and optional plug-in module, and LED indicators of the DES-3350SR.

Front Panel

The front panel of the Switch consists of LED indicators, an RS-232 communication port, 48 (10/100 Mbps) Ethernet/Fast Ethernet ports, and a pair of Gigabit Ethernet Combo ports for 1000BASE-T (plug-in module provided) and Mini GBIC connections (optional plug-in module).
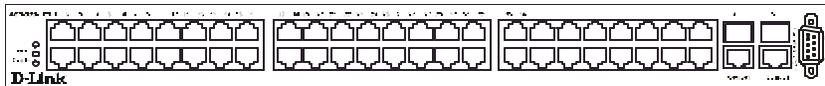
Figure 3 - 1. Front panel view of the Switch

Comprehensive LED indicators display the status of the switch and the network (see the *LED Indicators* section below).

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

- Forty-eight high-performance NWay Ethernet ports, all of which operate at 10/100 Mbps for connections to end stations, servers and hubs. All ports can auto-negotiate between 10Mbps or 100Mbps and full or half duplex.

- Two Gigabit Ethernet Combo ports for making 1000BASE-T and Mini GBIC connections.

Rear Panel

The rear panel of the switch consists of two fans and an AC power connector.

Figure 3 - 2. Rear panel view of the Switch

The system fans are used to dissipate heat. The sides of the system also provide heat vents to serve the same purpose. Do not block these openings, and leave at least 6 inches of space at the rear and sides of the switch for proper ventilation. Be reminded that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure. The AC power connector is a standard three-pronged connector that supports the power cord. Plug-in the female connector of the provided power cord into this socket, and the male side of the cord into a power outlet. Supported input voltages range from 100 ~ 240 VAC at 50 ~ 60 Hz.

Side Panels

Each side panel contains heat vents to help to dissipate heat.

Figure 3 - 3. Side panel views of the Switch

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

7

Gigabit Combo Ports

In addition to the 48 10/100 Mbps ports, the Switch features two Gigabit Ethernet Combo ports. These two ports are 1000BASE-T copper ports (provided) and Mini-GBIC ports (optional). See the diagram below to view the two Mini-GBIC port modules being plugged into the Switch. Please note that although these two front panel modules can be used simultaneously, the ports must be different. The GBIC port will always have the highest priority.
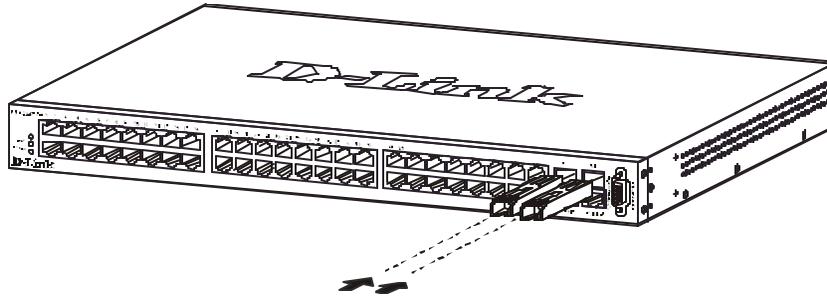
Figure 3 - 4. Mini-GBIC modules plug-in to the Switch

LED Indicators

The LED indicators of the Switch include Power, Console, and Link/Act. The following shows the LED indicators for the Switch along with an explanation of each indicator.
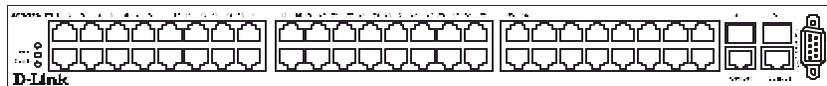
Figure 3 - 5. The LED Indicators

Power – This indicator on the front panel should be lit during the Power-On Self Test (POST). It will light green approximately 2 seconds after the switch is powered on to indicate the ready state of the device.

Console – This indicator is lit green when the switch is being managed via local console management through the RS-232 console port.

Link/Act – These indicators are located to the left and right of each port. They are lit when there is a secure connection (or link) to a device at any of the ports. The LEDs blink whenever there is reception or transmission (i.e. Activity--Act) of data occurring at a port.

8

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

Section 4

</div>

Connecting the Switch

> **Switch to End Node**
> **Switch to Hub or Switch**
> **10BASE-T Device**
> **100BASE-TX Device**

This chapter describes how to connect the DES -3350SR to your Ethernet/Fast Ethernet/Gigabit Ethernet network. The Switch's auto-detection feature allows all 48 10/100 ports to support both MDI-II and MDI-X connections.

Switch to End Node

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

An end node can be connected to the Switch via a two-pair Category 3, 4, or 5 UTP/STP cable. The end node should be connected to any of the ports (1x - 48x) on the switch.
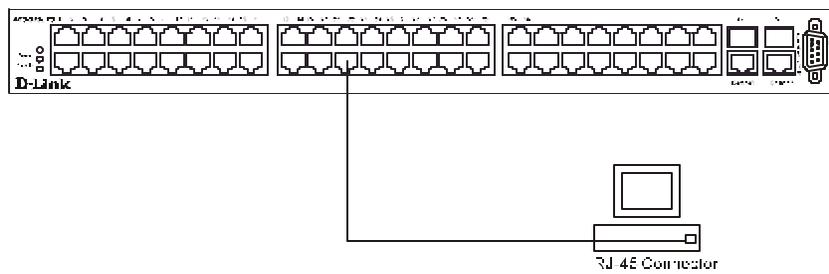
Figure 4 - 1. Switch connected to an End Node

The Link/Act LEDs in the top row for each UTP port light green when the link is valid. A blinking LED in the top row 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 two-pair Category 3, 4 or 5 UTP/STP cable.
- A 100BASE-TX hub or switch can be connected to the Switch via a two-pair Category 5 UTP/STP cable.
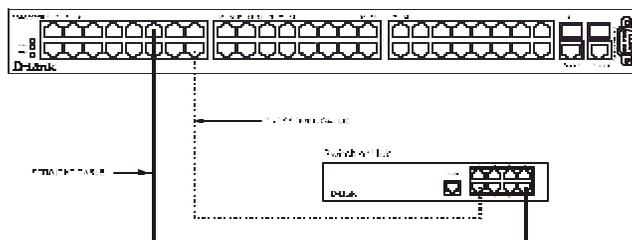
Figure 4 - 2. Switch connected to a port on a hub or switch using a straight or crossover cable

10BASE-T Device

For a 10BASE-T device, the Switch's LED indicators should display the following:

- Link/Act indicator is *ON*.

100BASE-TX Device

For a 100BASE-TX device, the Switch's LED indicators should display the following:

- Link/Act is *ON*.

9

| **Section 5** |

Introduction to Switch Management

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

Management Options

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

Web-based Management Interface

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

SNMP-Based Management

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

Command Line Console Interface Through the Serial Port

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

Connecting the Console Port (RS-232 DCE)

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

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

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

To connect a terminal to the console port:
1. Connect the female connector of the RS-232 cable directly to the console port on the Switch, and tighten the captive retaining screws.
2. Connect the other end of the cable to a terminal or to the serial connector of a computer running terminal emulation software. Set the terminal emulation software as follows:
3. Select the appropriate serial port (COM port 1 or COM port 2).
4. Set the data rate to 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. Usernames and Passwords are not required on the initial screen after the first connection. Any additional 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-3350SR 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 emu lator 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, the user name and password are not required. These can be changed or deleted later.


```
        D-Link DES-3350 Ethernet Switch Command Line Interface

                      Firmware: Build 3.01.B02
          Copyright(C) 2002-2005 D-Link  Corporation. All rights reserved.
UserName:
```
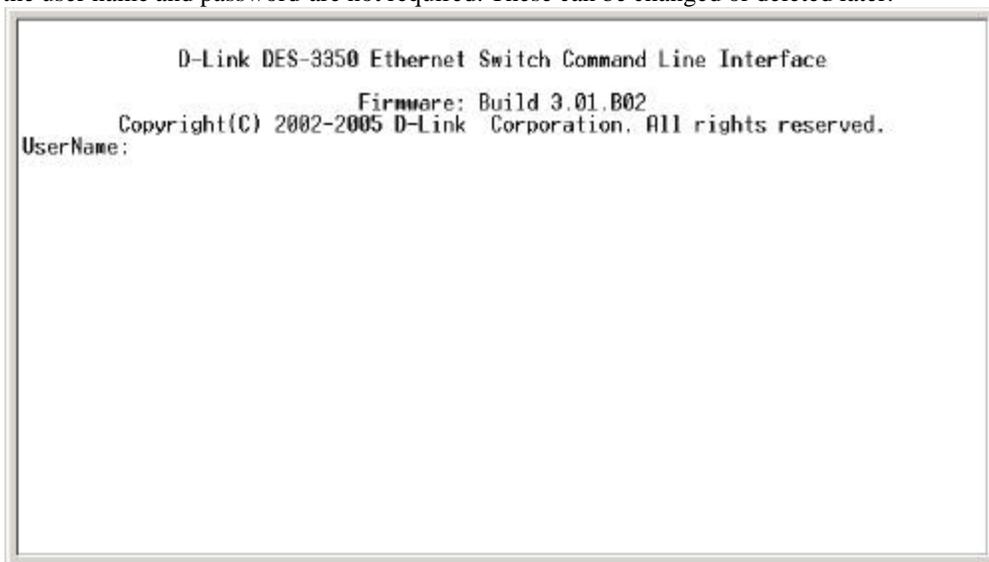
Figure 5 - 1. Initial screen after first connection

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.

```
        D-Link DES-3350 Ethernet Switch Command Line Interface

                      Firmware: Build 3.01.B02
            Copyright(C) 2002-2005 D-Link  Corporation. All rights reserved.
UserName:
PassWord:
```
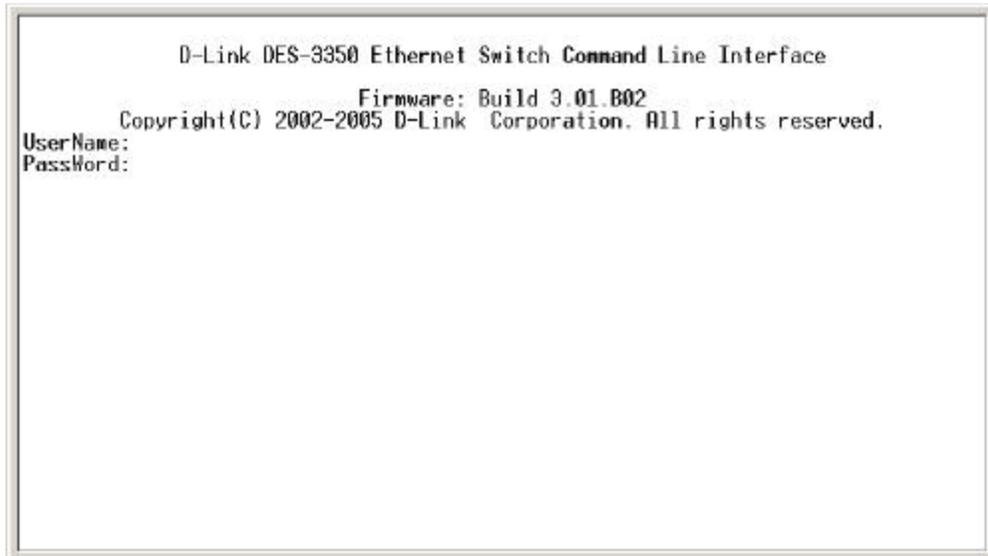
Figure 5 - 2. Initial screen, first time connecting to the Switch

Usernames and Passwords are not required on the initial screen after the first connection. Any additional user names and passwords must first be created by the administrator. You will be g iven access to the command prompt **local>** shown below:

```
        D-Link DES-3350 Ethernet Switch Command Line Interface

                      Firmware: Build 3.01.B02
            Copyright(C) 2002-2005 D-Link  Corporation. All rights reserved.
UserName:
PassWord:
local>
```
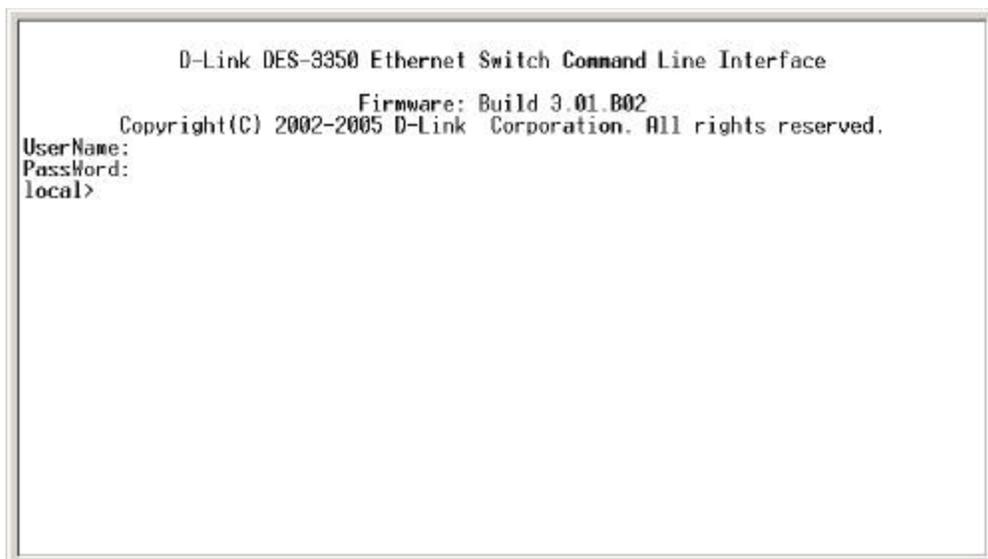
Figure 5 - 3. Command Prompt

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-3350SR does not have a default user name and password. One of the first tasks when settings up the Switch is to create user accounts. If you log in using a predefined administrator-level user name, you have privileged access to the Switch's management software.

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

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

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

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

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

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

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

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

```
local>create account admin newmanager
Command: create account admin newmanager

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

local>
```

Figure 5 - 4.Creation of a new Admin 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-3350SR supports SNMP versions 1, 2c, and 3. You can specify which version of SNMP you want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

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

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

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

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

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

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

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

Traps

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

MIBs

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

IP Address Assignment

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 10.90.90.90. You can change the default Switch IP address to meet the specification of your networking address scheme.
The Switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found by entering the command "show switch" into the command line interface, as shown below.

```
MAC Address       : 00-01-02-03-04-00
IP Address        : 10.58.44.222 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.00.002
Firmware Version  : Build 3.01.B02
Hardware Version  : 0A1
System Up Time    : 0 days 00:12:23
Time              : Unknown
Time Source       : System Clock
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Enabled
GVRP              : Disabled
IGMP Snooping     : Enabled
RIP               : Enabled
DVMRP             : Enabled
PIM-DM            : Enabled
OSPF              : Enabled
TELNET            : Enabled (TCP 23)
SNTP              : Disabled
CTRL+C ESC n Quit SPACE n Next Page ENTER Next Entry a All
```

Figure 5 - 5. Show switch command

The Switch's MAC address can also be found from the Web management program on the Switch Information (Basic Settings) window on the Configuration menu.
The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known.
The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:
Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy.** Where the **x's** represent the IP address to be assigned to the IP interface named System and the **y's** represent the corresponding subnet mask.
Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the **x's** represent the IP address to be assigned to the IP interface named System and the **z** represents the corresponding number of subnets in CIDR notation.
The IP interface named System on the Switch can be assigned an IP address and subnet mask that can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

```
local>config ipif System ipaddress 10.58.44.221/255.0.0.0
Command: config ipif System ipaddress 10.58.44.221/8

 Success.

local>
```

Figure 5 - 6. Assigning the Switch an IP Address

In the above example, the Switch was assigned an IP address of 10.58.44.221 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 6

Web-based Switch Management

Introduction
Login to Web Manager
User Accounts Management
Admin and User Privileges
Save Changes
Areas of the User Interface
Web Pages

Introduction

The DES-3350SR offers an embedded Web-based (HTML) interface allowing users to manage the switch from anywhere on the network through a standard browser such as Netscape Navigator/Communicator or Microsoft Internet Explorer. The Web 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.

Note: *This Web-based Management Module does not accept Chinese language input (or other languages requiring 2 bytes* per character).*

Login to Web Manager

The first step in getting started in using Web-based management for your Switch is to secure a browser. A Web browser is a program that allows a person to read hypertext, for example, Opera, Netscape Navigator, or Microsoft Internet Explorer. Follow the installation instructions for your browser.

The second step is to give the switch an IP address. This can be done manually through the console or automatically using BOOTP/DHCP.

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

Note: *The Factory default IP address for the switch is 10.90.90.90.*

In the page that opens, click on the **Login to make a setup** button:

Figure 6 - 1. Login button

This opens the management module's main page.

The switch management features available in the Web-based manager are explained below.

User Accounts Management

From the **Management** menu, click **User Accounts** and then the **User Account Management** window appears.
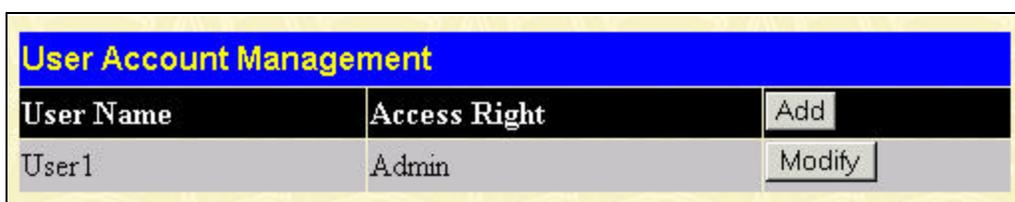
Figure 6 - 2. User Account Management window

Click **Add** to add a user.

User Account Modify Table

User Name	
New Password	
Confirm New Password	
Access Right	Admin ▼
	Apply

Show All User Account Entries

Figure 6 - 3. User Account Modify Table window

1. Enter the new user name, assign an initial password, and then confirm the new password. Determine whether the new user should have *Admin* or *User* privileges.

2. Click **Apply** to make the user addition effective.

3. A listing of all user accounts and access levels is shown in the **User Account Management** window. This list is updated when Apply is executed. Click **Show All User Account Entries** to access this window.

4. Please remember that Apply makes changes to the switch configuration for the *current session only*. All changes (including User additions or updates) must be entered into non-volatile ram using the **Save Changes** command on the **Main Menu** - if you want these changes to be permanent.

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:

Switch Configuration	*Privilege*	
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	Read Only
System Utilities	Yes	Ping Only
Factory Reset	Yes	No
Reboot Switch	Yes	No
User Account Management		
Add/Update/Delete User Accounts	Yes	No
View User Accounts	Yes	No

Table 6-1. Admin and User Privileges

After establishing a User Account with *Admin*-level privileges, go to the **Maintenance** menu and click **Save Changes**. Next click **Save Configuration**. The switch will now save any changes to its non-volatile ram and reboot. You can logon again and are now ready to continue configuring the Switch.

Save Changes

The DES -3350SR has two levels of memory; normal RAM and non-volatile or NV-RAM. Configuration changes are made effective by clicking the **Apply** button. When this is done, the settings will be immediately applied to the switching software in RAM, and will immediately take effect.

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

To retain any configuration changes permanently, click `Save Changes` from the **Maintenance** menu. The following window will appear:
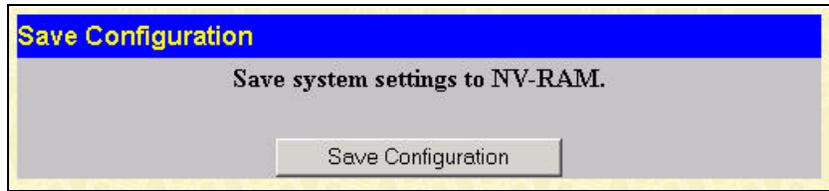
Figure 6 - 4. Save Configuration window

Click the **Save Configuration** button to save the current switch configuration in NV-RAM. The following dialog box will confirm that the configuration has been saved:

Figure 6 - 5. Save Configuration Confirmation dialog box

Click the **OK** button to continue.

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

Areas of the 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. The figure below shows the user interface. The user interface is divided into 3 distinct areas as described in the table.
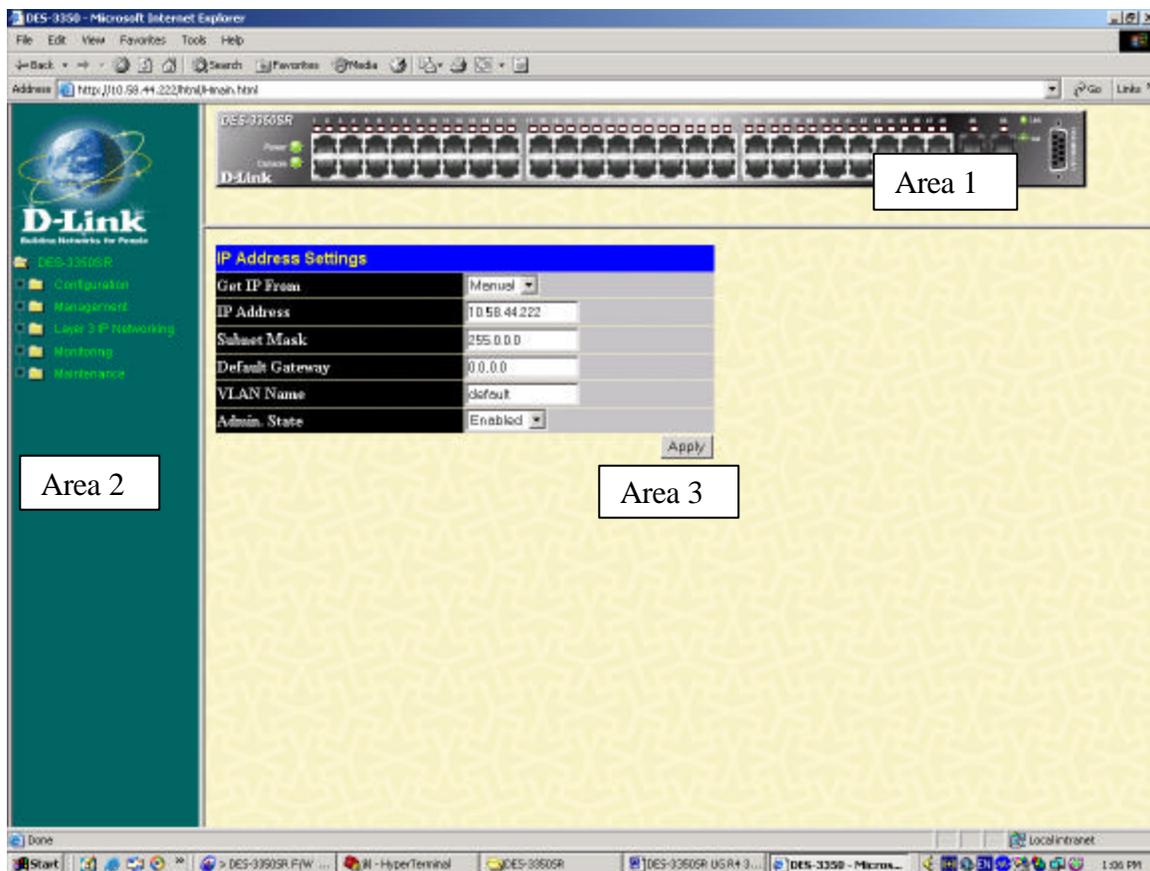
Figure 6 - 6. Main Web-Manager window

Area	Function
1	Presents a graphical near real-time image of the front panel of the switch. This area displays the switch's ports and expansion modules, showing port activity, or duplex mode, depending on the specified mode. Various areas of the graphic can be selected for performing management

	functions, including the ports, expansion modules, management module, or the case.
2	Allows the selection of commands.
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 use the command line interface (CLI) command save.**

Web Pages

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

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

Configuration – Contains windows concerning configurations for IP Address, Switch Information, Advanced Settings, Port Description, Port Configuration, Port Mirroring, IGMP, Spanning Tree, Forwarding Filtering, VLANs, Port Bandwidth, SNTP Settings, Port Security, QoS, LACP, Access Profile Table, IP-MAC Binding, PAE Access Entity, and Layer 3 IP Networking.

Management – Contains windows concerning configurations for Security IP, User Accounts, and SNMP V3.

Layer 3 IP networking - Contains windows concerning configurations for IP Interface Settings, Layer 3 Global Settings, MD5 Key Table Settings, Route Redistribution Settings, Static/Default Route Settings, Static ARP Settings, RIP, OSPF, DHCP/Bootp Relay, DNS Relay, and IP Multicast Routing Protocol

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

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

.

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

Configuration

> *IP Address*
> *Switch Information*
> *Advanced Settings*
> *Port Description*
> *Port Configuration*
> *Port Mirroring*
> *IGMP*
> *Spanning Tree*
> *Forwarding Filtering*
> *VLANs*
> *Port Bandwidth*
> *SNTP Settings*
> *Port Security*
> *QoS*
> *LACP*
> *Access Profile Table*
> *IP-MAC Binding*
> *PAE Access Entity*

This section, arranged by topic, describes how to perform common configuration tasks on the DES-3350SR switch using the Web-based Manager.

IP Address

The Switch needs to have an IP address assigned to it so that an In-Band network management system (for example, the Web Manager or Telnet) client can find it on the network. The **IP Address Settings** window allows you to change the settings for the Ethernet interface used for in-band communication.

To set the switch's IP address:

Click **IP Address** on the **Configuration** menu to open the following window:

Figure 7 - 1. IP Address Settings window

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

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

Select **Manual** from the **Get IP From** drop-down menu. Enter the appropriate IP address and subnet mask. If you want to access the switch from a different subnet from the one it is installed on, enter the IP address of the gateway. If you will manage the switch from the subnet on which it is installed, you can leave the default address in this field. If no VLANs have been previously configured on the switch, you can use the default VLAN − named "default." 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 name of the VLAN that contains the port that the management station will access the switch on.

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

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

The following fields can be set:

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. The fields which require entries under this option are as follows:
IP Address	Determines the IP address used by the switch for receiving SNMP and Telnet communications. These fields should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal) between 0 and 255. This address should be a unique address on a network assigned to you by the central Internet authorities.
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 (a computer) will be allowed to manage the switch using TCP/IP (in-band, or over the network). Management stations that are on VLANs other than the one entered in the VLAN Name field will not be able to manage the switch in-band unless their IP addresses are entered in the Management Station IP Addresses field. The default VLAN is named default and contains all of the switch's ports. There are no entries in the Management Station IP Addresses table, by default – so any management station can access the switch.
Admin. State	This setting allows the IP interface named "System" to be enabled or disabled.

"System" to be enabled or disabled.

Switch Information

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

Figure 7 - 2. Switch Information (Basic Settings) window

This window shows which (if any) external modules are installed, and the switch's MAC Address (assigned by the factory and unchangeable). In addition, the Boot PROM Version and Firmware Version numbers are shown. 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.

You can also enter the name of the System, its location, and the name and telephone number of the System Administrator. It is recommended that the person responsible for the maintenance of the network system that this switch is installed on be listed here.

Advanced Settings

Click **Advanced Settings** on the **Configuration** menu:

Figure 7 - 3. Switch Information (Advanced Settings) window

The following fields can be set:

Parameter	Description
Serial-port auto logout time	The Auto Logout field may be set to Never, 2 minutes, 5 minutes, 10 minutes, and 15 minutes, depending on the time the user wishes the Switch to be idle before automatically

	logging out. The default for this setting is 10 minutes.
MAC Address Aging Time *<300>*	The MAC Address Aging Time specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The Aging Time can be set to any value between *10* and *1,000,000* seconds.
IGMP Snooping *<Disabled>*	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. It can be enabled globally by toggling *Disabled* to *Enabled*.
GVRP Status *<Disabled>*	To enable GVRP on the switch globally, toggle *Disabled* to *Enabled*.
Telnet Status *<Disabled>*	The Switch can be accessed using Telnet. Toggle *Disabled* to *Enabled*.
Web Status *<Disabled>*	To enable the Web status, toggle *Disabled* to *Enabled*.
Link Aggregation Algorithm *<Mac Source>*	The Link Aggregation Algorithm can be set to one of the following: *IP Src & Dest*, *IP Destination*, *IP Source*, *Mac Src & Dest*, *Mac Destination*, or *Mac Source*.
RMON Status *<Disabled>*	To enable RMON capability, toggle *Disabled* to *Enabled*.
802.1x Status	To enable 802.1x port control access on a global basis, toggle *Disabled* to *Enabled*.

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 the **Port Description** on the **Configuration** menu:

Port Description Setting

From	To	Description	Apply
Port 1 ▾	Port 1 ▾		Apply

Port Description Table

Port	Description
1	24
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	

Figure 7 - 4. Port Description Settings window

Use the **From** and **To** pull down menu to choose a port or range of ports to describe and **Unit** to choose the Switch in the switch stack, and then enter a description of the port(s). Clic k **Apply** to set the descriptions in the Port Description Settings Table.

Port Configuration

Click the **Port Configuration** link in the **Configuration** menu:

Port Configuration

From	To	State	Speed/Duplex	Apply
Port 1 ▼	Port 1 ▼	Disabled ▼	Auto ▼	Apply

The Port Information Table

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

Figure 7 - 5. Port Configuration window

The **From** and **To** drop-down dialog boxes allow different ports to be selected for configuration.

Use the **State** pull-down menu to either enable or disable the selected port.

Use the **Speed/Duplex** pull-down menu to select the speed and duplex/half-duplex state of the port. The *Auto* setting allows the port to automatically determine the fastest settings the port on the device connected to the DES-3350SR can handle, and then use those settings. The other options for ports 1-48 are *100M/Full, 100M/Half, 10M/Full,* and *10M/Half.* For Combo ports 49 and 50, if the optional Mini-GBIC plug-in module is used, the options are *Auto* and *1000/Full*. Otherwise, the two 1000BASE-T Copper ports offer the same five choices for ports 1-48, plus a *1000/Full* option.

Please note that although the two front panel modules can be used simultaneously, the ports must be different. For example, if port 50x is used on the Mini GBIC module, port 50x is not available on the 1000BASE-T module. In addition, the fiber port will always be the highest priority.

The following fields can be set:

Parameter	Description
From and **To**	Enter the desired range of ports to be configured in these fields.
State *<Enabled>*	Toggle the State field to either enable or disable a given port.
Speed/Duplex *<Auto>*	Toggle the Speed/Duplex field to either select the speed and duplex/half-duplex state of the port. *Auto* – auto-negotiation between 10 and 100 Mbps devices, full- or half-duplex. The

Auto setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are *100M/Full*, *100M/Half, 10M/Full,* and *10M/Half.* There is no automatic adjustment of port settings with any option other than *Auto*.

Port Mirroring

Click **Port Mirroring** on the **Configuration** menu:

Figure 7 - 6. Setup Port Mirroring window

The target port is where information will be duplicated and sent for capture and network analysis. A network analyzer would be attached to this port to capture packets duplicated from the source port.

It should be noted that a faster port (a 1000 Mbps Gigabit Ethernet port, for example) should not be mirrored to a slower port (one of the 48 100 Mbps Fast Ethernet ports), because many packets will be dropped.

The following fields can be set:

Parameter	Description
Source Port	Allows multiple ports to be mirrored. These ports are the sources of the packets to be duplicated and forwarded to the Target port.
None	Selecting this option prevents any packets from either being received or transmitted.
Ingress	Selecting this option mirrors only received packets.
Egress	Selecting this option mirrors only transmitted packets.
Both	Selecting this option mirrors both received and transmitted packets.
Target Port	This port is where information will be duplicated and sent for capture and network analysis.

Status	Toggle between *Enabled* and *Disabled*.

IGMP

IGMP Snooping

From the **Configuration** menu, select the **IGMP** folder, and then click **IGMP Snooping** to open the following window:

Figure 7 - 7. Current IGMP Snooping Group Entries window

To edit an IGMP Snooping entry on the switch, click the **Modify** button next to the entry on the **Current IGMP Snooping Group Entries** window. The **IGMP Snooping Settings** window, shown below, will appear.

Figure 7 - 8. **IGMP Snooping Settings window**

The following fields can be set:

Parameter	Description
VLAN ID	Allows the entry of the VLAN ID for which IGMP Snooping is to be configured.
VLAN Name	Allows the entry of the name of the VLAN for which IGMP Snooping is to be configured.
Query Interval (1-65535)	Allows the entry of a value between *1* and *65535* seconds, with a default of *125* seconds. This specifies the length of time between sending IGMP queries.
Max Response Time(1-125)	Sets the maximum amount of time allowed before sending an IGMP response report. A value between *1* and *25* seconds can be entered, with a default of *10* seconds.
Robustness Value	A tuning variable to allow for VLANs that are expected to lose a large number of

27

	packets. A value between *2* and *255* can be entered, with larger values being specified for VLANs that are expected to lose larger numbers of packets.
Last Member Query Interval	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. The default is *1* second.
Host Timeout (1-16711450)	Specifies the maximum amount of time a host can be a member of a multicast group without the switch receiving a host membership report. The default is *260* seconds.
Router Timeout (1-16711450)	Specifies the maximum amount of time a route will remain in the switch's forwarding table without receiving a membership report. The default is *260* seconds.
Leave Timer (1-16711450)	Specifies the maximum amount of time between the switch receiving a leave group message from a host, and the switch issuing a group membership query. If the switch does not receive a response from the group membership query before the Leave Timer expires, the forwarding table entry for the multicast address is deleted from the switch's forwarding table. The default is *2* seconds.
Querier State	This field can be switched using the pull-down menu between *Disabled* and *Enabled*.
State	This field can be switched using the pull-down menu between *Disabled* and *Enabled*. This is used to enable or disable IGMP Snooping for the specified VLAN.

Static Router Ports Entry

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

A router port has the following behavior:

- All IGMP Report packets will be forwarded to the router port.
- IGMP queries (from the router port) will be flooded to all ports.
- All UDP multicast packets will be forwarded to the router port. Because routers do not send IGMP reports or implement IGMP snooping, a multicast router connected to the router port of the Layer 2 switch would not be able to receive UDP data streams unless the UDP multicast packets were all forwarded to the router port.

Click **Static Router Ports Entry** under the **IGMP** folder on the **Configuration** menu:
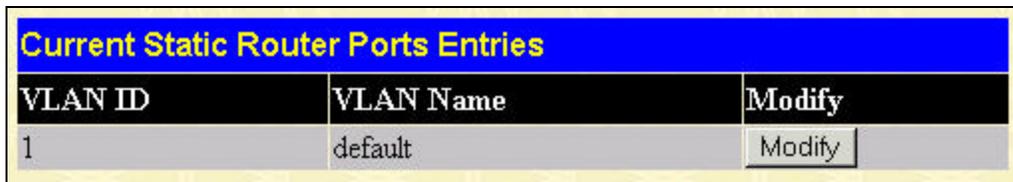
Figure 7 - 9. Current Static Router Ports Entries window

To add a static router port configuration, click the pointer icon:
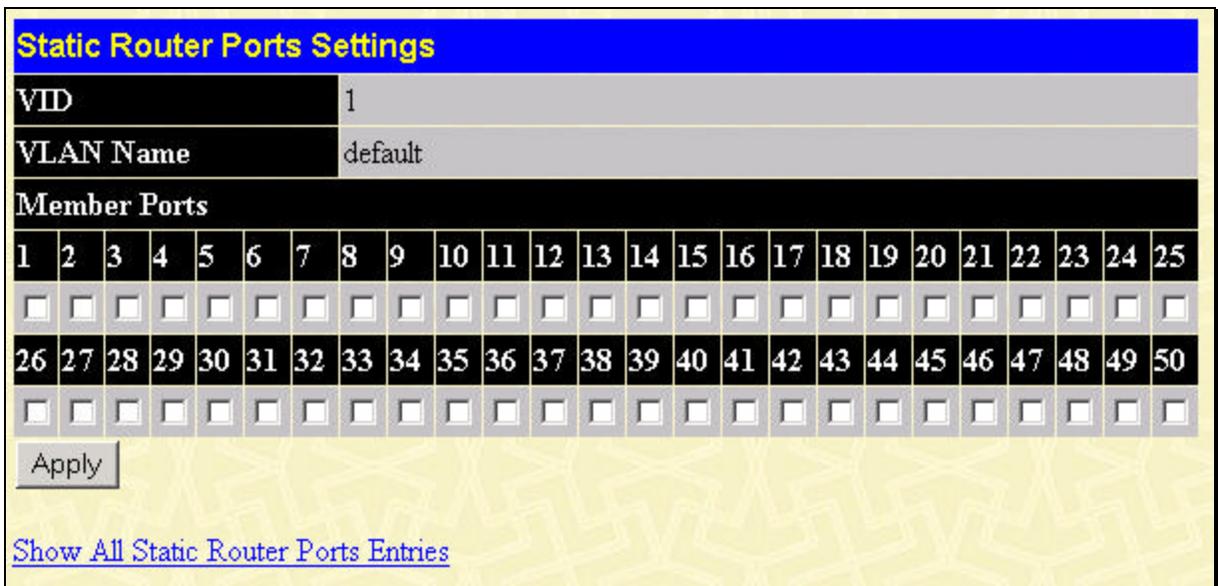
Figure 7 - 10. Static Router Ports Settings window

The following fields are displayed:

Parameter	Description
VID	Displays the name of the VLAN ID the static router port belongs to.
VLAN Name	Displays the name of the VLAN the static router port belongs to.
Member Ports	Each port can be set individually as a router port by clicking the port's click-box entry.

Spanning Tree

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

802.1w Rapid Spanning Tree

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

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1d STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 function that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the two protocols is in the way ports transition to a forwarding state and the in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. RSTP combines the transition states disabled, blocking, and listening used in 802.1d and creates a single state: discarding. In either case, ports do not forward packets; in the STP port transition states disabled, blocking, or listening, or in the RSTP port state discarding, there is no functional difference, the port is not active in the network topology. Table 5-1 below compares how the two protocols differ regarding the port state transition.

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

29

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

Edge Port

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

P2P Port

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

802.1d/802.1w Compatibility

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

STP Switch Settings

In the **Configuration** folder open the **Spanning Tree** folder, then click on the **STP Switch Settings** link.

Switch Spanning Tree Settings	
Spanning Tree Protocol	Enabled
Bridge Max Age (6-40 Sec)	20
Bridge Hello Time (1-10 Sec)	2
Bridge Forward Delay (4-30 Sec)	15
Bridge Priority (0-65535 Sec)	32768
STP Version	StpCompatiblility
TX Hold Count(1-10)	3
Forwarding BPDU	Enabled
	Apply
Designated Root Bridge	003350000100
Root Priority	8192
Cost to Root	200004
Root Port	5
Time Topology Change(secs)	760
Topology Changes Count	5
Protocol Specification	0
Max Age	20
Hello Time	2
Forward Delay	15
Hold Time	3

Note: 2*(Forward Delay-1) >= Max Age,
Max Age >= 2*(Hello Time +1)

Figure 7 - 11. Switch Spanning Tree Settings window

Note: The factory default setting should cover the majority of installations. It is advisable to keep the default settings as set at the factory unless it is absolutely necessary to change them.

The following fields can be set:

Parameter	Description
Spanning Tree Protocol *<Disabled>*	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. This will enable or disable the Spanning Tree Protocol (STP), globally, for the switch.
Bridge Max Age (6-40 Sec) *<20>*	The Bridge Maximum Age can be set from *6* to *40* seconds. At the end of the Max. Age, if a BPDU has still not been received from the Root Bridge, your switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge.
Bridge Hello Time (1-10 Sec) *< 2 >*	The Bridge Hello Time can be set from *1* to *10* seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge.
Bridge Forward Delay (4-30 sec) *<15>*	The Bridge Forward Delay can be from *4* to *30* seconds. This is the time any port on the switch spends in the listening state while moving from the blocking state to the forwarding state.
Bridge Priority (0-65535 Sec) *<32768>*	A Bridge Priority for the switch can be set from *0* to *65535*. This number is used in the voting process between switches on the network to determine which switch will be the root switch. A low number indicates a high priority, and a high probability that this switch will be elected as the root switch.
STP Version	Choose *rstp* or *StpCompatibility*. Both versions use STP parameters in the same way. RSTP is fully compatible with IEEE 802.1d STP and will function with legacy equipment.
TX Hold Count(1-10)	This is the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default value is *3*.
Forwarding BPDU *<Enabled>*	This allows you to control whether or not to forward Bridge Protocol Data Units. Disabling this setting can be useful if, for example, the present switch has been designated as the root bridge and you do not want that status to change.

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

Observe the following formulas when setting the above parameters:

> Max. Age = 2 x (Forward Delay - 1 second)
>
> Max. Age = 2 x (Hello Time + 1 second)

STP Port Settings

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

To configure STP, click the Spanning Tree folder on the Configuration menu and then click on the STP Port Settings link:

STP Port Settings

From	To	State	Cost	Priority	Migration	Edge	P2P	Apply
Port 1 ▾	Port 1 ▾	Disabled ▾	200000	128	No ▾	No ▾	No ▾	Apply

The STP Port Information

Port	Designated Bridge	State	Cost	Priority	Edge	P2P	STP Status	Role
1	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
2	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
3	N/A	Yes	*200000	128	No	Yes	Forwarding	NonStp
4	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
5	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
6	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
7	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
8	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
9	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
10	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
11	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
12	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
13	N/A	Yes	*200000	128	No	Yes	Forwarding	NonStp
14	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
15	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
16	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
17	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
18	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
19	N/A	Yes	*200000	128	No	Yes	Forwarding	NonStp
20	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
21	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
22	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
23	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
24	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
25	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
26	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
27	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
28	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
29	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled
30	N/A	Yes	*200000	128	No	Yes	Disabled	Disabled

Figure 7 - 12. STP Port Settings window

In addition to setting Spanning Tree parameters for use on the switch level, the switch allows for the configuration of a group of ports. This STP Group will use the switch-level parameters entered above, with the addition of Port Priority and Port Cost.

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

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

The following fields can be set:

Parameter	Description
From and **To**	Consecutive groups of ports may be configured starting with the selected port.
State<*Disabled*>	Toggle to enable STP on the selected ports.
Cost	A Port Cost can be set from *1* to *200000000*. The lower the number, the greater the

	probability the port will be chosen to forward packets.
	Default port cost:
	100Mbps port = 200000
	Gigabit ports = 20000
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 *<No>*	Select *Yes* or *No*. Choosing *Yes* will enable the port to migrate from 802.1d STP status to 802.1w RSTP status. RSTP can coexist with standard STP, however the benefits of RSTP are not realized on a port where an 802.1d network connects to an 802.1w enabled network. Migration should be enabled (*Yes*) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment.
Edge *<No>*	Select *Yes* or *No*. Choosing *Yes* designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. *No* indicates the port does not have edge port status.
P2P *<No>*	Select *Yes* or *No*. Choosing *Yes* indicates a point-to-point (p2p) shared link. These are similar to edge ports, however they are restricted in that a p2p port must operate in full duplex. Like edge ports, p2p ports transition to a forwarding state rapidly thus benefiting from RSTP.

Unicast Forwarding

To enter a MAC address into the switch's forwarding table, click on the **Forwarding Filtering** folder on the **Configuration** menu and then click **Unicast For warding**:

Figure 7 - 13. Setup Static Unicast Forwarding Table window

The following fields can be set:

Parameter	Description
VLAN ID	Allows the entry of the VLAN ID of the VLAN the MAC address below is a member of − when editing. Displays the VLAN ID the currently selected MAC address is a member of − when editing an existing entry.
MAC Address	Allows the entry of the MAC address of an end station that will be entered into the

switch's static forwarding table when adding a
new entry. Displays the currently selected
MAC address when editing.

Allowed to Go Port	Allows the selection of the port number on which the MAC address entered above resides.

Multicast Forwarding

Multicast MAC addresses can be statically entered into the switch's MAC Address Forwarding Table. These addresses will never age out.

To enter a Multicast MAC address into the switch's forwarding table, click on the **Forwarding Filtering** folder on the C**onfiguration** menu and then click **Multicast Forwarding**:
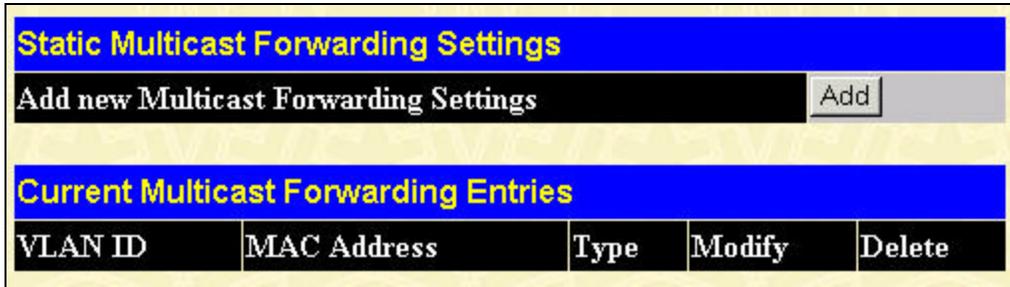
Figure 7 - 14. Static Multicast Forwarding Settings window

To add a new multicast MAC address to the Switch's forwarding table, click the **Add** button:
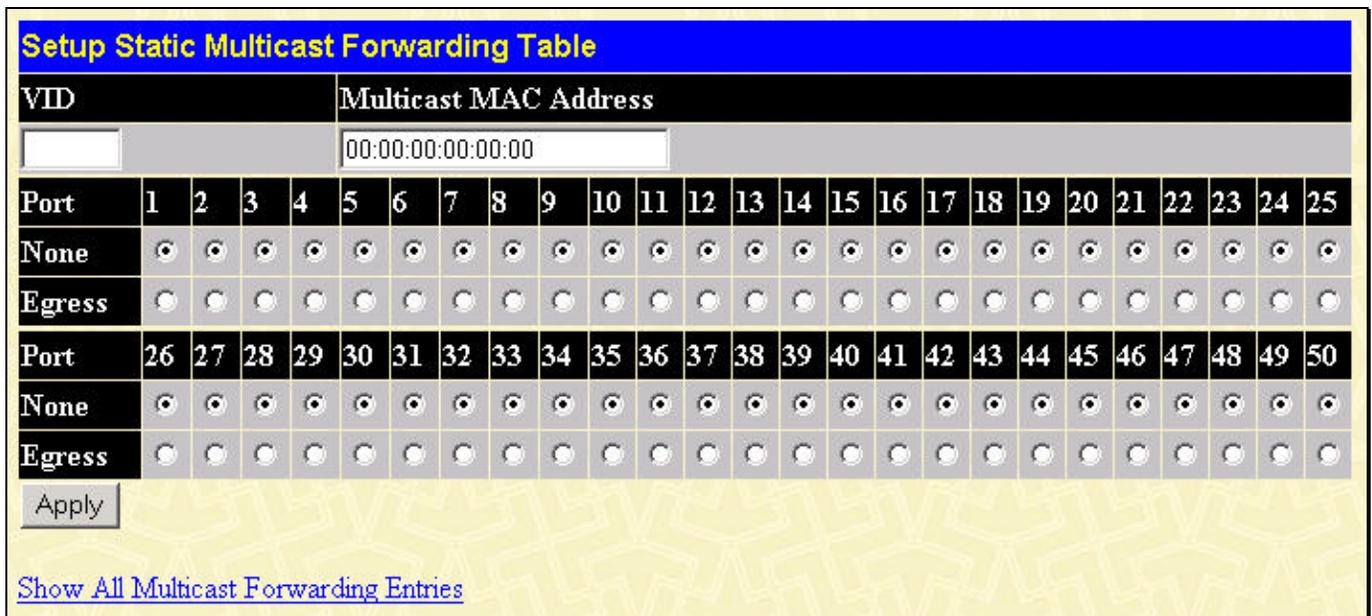
Figure 7 - 15. Setup Static Multicast Forwarding Table window

The following fields can be set:

Parameter	Description
VID	Allows the entry of the VLAN ID of the VLAN the MAC address below is a member of.
Multicast MAC Address	Allows the entry of the multicast MAC address of an end station that will be entered into the switch's static forwarding table.
Port	Select the port number on which the MAC address entered above resides.
None	Specifies the port as being none.
Egress	Specifies the port as being a source of multicast packets originating from the MAC address specified above.

VLANs

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

VLANs on the DES-3350SR

The DES-3350SR 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 (that is, network devices that do not support IEEE 802.1Q VLANs or tagging). The switch's default is to assign all ports to a single 802.1Q VLAN named "default."

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 DES-3350SR Layer 2 switch. 802.1Q VLANs require tagging, which enables the VLANs to span an entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

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

802.1Q VLAN Packet Forwarding

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

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

- Forwarding rules between ports – decides filter or forward the packet

- Egress rules – determines if the packet must be sent tagged or untagged.
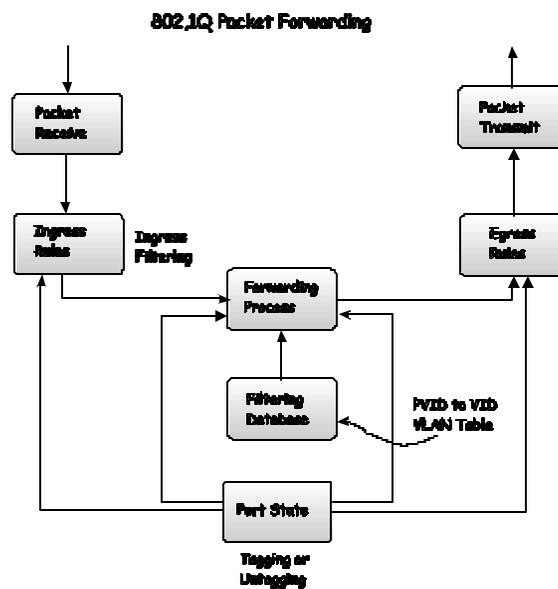
Figure 7 - 16. IEEE 802.1Q Packet Forwarding

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 or 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 four octets. All of the information contained in the packet originally is retained.
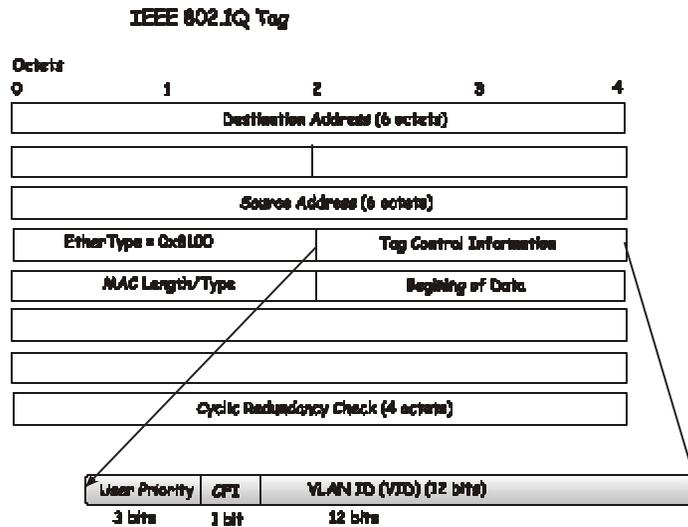
IEEE 802.1Q Tag

Figure 7 - 17. 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.

Adding an IEEE 802.1Q Tag
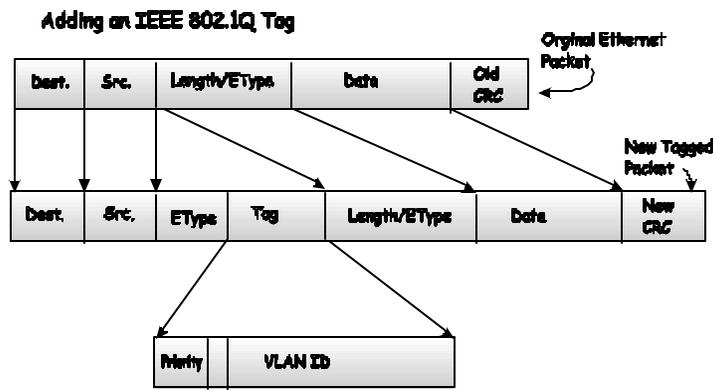
Figure 7 - 18. Adding an IEEE 802.1Q Tag

Static VLAN Entry

The VLAN menu adds an entry to edit the VLAN definitions and to configure the port settings for IEEE 802.1Q VLAN support. Go to the **Configuration** menu, select the **VLANs** folder, and click **Static VLAN Entry** to open the following window:
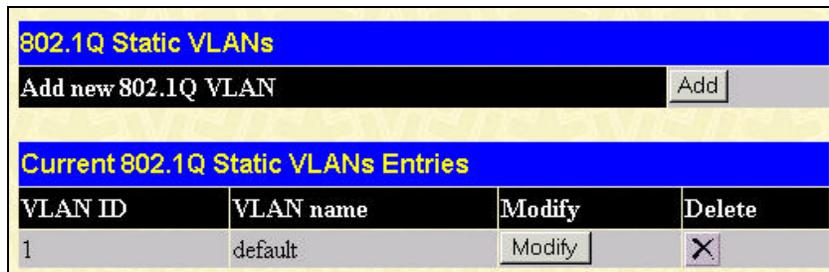
Figure 7 - 19. 802.1Q Static VLANs window

To delete an existing 802.1Q VLAN, click the corresponding click-box to the left of the VLAN you want to delete fro m the switch and then click the **Delete** button.

To create a new 802.1Q VLAN, click the **Add** button:

Figure 7 - 20. (Add) 802.1Q Static VLAN window

To edit an existing 802.1Q VLAN, click the corresponding **Modify** button on the 802.1Q Static VLANs window. The following window will open:

Figure 7 - 21. (Modify) 802.1Q Static VLAN window

The following fields can then be set in either of the two **802.1Q Static VLAN** windows:

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

Advertisement	Advertising can be enabled or disabled using this pull-down menu. Advertising allows members to join this VLAN through GVRP.
Port Settings	Allows an individual port to be specified as member of a VLAN.
Tagged/None	Allows an individual port to be specified as Tagging. A check in the Tagged field specifies the port as a Tagging member of the VLAN. When an untagged packet is transmitted by the port, the packet header is changed to include the 32-bit tag associated with the VID (VLAN Identifier – see below). When a tagged packet exits the port, the packet header is unchanged.
None	Allows an individual port to be specified as None. When an untagged packet is transmitted by the port, the packet header remains unchanged. When a tagged packet exits the port, the tag is stripped and the packet is changed to an untagged packet.
Egress	Egress Member - specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.
Forbidden	Forbidden Non-Member - specifies the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

Port VLAN ID(PVID)

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

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

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

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

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

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

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

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

Tagging and Untagging

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

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

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

Ingress Checking

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.

The "Default" VLAN

The switch initially configures one VLAN, VID = 1, called the "default" VLAN. The factory default setting assigns all ports on the switch to the "default" VLAN.

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

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

The **802.1Q Port Settings** window, shown below, allows you to determine whether the switch will share its VLAN configuration information with other **GVRP** (GARP VLAN Registration Protocol)-enabled switches. In addition, **Ingress Checking** can be used to limit traffic by filtering incoming packets whose **PVID** does not match the **PVID** of the port.

To view the **802.1Q Port Settings** window, open the **Configuration** menu, click on **VLAN**, and then click the **Port VLAN ID (PVID)**.

802.1Q Port Settings

From	To	PVID	GVRP	Ingress	Acceptable Frame Type	Apply
Port 1 ▼	Port 1 ▼	1	Disabled ▼	Disabled ▼	Tagged Only ▼	Apply

802.1Q Port Table

Port	PVID	GVRP	Ingress Checking	Acceptable Frame Type
1	1	Disabled	Enabled	Admit All
2	1	Disabled	Enabled	Admit All
3	1	Disabled	Enabled	Admit All
4	1	Disabled	Enabled	Admit All
5	1	Disabled	Enabled	Admit All
6	1	Disabled	Enabled	Admit All
7	1	Disabled	Enabled	Admit All
8	1	Disabled	Enabled	Admit All
9	1	Disabled	Enabled	Admit All
10	1	Disabled	Enabled	Admit All
11	1	Disabled	Enabled	Admit All
12	1	Disabled	Enabled	Admit All
13	1	Disabled	Enabled	Admit All
14	1	Disabled	Enabled	Admit All
15	1	Disabled	Enabled	Admit All
16	1	Disabled	Enabled	Admit All
17	1	Disabled	Enabled	Admit All
18	1	Disabled	Enabled	Admit All
19	1	Disabled	Enabled	Admit All
20	1	Disabled	Enabled	Admit All
21	1	Disabled	Enabled	Admit All
22	1	Disabled	Enabled	Admit All
23	1	Disabled	Enabled	Admit All
24	1	Disabled	Enabled	Admit All
25	1	Disabled	Enabled	Admit All
26	1	Disabled	Enabled	Admit All
27	1	Disabled	Enabled	Admit All
28	1	Disabled	Enabled	Admit All

Figure 7 - 22. 802.1Q Port Settings window

The following fields can be set:

Parameter	Description
From and **To**	Enter the desired ports in these two fields.
PVID	A Port VLAN Identifier is a classification mechanism that associates a port with a specific VLAN and is used to make forwarding decisions for untagged packets received by the port. For example, if port #2 is assigned a PVID of 3, then all untagged packets received on port #2 will be assigned to VLAN 3. This number is generally the same as the VID# number assigned to the port in the Modify 802.1Q VLANs menu above.

GVRP *<Disabled>*	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN.
Ingress *<Disabled>*	This field can be toggled using the space bar between *Enabled* and *Disabled*. *Enabled* enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. *Disabled* disables Ingress filtering.
Acceptable Frame Types	This field denotes the type of frame that will be accepted by the port. The user may choose between *Tagged Only*, which means only VLAN tagged frames will be accepted, and *Admit_All*, which means both tagged and untagged frames will be accepted. *Admit_All* is enabled by default.

To enable or disable GVRP, globally, on the switch:

Go to the **Configuration** menu and click **Advanced Settings**. Toggle the drop-down menu for GVRP Status between *Enabled* and *Disabled*. Click **Apply** to let your change take effect.

Port Bandwidth

The **Bandwidth Settings** window allows you to set and display the Ingress bandwidth and Egress bandwidth of specified ports on the switch.

Bandwidth Settings

From	To	Type	no_limit	Rate	Apply
Port 1 ▾	Port 1 ▾	RX ▾	Disabled ▾	1	Apply

Port Bandwidth Table

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

Figure 7 - 23. Bandwidth Settings window

To use the bandwidth feature, enter the port or range of ports in the **From** and **To** fields. The third field allows you to set the type of packets being received and/or transmitted by the Switch. Toggle the **no_limit** setting to *Enabled* in the fourth field, or if you prefer, manually enter a value in the **Rate** field, and then click **Apply**. Please note that if **no_limit** is *Enabled*, the Switch will not permit you to set the bandwidth rate manually.

SNTP Settings

The DES-3350SR supports Simple Network Time Protocol (SNTP), an adaptation of the Network Time Protocol (NTP). As specified in RFC-1305 [MIL92], NTP is used to synchronize computer clocks in the global Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet, and adjust the local clock in each participating subnet peer.

The access paradigm is identical to the UDP/TIME Protocol and, in fact, it is usually easy to adapt a UDP/TIME client implementation to operate using SNTP. Moreover, SNTP is also designed to operate in a dedicated server configuration including an integrated radio clock. With careful design and control of the various latencies in the system, it is possible to deliver time accurate to the order of microseconds.

Current Time Settings

To enable **SNTP** on the Switch, click **SNTP Settings** in the **Configuration** folder and then click **Current Time Settings**:

Figure 7 - 24. Current Time window

To use SNTP, toggle the SNTP State in the Current Time: SNTP Settings section to *Enabled* and enter the IP address of the relay the SNTP Primary Server and/or the SNTP Secondary Server. Enter an SNTP polling interval in the bottom field. The default setting of 720 seconds is usually fine for most network configurations; a greater polling frequency will draw more network resources. Click **Apply** to let your changes take effect.

To complete SNTP configuration, fill in the desired values in the Current Time: Set Current Time section and then click **Apply**.

Time Zone and DST

To make time zone and Daylight Savings Time changes to the SNTP configuration, click SNTP Settings in the Configuration folder and then click Time Zone and DST:

Figure 7 - 25. Time Zone and DST Settings window

This window allows you to set the Daily Saving Time repeated and annual settings. Click **Apply** to let your changes take effect.

Port Security

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

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

44

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

Port Security Table			
Port	Admin State	Max. Learning Addr.	Lock Address Mode
1	Disabled	1	DeleteOnReset
2	Disabled	1	DeleteOnReset
3	Disabled	1	DeleteOnReset
4	Disabled	1	DeleteOnReset
5	Disabled	1	DeleteOnReset
6	Disabled	1	DeleteOnReset
7	Disabled	1	DeleteOnReset
8	Disabled	1	DeleteOnReset
9	Disabled	1	DeleteOnReset
10	Disabled	1	DeleteOnReset
11	Disabled	1	DeleteOnReset
12	Disabled	1	DeleteOnReset
13	Disabled	1	DeleteOnReset
14	Disabled	1	DeleteOnReset
15	Disabled	1	DeleteOnReset
16	Disabled	1	DeleteOnReset
17	Disabled	1	DeleteOnReset
18	Disabled	1	DeleteOnReset
19	Disabled	1	DeleteOnReset
20	Disabled	1	DeleteOnReset
21	Disabled	1	DeleteOnReset
22	Disabled	1	DeleteOnReset
23	Disabled	1	DeleteOnReset
24	Disabled	1	DeleteOnReset
25	Disabled	1	DeleteOnReset
26	Disabled	1	DeleteOnReset
27	Disabled	1	DeleteOnReset
28	Disabled	1	DeleteOnReset
29	Disabled	1	DeleteOnReset
30	Disabled	1	DeleteOnReset
31	Disabled	1	DeleteOnReset

Figure 7 - 26. Port Security Settings window

The following fields can be set:

Parameter	Description
From & **To**	Use this to specify a consecutively numbered group of ports on the switch for configuration.
Admin State *<Disabled>*	Allows the selected port(s) dynamic MAC address learning to be locked such that new source MAC addresses cannot be entered into the MAC address table for the locked port or group of ports. It can be changed by toggling between *Disabled* and *Enabled*.
Max Learning Addr.(0-10) *<1 >*	Select the maximum number of addresses that may be learned for the port. The port can be restricted to 10 or less MAC addresses that are allowed for dynamically learned MAC addresses in the forwarding table.
Lock Address Mode *<Delete On Reset>*	Select *Delete On Timeout* to clear dynamic entries for the ports on timeout of the Forwarding Data Base (FDB). Specify *Delete On Reset* to delete all FDB entries, including static entries upon system reset or rebooting.

QOS (Quality of Service)

The DES-3350SR switch supports 802.1p priority queuing. The switch has four priority queues. These priority queues are numbered from 0 — the lowest priority queue — to 3 — the highest priority queue. The eight priority queues specified in IEEE 802.1p (Q0 to Q7) are mapped to the switch's priority queues as follows:

> Q2 and Q1 are assigned to the switch's Q0 queue.
>
> Q3 and Q0 are assigned to the switch's Q1 queue.
>
> Q5 and Q4 are assigned to the switch's Q2 queue.
>
> Q7 and Q6 are assigned to the switch's Q3 queue.

The switch's four priority queues are emptied in a round-robin fashion—beginning with the highest priority queue, and proceeding to the lowest priority queue before returning to the highest priority queue.

For strict priority-based scheduling, any packets residing in the higher priority queues are transmitted first. Only when these queues are empty, are packets of lower priority transmitted.

The weighted-priority based scheduling alleviates the main disadvantage of strict priority-based scheduling – in that lower priority queues get starved of bandwidth – by providing a minimum bandwidth to all queues for transmission. This is accomplished by configuring the maximum number of packets allowed to be transmitted from a given priority queue and the maximum amount of time a given priority queue 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 queues.

The possible range for maximum packets is: 0 to 255 packets.

The possible range for maximum latency is: 0 to 255 (in increments of 16 microseconds each).

Remember that the DES-3350SR has four priority queues (and thus four Classes of Service) for each port on the switch.

Traffic Control

This window allows you to manage traffic control on the switch.

Click **Traffic control** in the **QoS** folder on the **Configuration** menu:

Traffic Control Setting

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

Traffic Control Information Table

Group[ports]	Broadcast Storm	Multicast Storm	Destination Lookup Fail	Threshold
1[1-8]	Disabled	Disabled	Disabled	128
2[9-16]	Disabled	Disabled	Disabled	128
3[17-24]	Disabled	Disabled	Disabled	128
4[25-32]	Disabled	Disabled	Disabled	128
5[33-40]	Disabled	Disabled	Disabled	128
6[41-48]	Disabled	Disabled	Disabled	128
7[49]	Disabled	Disabled	Disabled	128
8[50]	Disabled	Disabled	Disabled	128

Figure 7 - 27. Traffic Control Setting window

The following fields can be set:

Parameter	Description
Group *<1>*	Select the desired group of ports from the drop-down menu.
Broadcast Storm *<Disabled>*	This field can be toggled between *Enabled* and *Disabled* using the drop-down menu. This enables or disables, globally, the

	Switch's reaction to Broadcast storms, triggered at the threshold set in the last field.
Multicast Storm *<Disabled>*	This field can be toggled between *Enabled* and *Disabled* using the drop-down menu. This enables or disables, globally, the Switch's reaction to Multicast storms, triggered at the threshold set above.
Destination Lookup Fail *<Disabled>*	This field can be toggled between *Enabled* and *Disabled* using the drop-down menu. This enables or disables, globally, the Switch's reaction to Destination Address Unknown storms, triggered at the threshold set above.
Threshold *<128>*	This is the value in units of packets per second, beyond which the ingress port for that block discards packets. Each port contains three counters, one each for Broadcast, Multicast, and Destination Lookup Fail packets. The counters are cleared every second. If the counter for a particular type of packet exceeds this threshold within one second, then further packets of that type will be dropped.

802.1p Default Priority

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

Click **802.1p default_priority** in the **QoS** folder on the **Configuration** menu:

802.1p default_priority Settings			
From	To	Priority(0~7)	Apply
Port 1 ▼	Port 1 ▼	0	Apply

802.1p default_priority Table	
Port	Priority
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1
17	1
18	1
19	1
20	1
21	1
22	1
23	1
24	1
25	1
26	1
27	1
28	1
29	1

Figure 7 - 28. 802.1p default_priority Settings window

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

802.1p User Priority

The DES -3350SR allows the assignment of a Class of Traffic to each of the 802.1p priorities.

Click **802.1p user_priority** in the **QoS** folder on the **Configuration** menu:

Figure 7 - 29. QoS Class of Traffic window

Once you have assigned a maximum number of packets and a maximum latency to a given Class of Service on the switch, you can then assign this Class to each of the eight levels of 802.1p priorities.

Scheduling

Click **QoS** on the **Configuration** menu, and then click **scheduling**:
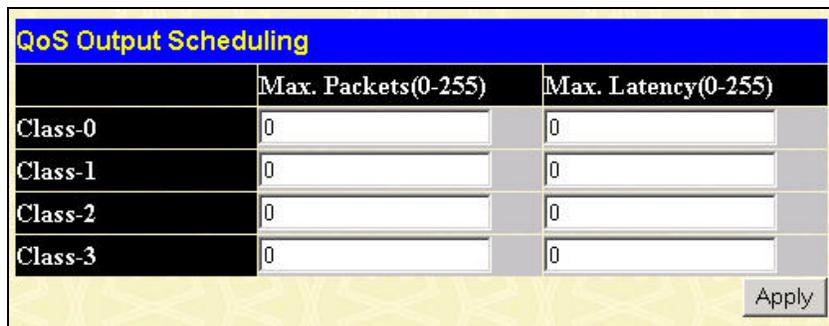
Figure 7 - 30. QoS Output Scheduling window

The Max. Packets(O-255) field specifies the number of packets that a queue will transmit before surrendering the transmit buffer to the next lower priority queue in a round-robin fashion.

The Max. Latency(0-255) field specifies the maximum amount of time that a queue will have to wait before being given access to the transmit buffer. The Max. Latency(0-255) is a priority queue timer. When it expires, it overrides the round-robin and gives the priority queue that it was set for access to the transmit buffer.

There is a small amount of additional latency introduced because the priority queue that is transmitting at the time the Max. Latency(0-255) time expires will finish transmitting its current packet before giving up the transmit buffer.

Traffic Segmentation

This window allows you to manage traffic segmentation on the switch.

Click **Traffic Segmentation** in the **QoS** folder on the **Configuration** menu:

**Figure 7 - 31. Traffic Segmentation Setting window**

Enter a source port number in the first field and the range of the ports that you want to segment in the second field. For examp le, if you enter "5" in the first field and "5-8" in the second field, packets from port 5 will only be forwarded to ports 5 to 8. Packets to port 9, then, will be dropped. Click **Apply** to let your changes take effect.

LACP

Link Aggregation

Link aggregation is used to combine a number of ports together to make a single high-bandwidth data pipeline. The participating parts are called members of a link aggregation group, with one port designated as the **master port** of the group. Since all members of the link aggregation group must be configured to operate in the same manner, the configuration of the master port is applied to all members of the link aggregation group. Thus, when configuring the ports in a link aggregation group, you only need to configure the master port.

The DES -3350SR supports link aggregation groups, which may include from two to eight switch ports each, except for a Gigabit link aggregation group which consists of the two (optional) Gigabit Ethernet ports of the front panel.
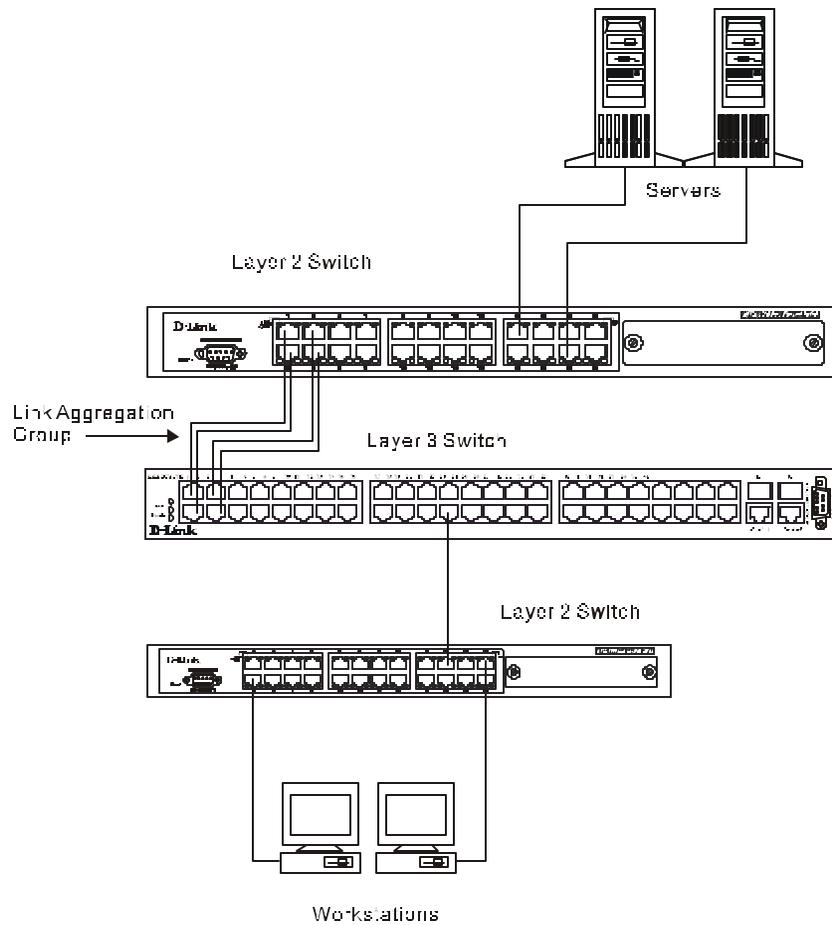
Figure 7 - 32. Link Aggregation Group

Data transmitted to a specific host (destination address) will always be transmitted over the same port in a link aggregation group. This allows packets in a data stream to arrive in the same order they were sent. An aggregated link connection can be made with any other switch that maintains host-to-host data streams over a single link aggregate port. Switches that use a load-balancing scheme that sends the packets of a host-to-host data stream over multiple link aggregation ports cannot have an aggregated connection with the DES-3350SR switch.

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

The switch allows the creation of up to six link aggregation groups, each group consisting of up to eight links (ports). All of the ports in the group must be members of the same VLAN. Further, the aggregated links must all be of the same speed and should be configured as full duplex.

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

To configure link aggregation, click on the **Link Aggregation** hyperlink in the **Configuration** folder to bring up the **Link Aggregation Group Entries** table:

Figure 7 - 33. Port Link Aggregation Group window

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

Figure 7 - 34. Port Link Aggregation Settings (Add) window

Figure 7 - 35. Port Link Aggregation Settings (Modify) window

The following fields can be set:

Parameter	Description
Group ID(1 -6)	Allows the entry of a number used to identify the link aggregation group – when adding a new group. Displays the Group ID of the currently selected link aggregation group – when editing and existing entry.
State *<Disabled>*	This field can be toggled between *Enabled* and *Disabled*. This is used to turn a link aggregation group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device, or to have an absolute backup link aggregation group that is not under automatic control.
Master Port *<Port 1 >*	The Master port of link aggregation group.
Member Port	Allows the specification of the ports that will make up the link aggregation group.

Type *<Static>*	Select *Static* or *LACP* (Link Aggregation Control Protocol).
Active Port	Shows the port that is currently forwarding packets.
Flooding Port	A trunking group must designate one port to allow transmission of broadcasts and unknown unicasts.

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

LACP Port

The DES-3350SR supports Link Aggregation Control Protocol. LACP allows you to bundle several physical ports together to form one logical port. After the LACP negotiation, these candidates for trunking ports can be trunked as a logical port. If any one of the connected port pairs does not have LACP capability, these two ports will stand as regular ports until the LACP negotiation is successfully completed. Like the traditional port trunking explained earlier in this manual, the member ports of an LACP trunk group can only be from a trunk with a peer LACP trunk group.

Lacp Port Settings

From	To	Mode	Apply
Port 1 ▾	Port 1 ▾	Passive ▾	Apply

Lacp Port Table

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

Figure 7 - 36. Link Aggregation Settings window

Enter the port range in the **From** and **To** fields, select the desired **Mode** in the next field, and then click **Apply** to let your changes take effect.

Access Profile Table

Access profiles allow you to establish criteria to determine whether the Switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of VLAN, MAC address or IP address.

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

Part 1

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

Figure 7 - 37. Access Profile Table

To add an entry to the **Access Profile Table**, click the **Add** button. This will open the **Access Profile Configuration** page, as shown below. There are three **Access Profile Configuration** pages; one for **Ethernet** (or MAC address-based) profile configuration, one for **IP** address-based profile configuration and one 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 Access Profile Configuration** page.

Ethernet

Figure 7 - 38. Access Profile Table (Ethernet)

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

Parameter	Description
Profile ID (1 -255)	Type in a unique identifier number for this profile set. This value can be set from 1 - 255.

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 priority value of each packet header and use this as the, or part of the criterion for forwarding.
Ethernet type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.
Port	The user may set the **Access Profile Table** on a per-port basis by entering a port number in this field. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon.

IP

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

Figure 7 - 39. Access Profile Configuration (IP)

The following parameters can be set, for IP:

Parameter	Description
Profile ID (1 -255)	Type in a unique identifier number for this profile set. This value can be set from 1 - 255.
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.

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 TCP port mask for the source port in hex form (hex 0x0-0xffff).

dest port mask - Specify a TCP 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).

Port	The user may set the **Access Profile Table** on a per-port basis by entering an entry in this field. Entering all will denote all ports on the Switch. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3 - 2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.

Packet Content Mask

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

Figure 7 - 40. Access Profile Configuration window (Packet Content Mask)

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 -255)	Type in a unique identifier number for this profile set. This value can be set from 1 -255.
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:

58

	value (0-15) - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte.
	value (16-31) – Enter a value in hex form to mask the packet from byte 16 to byte 31.
	value (32-47) – Enter a value in hex form to mask the packet from byte 32 to byte 47.
	value (48-63) – Enter a value in hex form to mask the packet from byte 48 to byte 63.
	value (64-79) – Enter a value in hex form to mask the packet from byte 64 to byte 79.
Port	The user may set the **Access Profile Table** on a per-port basis by entering an entry in this field. Entering all will denote all ports on the Switch. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3 - 2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.

Click **Apply** to implement changes made.

To establish the rule for a previously created Access Profile:

Part 2

IP

In the **Configuration** folder, click the **Access Profile Table** link to open the **Access Profile Table**. Under the heading **Access Rule**, clicking **Modify**, will open the following window.
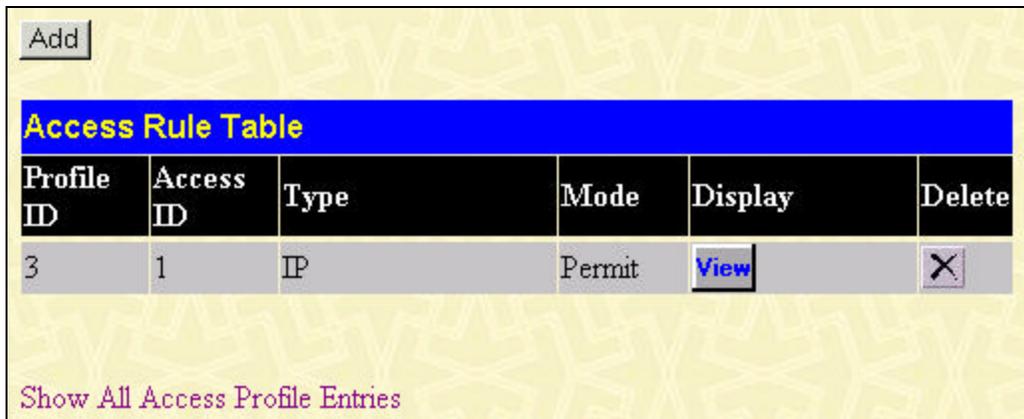
Figure 7 - 41. Access Rule Table window (IP)

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 [X] button.

Figure 7 - 42. Access Rule Configuration window (IP)

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

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

	to its original value before being forwarded by the Switch.
	For more information on priority queues, CoS queues and mapping for 802.1p, see the **QoS** section of this manual.
Replace Dscp (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
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)	Destination IP Address- Enter an IP Address mask for the destination IP address.
Protocol	This field allows the user to modify the protocol used to configure the **Access Rule Table;** depending on which protocol the user has chosen in the **Access Profile Table**.

To view the settings of a previously correctly configured rule, click View in the **Access Rule Table** to view the following screen:
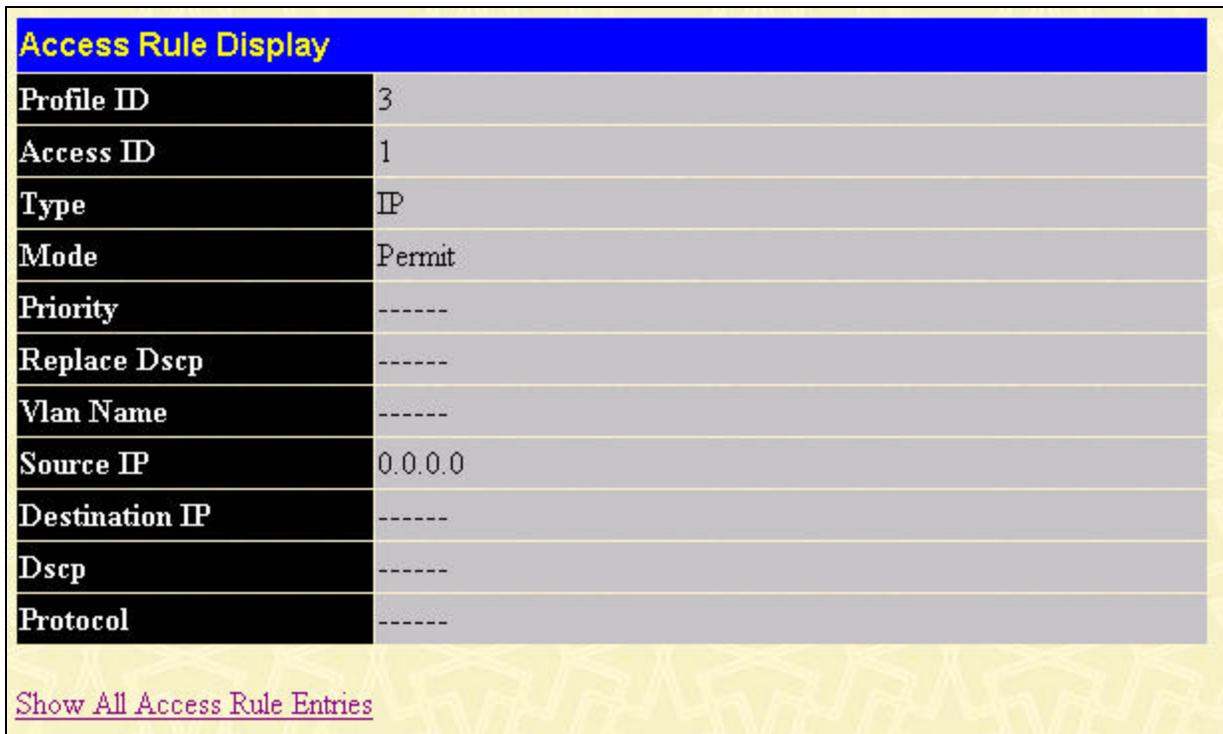
Figure 7 - 43. Access Rule Display window (IP)

Ethernet

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

Figure 7 - 44. Access Rule Table (Ethernet)

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

Figure 7 - 45. Access Rule Configuration window (Ethernet)

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

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Access ID	Type in a unique identifier number for this access. This value can be set from 1 - 50.
Mode	Select **Permit** to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).
	Select **Deny** to specify that packets that do not match the access profile are not forwarded by the Switch and will be filtered.
Priority(0-7)	This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.

	Replace priority with – Click the corresponding box if you want to re-write the 802.1p default priority of a packet to the value entered in the **Priority** field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.	
	For more information on priority queues, CoS queues and mapping for 802.1p, see the **QoS** section of this manual.	
VLAN Name	Allows the entry of a name for a previously configured VLAN.	
Source MAC	Source MAC Address - Enter a MAC Address for the source MAC address.	
Destination MAC	Destination MAC Address - Enter a MAC Address mask for the destination MAC address.	
802.1p (0-7)	Enter a value from 0-7 to specify that the access profile will apply only to packets with this 802.1p priority value.	
Ethernet Type	Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value (hex 0x0-0xffff) in the packet header. The Ethernet type value may be set in the form: hex 0x0-0xffff, which means the user may choose any combination of letters and numbers ranging from a-f and from 0-9999.	

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

Access Rule Display	
Profile ID	1
Access ID	1
Type	Ethernet
Mode	Permit
Priority	------
Vlan Name	------
Source Mac	------
Destination Mac	------
802.1p	------
Ethernet Type	------

Show All Access Rule Entries

Figure 7 - 46. Access Rule Display window (Ethernet)

Packet Content Mask

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

Figure 7 - 47. Access Rule Table (Packet Content Mask)

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

Figure 7 - 48. Access Rule Configuration window (Packet Content Mask)

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

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select **Permit** to specify that the packets that match the access profile are forwarded by the Switch, according to

any additional rule added (see below).

Access ID	Type in a unique identifier number for this access. This value can be set from 1 - 50.
Type	Selected profile based on Ethernet (MAC Address), IP address or Packet Content Mask.
	Ethernet instructs the Switch to examine the layer 2 part of each packet header.
	IP instructs the Switch to examine the IP address in each frame's header.
	Packet Content Mask instructs the Switch to examine the packet header.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified:
	value (0-15) - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte.
	value (16-31) - Enter a value in hex form to mask the packet from byte 16 to *byte 31.*
	value (32-47) - Enter a value in hex form to mask the packet from byte 32 to byte 47.
	value (48-63) - Enter a value in hex form to mask the packet from byte 48 to byte 63.
	value (64-79) - Enter a value in hex form to mask the packet from byte 64 to byte 79.

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

Figure 7 - 49. Access Rule Display window (Packet Content Mask)

IP-MAC Binding

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC addresses with the pre-configured database. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet. The maximum number of IP-MAC binding entries is dependant on chip capability (e.g. the ARP table size) and storage size of the device. For DES-3350SR, the maximum number of IP-MAC Binding entries is 512. 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 Binding Port

To enable or disable IP-MAC binding on specific ports, click **IP-MAC Binding Port** in the **IP-MAC Binding** folder on the **Configuration Menu** to open the **IP-MAC Binding Ports Setting** window. Select a port or a range of ports with the **From** and **To** fields. Enable or disable the port with the **State** field. Click **Apply** to save changes.

IP-MAC Binding Ports Setting

From	To	State	Apply
Port 1 ▾	Port 1 ▾	Disabled ▾	Apply

IP-MAC Binding Port State Table

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

Figure 7 - 50. IP-MAC Binding Ports window

IP-MAC Binding Table

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

IP-MAC Binding Setting

IP Address	0.0.0.0	MAC Address	00-00-00-00-00-00
		Add Modify Find Delete All	

Total Entries: 0

IP-MAC Binding Table

IP Address	MAC Address	Delete

Figure 7 - 51. IP-MAC Binding Table window

67

IP-MAC Binding Blocked

To view unauthorized devices that have been blocked by IP-MAC binding restrictions open the **IP-MAC Binding Blocked** window show below. Click **IP-MAC Binding Blocked** in the **IP-MAC Blocked** folder on the **Configuration** menu to open the **IP-MAC Binding Blocked** window.
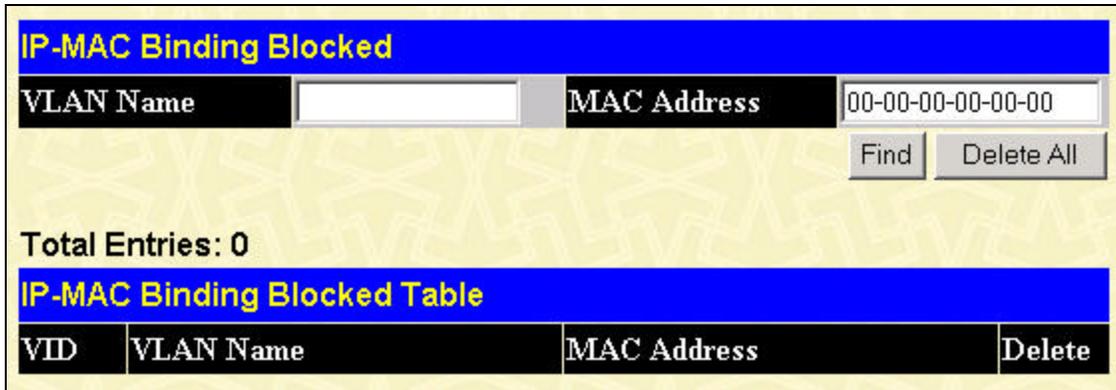
Figure 7 - 52. IP-MAC Binding Blocked window

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

Port Access Entity (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:
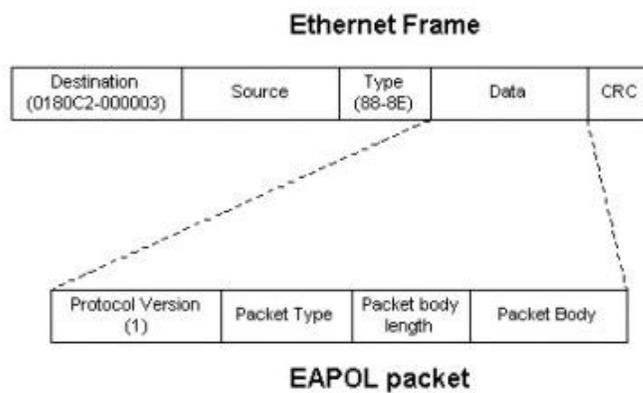
Figure 7 - 53. The EAPOL Packet

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 holds three roles, each of which are vital to creating and upkeeping a stable and working Access Control security method.
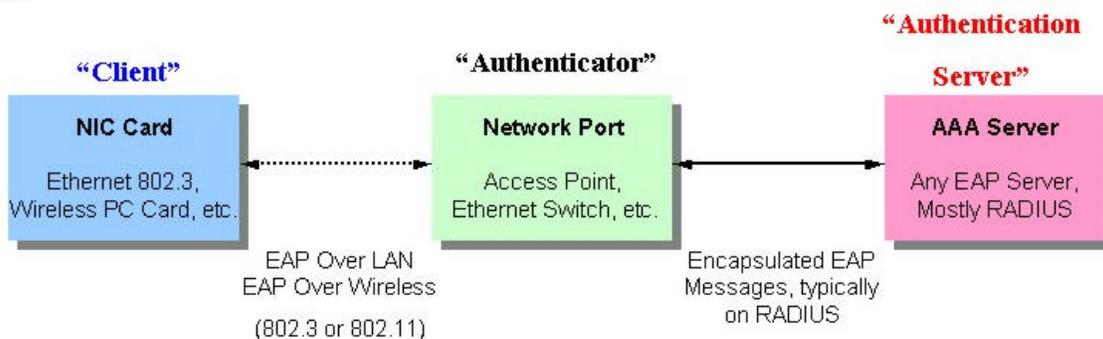
Figure 7 - 54. The three roles of 802.1x

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.
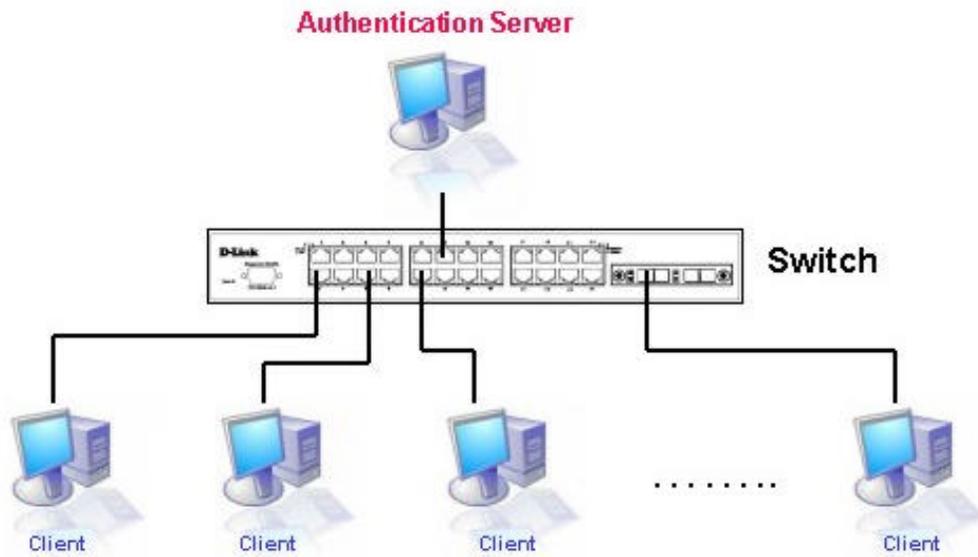
Figure 7 - 55. The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator servers 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. (Configuration / Advanced Settings)
2. The 802.1x settings must be implemented by port (Configuration / Port Access Entity / Configure Authenticator)
3. A RADIUS server must be configured on the Switch. (Configuration / Port Access Entity / RADIUS Server)
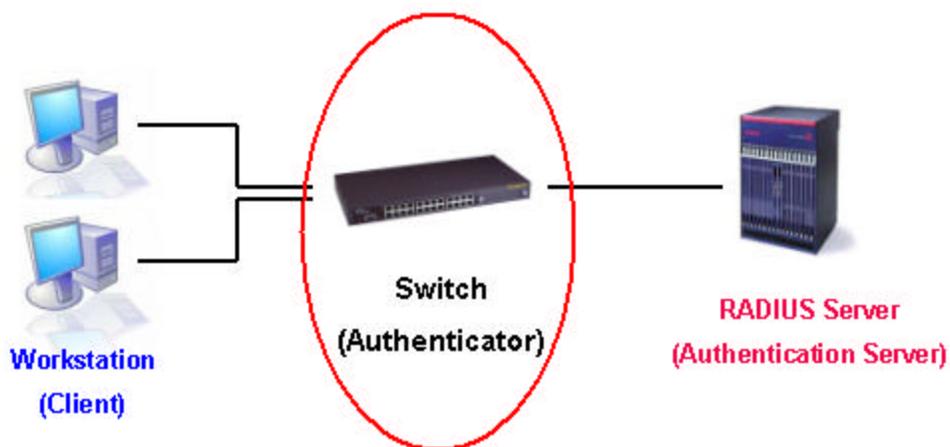
Figure 7 - 56. The Authenticator

Client

The Client is simply the endstation that wishes to gain access to the LAN or switch services. All endstations 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.
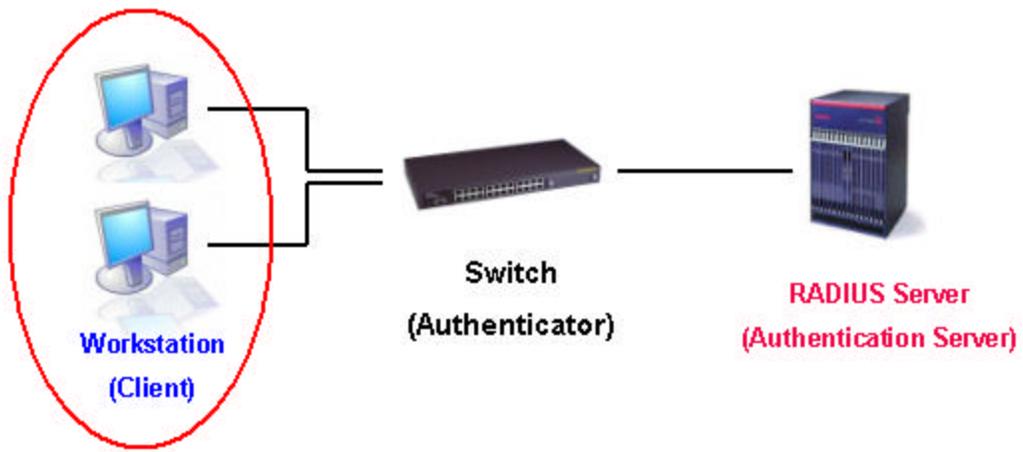
Figure 7 - 57. The Client

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 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 7 - 58. 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 three 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
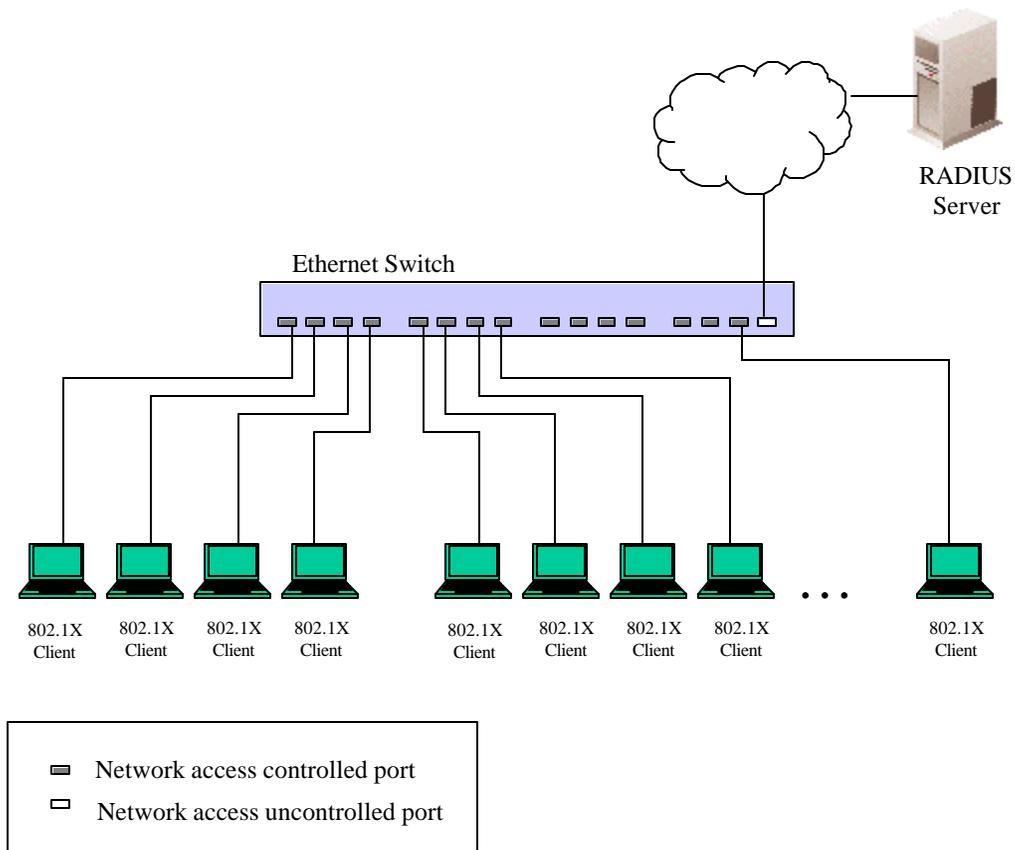
Figure 7 - 59. Example of Typical Port-Based Configuration

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
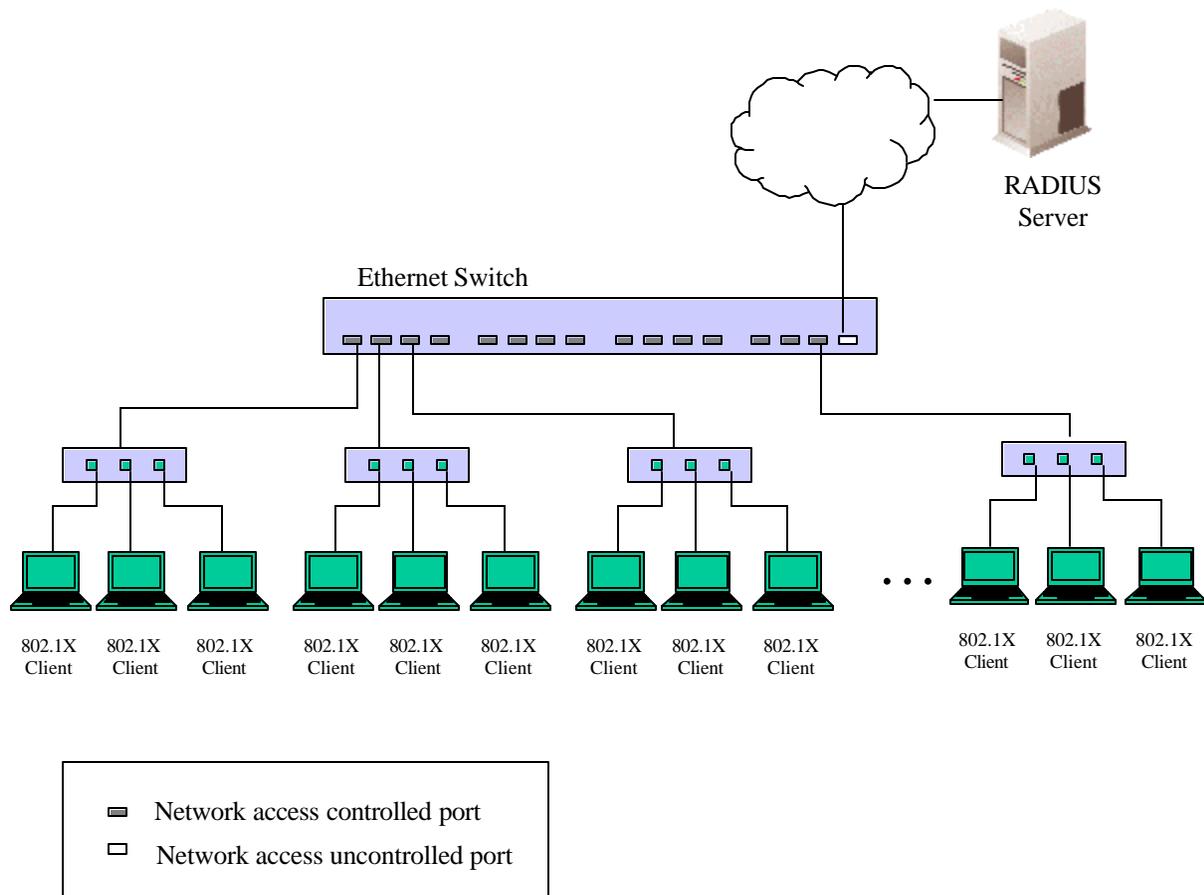
Figure 7 - 60. Example of Typical MAC-Based Configuration

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

Configure Authenticator

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

Click **Configure Authenticator** on the **PAE Access Entity** folder on the **Configuration** menu to open the **802.1X Authenticator Settings** window:

802.1X Authenticator Settings

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

Figure 7 - 61. First 802.1X Authenticator Settings window

Click the selection button on the far left that corresponds to the port you want to configure. Use the **Authenticator Settings** window shown below to configure settings on individual ports or on a range of ports.

802.1X Authenticator Settings

From	Port 6
To	Port 6
AdmDir	both
PortControl	forceUnauthorized
TxPeriod	30
QuietPeriod	60
SuppTimeout	30
ServerTimeout	30
MaxReq	2
ReAuthPeriod	3600
ReAuth	Disabled

Show Authenticators Setting   Apply

Figure 7 - 62. Second 802.1X Authenticator Settings window

Configure the following 802.1x port settings:

Parameter	Description
Port	Port being configured for 802.1x settings.
AdmDir	From the pull-down menu, select whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.
Ctl Stat	This displays whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.
PortControl	From the pull-down menu, select *forceAuthorized*, *forceUnauthorized* or *auto* – Force Authorized forces the Authenticator of the port to become Authorized. Force Unauthorized forces the port to become Unauthorized.
TxPeriod	Select the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.
QuietPeriod	Select the time interval between authentication failure and the start of a new authentication attempt.
SuppTimeout	Select the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.
ServerTimeout	Select the length of time to wait for a response from a Radius server.
MaxReq	Select the maximum number of times to retry sending packets to the supplicant.
ReAuthPeriod	Select the time interval between successive re-authentications.
ReAuth	Enable or disable re-authentication.

Port Capability Settings

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

Click **Port Capability Settings** on the **PAE Access Entity** folder on the **Configuration** menu to open the **802.1X Capability Settings** window:

Figure 7 - 63. 802.1X Capability Settings window

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

Configure the following 802.1x port 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 is not controlled by the 802.1x functions.

Initialize Ports for Port Based 802.1x

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

Click **Initialize Port(s)** on the **PAE Access Entity** folder on the **Configuration** menu to open the Initialize Port window:

Figure 7 - 64. Initialize Port for Port Based 802.1x window

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

This window displays the following information:

Parameter	Description
Port	The port number.
MAC Address	The MAC address of the switch where the port resides.
Auth PAE State	The Authenticator PAE State will display one of the following: *Initialize*, *Disconnected*, *Connecting*, *Authenticating*, *Authenticated*, *Aborting*, *Held*, *ForceAuth*, *ForceUnauth*, and *N/A*.
Backend_State	The Backend Authentication State will display one of the following: *Request*, *Response*, *Success*, *Fail*, *Timeout*, *Idle*, *Initialize*, and *N/A*.
Oper Dir	The Operational Controlled Directions are *both* and *in.*
PortStatus	The status of the controlled port can be *authorized*, *unauthorized*, or *N/A*.

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

Figure 7 - 65. Initialize Ports for MAC Based 802.1x window

To initialize ports, first choose the switch in the switch stack by using the Unit pull-down menu, then 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** Advanced Settings **window in the** Configuration **folder before initializing ports. Information in the** Initialize Ports Table **cannot be viewed before enabling 802.1X.**

Reauthenticate Ports for Port Based 802.1x

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

Click **Reauthenticate Port(s)** on the **PAE Access Entity** folder on the **Configuration** menu to open the Reauthenticate Port(s) window:

Reauthenticate Port

From	To	Apply
Port 1 ▾	Port 1 ▾	Apply

Reauthenticate Port Table

Port	MAC Address	Auth State	BackendState	OperDir	PortStatus

Figure 7 - 66. Reauthenticate Port window

This window displays the following information:

Parameter	Description
Port	The port number.
MAC Address	The MAC address of the switch where the port resides.
Auth State	The Authenticator State will display one of the following: *Initialize*, *Disconnected*, *Connecting*, *Authenticating*, *Authenticated*, *Aborting*, *Held*, *ForceAuth*, ForceUnauth, and *N/A*.
BackendState	The Backend State will display one of the following: *Request*, *Response*, *Success*, *Fail*, *Timeout*, *Idle*, *Initialize,* and *N/A*.
Oper Dir	The Operational Controlled Directions are *both* and *in*.
PortStatus	The status of the controlled port can be *authorized*, *unauthorized*, or *N/A*.

Reauthenticate Ports 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. Click **Configuration > Port Access Entity > PAE System Control > Reauthenticate Port(s)** to open the following window:

Reauthenticate Port(s)

From	Port 1 ▾
To	Port 1 ▾
Mac Address	☐ 00:00:00:00:00:00
	Apply

Figure 7 - 67. Reauthenticate Port(s) for MAC-based 802.1x window

To reauthenticate ports, first choose the switch in the switch stack by using the **Unit** pull-down menu, then 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.

Click **Radius Server** on the **PAE Access Entity** folder on the **Configuration** menu to open the **Radius Server Authentication Setting** window:

Figure 7 - 68. Radius Server Authentication Setting window

This window displays the following information:

Parameter	Description
Succession *<First>*	Choose the desired RADIUS server to configure: *First*, *Second* or *Third*.
Radius Server *<0.0.0.0>*	Set the RADIUS server IP.
Authentic Port *<0>*	Set the RADIUS authentic server(s) UDP port. The default is *1812*.
Accounting Port *<0>*	Set the RADIUS account server(s) UDP port. The default is *1813*.
Key	Set the key the same as that of the RADIUS server.
Confirm Key	Confirm the shared key is the same as that of the RADIUS server.
Accounting Method	This allows you to either *Add/Modify* or *Delete* an entry on the table in the bottom half of this window.

<div style="border: 1px solid black; text-align: center">

Section 8

</div>

Management

> ***Security IP***
> ***User Accounts***
> ***SNMP V3***

This section, arranged by topic, describes how to manage the DES -3350SR via the **Management** menu.

Security IP

Some settings must be entered to allow the switch to be managed from an SNMP-based Network Management System such as SNMP v1 or to be able to access the Switch using the Telnet protocol or the Web Manager.

To setup the switch for remote management:

Click the **Security IP** link in the **Management** menu:
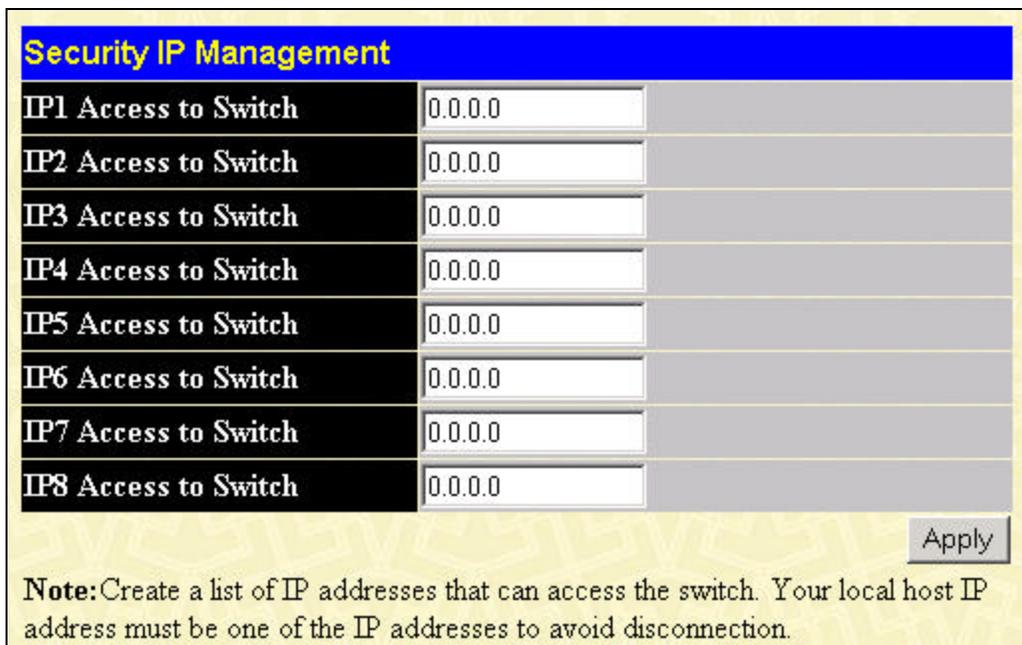
Figure 8 - 1. Security IP Management window

Management stations are computers on the network that will be used to manage the switch. You can limit the number of possible management stations by entering up to eight IP addresses. If the eight IP Address fields contain all zeros ("0"), then any station with any IP address can access the switch to manage and configure it. If there is one or more IP addresses entered in the IP Address fields, then only stations with the IP addresses entered will be allowed to access the switch to manage or configure it.

User Accounts

From the **Management** menu, click **User Accounts** and then the **User Account Management** window appears.

Figure 8 - 2. User Account Management window

Click **Add** to add a user.

Figure 8 - 3. User Account Modify Table window

1. Enter the new user name, assign an initial password, and then confirm the new password. Determine whether the new user should have *Admin* or *User* privileges.

2. Click **Apply** to make the user addition effective.

3. A listing of all user accounts and access levels is shown in the **User Account Management** window. This list is updated when Apply is executed. Click **Show All User Account Entries** to access this window.

Please remember that Apply makes changes to the switch configuration for the *current session only*. All changes (including User additions or updates) must be entered into non-volatile ram using the **Save Changes** command on the **Maintenance** menu - if you want these changes to be permanent.

SNMPV3

The DES-3350SR supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The SNMP version used to monitor and control the switch can be specified by the administrator. The three versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP settings are configured using the 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** window.

SNMP User Table

Use the SNMP User Table to create a new SNMP user and add the user to an existing SNMP group or to a newly created group.
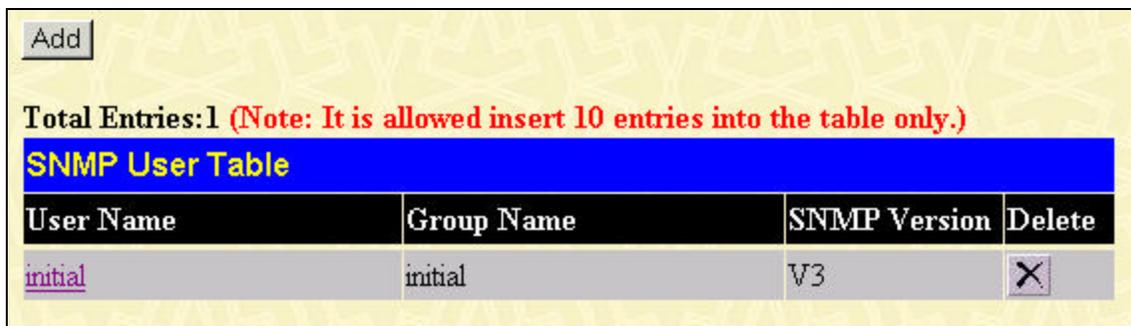
Figure 8 - 4. SNMP User Table window

To delete an existing entry, click the selection button in the Delete column on the far right that corresponds to the entry you want to configure. To create a new entry, click the **Add** button, a separate window will appear.

Figure 8 - 5. SNMP User Table Configuration window

81

To display the current SNMP User Table Configuration, click the User Name in the first column of the SNMP User Table window.

Figure 8 - 6. SNMP User Table Display window

The following parameters are used in the SNMP User Table windows:

Parameter	Description
User Name	Type in the new SNMP V3 user name or community string for V1 or V2. This can be any alphanumeric name of up to 32 characters that will identify the new SNMP user.
Group Name	Type in the new SNMP V3 group name. Again, this can be any alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.
SNMP Version	From the pull-down menu select:
	V1 – To specifies that SNMP version 1 will be used.
	V2 – To specify that SNMP version 2 will be used.
	V3 – To specify that the SNMP version 3 will be used.
If Encryption (V3 only) is checked configure also: **Auth-Protocol**	In the Space provided, type an alphanumeric sting of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host.
	From the pull-down menu select:
	MD5 – To specify that the HMAC-MD5-96 authentication level will be used.
	SHA – To specify that the HMAC-SHA-96 authentication level will be used.
If Encryption (V3 only) is checked configure also: **Priv-Protocol**	In the Space provided, type an alphanumeric string of between 8 and 16 characters that will be used to encrypt the contents of messages the host sends to the agent.

SNMP View Table

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

Figure 8 - 7. SNMP View Table window

To delete an existing SNMP View Table entry, click the selection button in the Delete column on the far right that corresponds to the port you want to configure. To create a new entry, click the **Add** button, a separate window will appear.

Figure 8 - 8. SNMP View Table Configuration window

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.

SNMP Group Table

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

Figure 8 - 9. SNMP Group Table window

To delete an existing entry, click the selection button in the Delete column on the far right that corresponds to the port you want to remove. To create a new entry, click the **Add** button, a separate window will appear.

Figure 8 - 10. SNMP Group Table Configuration window

To display the current SNMP Group Table Configuration, click the Group Name in the first column of the SNMP Group Table window.

Figure 8 - 11. SNMP Group Table Display window

The following parameters are used in the SNMP Group Table windows:

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

84

	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	Use the pull-down menu to select the SNMP version. Select one of the following:
	SNMPv1 – Specifies that SNMP version 1 will be used.
	SNMPv2 – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.
	SNMPv3– Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network.
Security Level	Use the pull-down menu to select the SNMP version:
	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.

SNMP Community Table

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

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

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

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

Figure 8 - 12. SNMP Community Table Configuration window

To delete an existing entry, click the selection button in the Delete column on the far right that corresponds to the port you want to configure. To create a new entry, configure the parameters as desired in the top part of the window above and click the **Apply** button. This will add the new string to the SNMP Community Table.

Configure the following for the new SNMP Community entry:

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	Use the pull-down menu to select the access right: *Read_Only* – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the switch. *Read_Write* – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the switch.

SNMP Host Table

Use the SNMP Host Table to set up trap recipients.
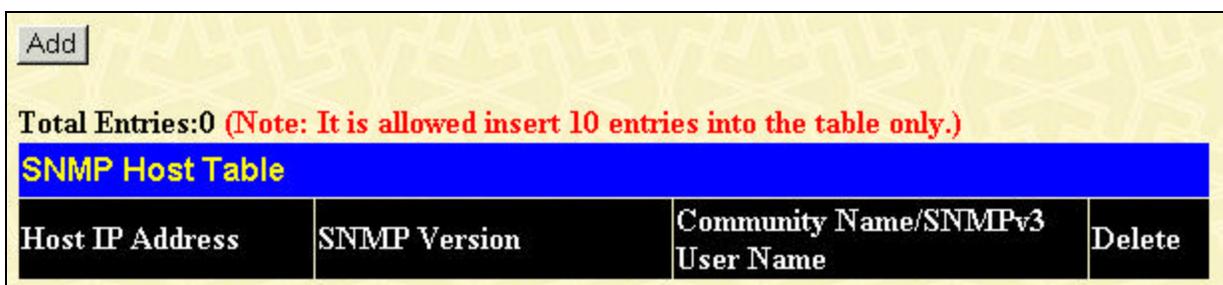
Figure 8 - 13. SNMP Host Table window

To delete an existing entry, click the selection button in the Delete column on the far right that corresponds to the port you want to remove. To create a new entry, click the **Add** button, a separate window will appear.
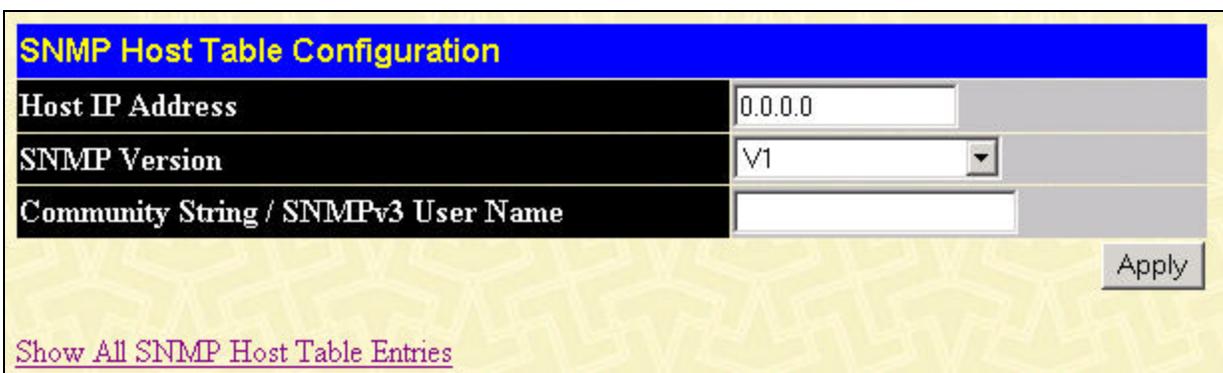
Figure 8 - 14. SNMP Host Table Configuration window

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	From the pull-down menu select:
	V1 – To specifies that SNMP version 1 will be used.
	V2c – To specify that SNMP version 2 will be used.
	V3 – To specify that the SNMP version 3 will be used.
Community String/SNMPv3 User Name	Type in the community string or SNMP V3 user name as appropriate.

SNMP Engine ID

The Engine ID is a unique identifier used for SNMP V3 implementations. This is an alphanumeric string used to identify the SNMP engine on the switch.
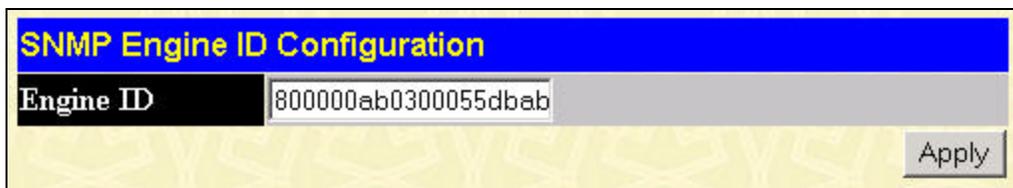
Figure 8 - 15. SNMP Engine ID Configuration window

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

Section 9

Layer 3 IP Networking

> **IP Interface Settings**
> **Layer 3 Global Settings**
> **MD5 Key Table Settings**
> **Route Redistribution Settings**
> **Static/Default Route Settings**
> **Static ARP Settings**
> **RIP**
> **OSPF**
> **DHCP/Bootp Relay**
> **DNS Relay**
> **IP Multicast Routing Protocol**

This section, arranged by topic, describes how to perform common configuration tasks at the OSI Layer 3 level on the DES-3350SR switch using the Web-based Manager.

IP Interface Settings

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

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineer	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4
Backbone	6	25, 26

Table 9 - 1. VLAN Example - Assigned Ports

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

Using a 10.xxx.xxx.xxx IP address notation, the above example would give 6 network addresses and 6 subnets.

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

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

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

Table 9 - 2. VLAN Example - Assigned IP Interfaces

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

To setup IP Interfaces on the Switch:

Go to the Configuration folder, and click on the Layer 3 IP Networking folder, and then click on the IP Interfaces Settings link to open the following dialog box:

Figure 9 - 1. IP Interface Table window

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

Figure 9 - 2. IP Interface Settings – Add

Figure 9 - 3. IP Interface Settings - Edit

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

The following fields can be set:

Parameters	Description
Interface Name	This field displays the name for the IP interface. The default IP interface is named "System".
IP Address	This field allows the entry of an IP address to be assigned to this IP interface.
Subnet Mask	This field allows the entry of a subnet mask to be applied to this IP interface.
VLAN Name	This field allows the entry of the VLAN Name for the VLAN the IP interface belongs to.

State	This field may be altered between *Enabled* and *Disabled* using the pull down menu. This entry determines whether the interface will be active or not.

Layer 3 Global Settings

The **L3 Global Settings window** allows the user to enable and disable Layer 3 settings and functions from a single window. To view this window, open the **Configuration** folder and then the **Layer 3 IP Networking folder** and click on the **L3 Global Settings** link to access the following window.
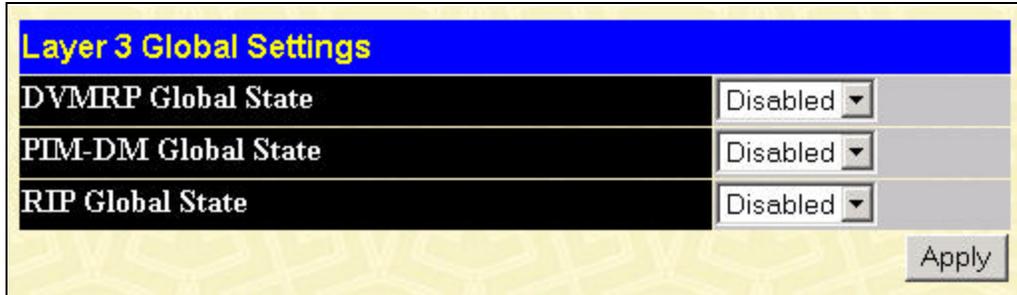
Figure 9 - 4. Layer 3 Global Settings window

The user may set the following:

Parameters	Description
DVMRP State	The user may globally enable or disable the Distance Vector Multicast Routing Protocol (DVMRP) function by using the pull down menu.
PIM-DM State	The user may globally enable or disable the Protocol Independent Multicast - Dense Mode (PIM-DM) function by using the pull down menu.
RIP State	The user may globally enable or disable the Routing Information Protocol (RIP) function by using the pull down menu.

Click **Apply** to implement changes made.

MD5 Key Table Settings

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

MD5 Keys created here can be used in the **OSPF** menu below.

To configure an **MD5 Key**, click the **MD5 Key Table Settings** on the **Layer 3 IP Networking** folder.

Figure 9 - 5. MD5 Key Setting and Table window

The following fields can be set:

Parameters	Description

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

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

Route Redistribution Settings

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

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

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

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

Entering the metric 0 specifies transparency.

This window will redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. To access the **Route Redistribution Settings** window, go to **Configuration > Layer 3 IP Networking > Route Redistribution Settings**:
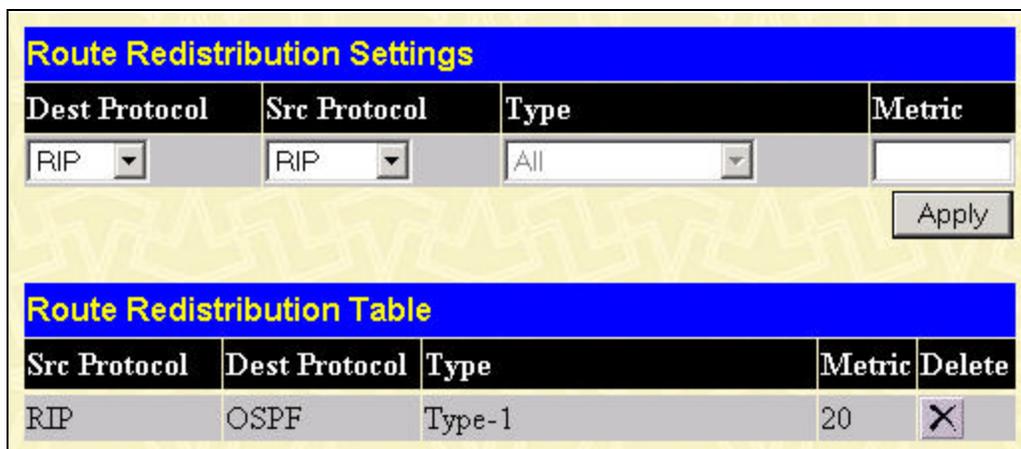
Figure 9 - 6. Route Redistribution Settings and Table window

The following parameters may be set or viewed:

Parameters	Description
Dest Protocol	Allows for the selection of the protocol for the destination device. Choose between *RIP* and *OSPF.*

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

Click **Apply** to implement changes made.

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

Static/Default Route Settings

Entries into the Switch's forwarding table can be made using both MAC addresses and IP addresses. Static IP forwarding is accomplished by the entry of an IP address into the Switch's Static IP Routing Table. To view the following window, click Configuration > Layer 3 IP Networking > Static/Default Route Settings.

Static/Default Route Settings						
IP Adderss	**Subnet Mask**	**Gateway**	**Cost**	**Protocol**	**Backup Status**	**Delete**
10.0.0.0	255.0.0.0	10.1.1.254	1	Static	Primary	✕

Figure 9 - 7. Static/Default Route Settings window

This window shows the following values:

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

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

Figure 9 - 8. Routing Table – Add window

The following fields can be set:

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

Click **Apply** to implement changes made.

Static ARP Settings

The *Address Resolution Protocol* (**ARP**) is a TCP/IP protocol that converts IP addresses into physical addresses. This table allows network managers to view, define, modify and delete ARP information for specific devices. Static entries can be defined in the **ARP Table**. When static entries are defined, a permanent entry is entered and is used to translate IP address to MAC addresses. To open the **Static ARP Table** open the **Configuration** folder, and then open the **Layer 3 IP Networking** folder and click on the **Static ARP Settings** link.

Figure 9 - 9. Static ARP Settings window

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

Static ARP Table - Add a New Entry

IP Address	0.0.0.0
MAC Address	00:00:00:00:00:00

Apply
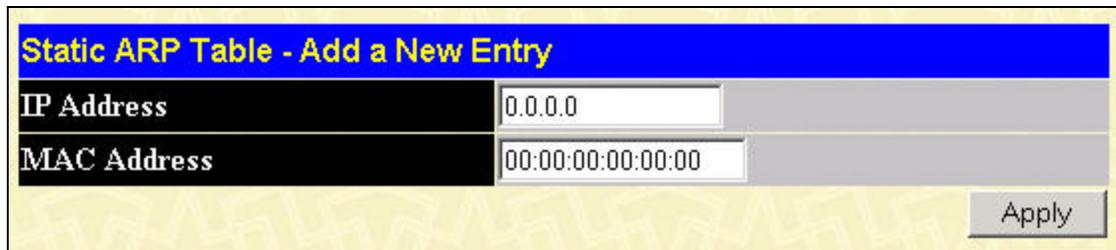
Figure 9 - 10. Static ARP Table – Add window

The following fields can be set or viewed:

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

After entering the IP Address and MAC Address of the **Static ARP** entry, click **Apply** to implement the new entry.

RIP

The Routing Information Protocol is a distance-vector routing protocol. There are two types of network devices running RIP - active and passive. Active devices advertise their routes to others through RIP messages, while passive devices listen to these messages. Both active and passive routers update their routing tables based upon RIP messages that active routers exchange. Only routers can run RIP in the active mode. Every 30 seconds, a router running RIP broadcasts a routing update containing a set of pairs of network addresses and a distance (represented by the number of hops or routers between the advertising router and the remote network). So, the vector is the network address and the distance is measured by the number of routers between the local router and the remote network. RIP measures distance by an integer count of the number of hops from one network to another. A router is one hop from a directly connected network, two hops from a network that can be reached through a router, etc. The more routers between a source and a destination, the greater the RIP distance (or hop count). There are a few rules to the routing table update process that help to improve performance and stability. A router will not replace a route with a newly learned one if the new route has the same hop count (sometimes referred to as 'cost'). So learned routes are retained until a new route with a lower hop count is learned. When learned routes are entered into the routing table, a timer is started. This timer is restarted every time this route is advertised. If the route is not advertised for a period of time (usually 180 seconds), the route is removed from the routing table. RIP does not have an explicit method to detect routing loops. Many RIP implementations include an authorization mechanism (a password) to prevent a router from learning erroneous routes from unauthorized routers. To maximize stability, the hop count RIP uses to measure distance must have a low maximum value. Infinity (that is, the network is unreachable) is defined as 16 hops. In other words, if a network is more than 16 routers from the source, the local router will consider the network unreachable.

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

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

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

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

RIP Version 1 Message Format

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

The Command field specifies an operation according to the following table:

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

94

9	Update Request
10	Update Response
11	Update Acknowledgement

RIP Command Codes

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

RIP 1 Message

RIP is not limited to TCP/IP. Its address format can support up to 14 octets (when using IP, the remaining 10 octets must be zeros). Other network protocol suites can be specified in the Family of Source Network field (IP has a value of 2). This will determine how the address field is interpreted. RIP specifies that the IP address, 0.0.0.0, denotes a default route. The distances, measured in router hops are entered in the Distance to Source Network, and Distance to Destination Network fields.

RIP 1 Route Interpretation

RIP was designed to be used with classed address schemes, and does not include an explicit subnet mask. An extension to version 1 does allow routers to exchange subnetted addresses, but only if the subnet mask used by the network is the same as the subnet mask used by the address. This means the RIP version 1 cannot be used to propagate classless addresses. Routers running RIP version 1 must send different update messages for each IP interface to which it is connected. Interfaces that use the same subnet mask as the router's network can contain subnetted routes, other interfaces cannot. The router will then advertise only a single route to the network.

RIP Version 2 Extensions

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

RIP2 Message Format

The message format used with RIP2 is an extension of the RIP1 format. RIP version 2 also adds a 16-bit route tag that is retained and sent with router updates. It can be used to identify the origin of the route. Because the version number in RIP2 occupies the same octet as in RIP1, both versions of the protocols can be used on a given router simultaneously without interference.

RIP Interface Settings

RIP settings are configured for each IP interface on the Switch. Click the **RIP Interface Settings** link in the **RIP** folder. The menu appears in table form listing settings for IP interfaces currently on the Switch. To configure RIP settings for an individual interface, click on the hyperlinked **Interface Name**. To view the next page of RIP Interface Settings, click the **Next** button.

Figure 9 - 11. RIP Interface Settings window

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

Figure 9 - 12. RIP Interface Settings - Edit window

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

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

Parameters	Description
Interface Name	The name of the IP interface on which RIP is to be setup. This interface must be previously configured on the Switch.
IP Address	The IP address corresponding to the Interface Name showing in the field above.
TX Mode	Toggle among *Disabled*, *V1 Only*, *V1 Compatible*, and *V2 Only*. This entry specifies which version of the RIP protocol will be used to transmit RIP packets. *Disabled* prevents the transmission of RIP packets.
RX Mode	Toggle among *Disabled*, *V1 Only*, *V2 Only*, and *V1 or V2*. This entry specifies which version of the RIP protocol will be used to interpret received RIP packets. *Disabled* prevents the reception of RIP packets.
Authentication	Toggle between *Disabled* and *Enabled* to specify that routers on the network should us the Password above to authenticate router table exchanges.
Password	A password to be used to authenticate communication between routers on the network.
State	Toggle between *Disabled* and *Enabled* to disable or enable this RIP interface on the switch.

Click **Apply** to implement changes made.

OSPF

The Open Shortest Path First (OSPF) routing protocol uses a *link-state* algorithm to determine routes to network destinations. A "link" is an interface on a router and the "state" is a description of that interface and its relationship to neighboring routers. The state contains information such as the IP address, subnet mask, type of network the interface is attached to, other routers attached to the network, etc. The collection of link-states is then collected in a link-state database that is maintained by routers running OSPF. OSPF specifies how routers will communicate to maintain their link-state database and defines several concepts about the topology of networks that use OSPF. To limit the extent of link-state update traffic between routers, OSPF defines the concept of *Area.* All routers within an area share the exact same link-state database, and a change to this database on one router triggers an update to the link-state database of all other routers in that area. Routers that have interfaces connected to more than one area are called *Border*

Routers and take the responsibility of distributing routing information between areas. One area is defined as *Area 0* or the *Backbone.* This area is central to the rest of the network in that all other areas have a connection (through a router) to the backbone. Only routers have connections to the backbone and OSPF is structured such that routing information changes in other areas will be introduced into the backbone, and then propagated to the rest of the network. When constructing a network to use OSPF, it is generally advisable to begin with the backbone (area 0) and work outward.

Link-State Algorithm

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

- When OSPF is started, or when a change in the routing information changes, the router generates a link-state advertisement. This advertisement is a specially formatted packet that contains information about all the link-states on the router.

- This link-state advertisement is flooded to all router in the area. Each router that receives the link-state advertisement will store the advertisement and then forward a copy to other routers.

- When the link-state database of each router is updated, the individual routers will calculate a Shortest Path Tree to all destinations – with the individual router as the root. The IP routing table will then be made up of the destination address, associated cost, and the address of the next hop to reach each destination.

- Once the link-state databases are updated, Shortest Path Trees calculated, and the IP routing tables written – if there are no subsequent changes in the OSPF network (such as a network link going down) there is very little OSPF traffic.

Shortest Path Algorithm

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

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

OSPF Cost

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

Cost = 100,000,000 / bandwidth in bps

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

Shortest Path Tree

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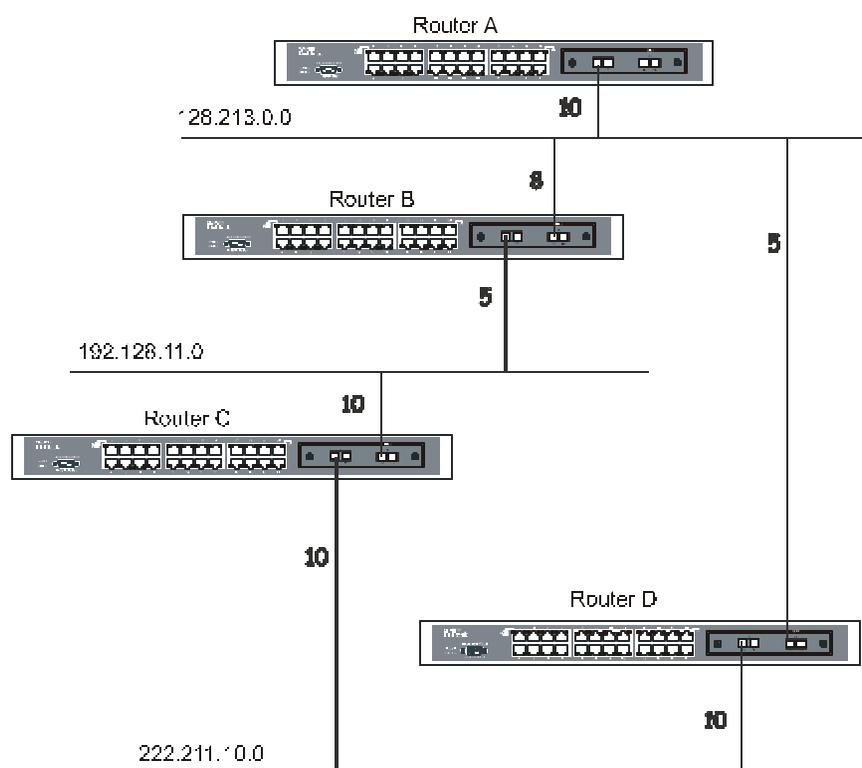

**Figure 9 - 13. Constructing a Shortest Path Tree**
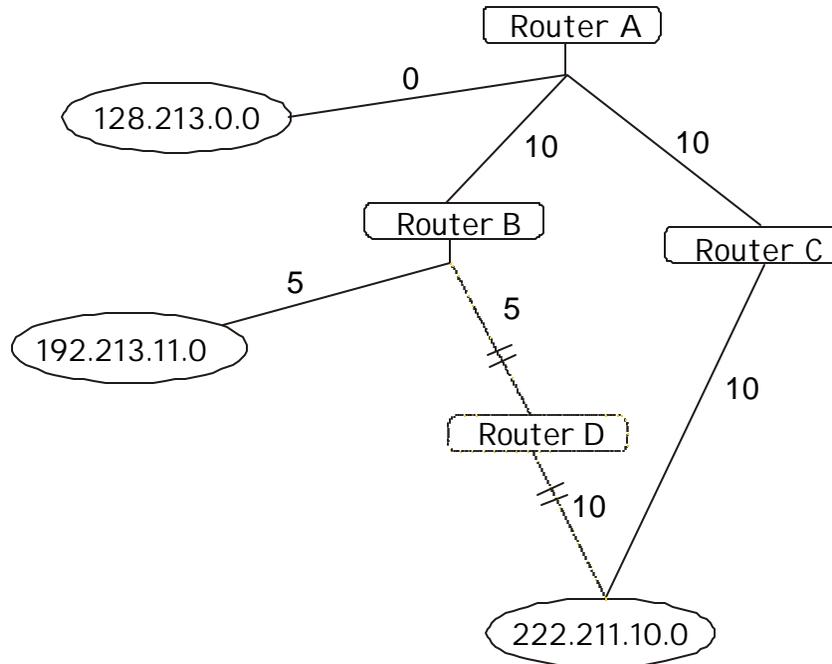
Figure 9 - 14. Constructing a Shortest Path Tree

The diagram above shows the network from the viewpoint of Router A. Router A can reach 192.213.11.0 through Router B with a cost of 10 + 5 = 15. Router A can reach 222.211.10.0 through Router C with a cost of 10 + 10 = 20. Router A can also reach 222.211.10.0 through Router B and Router D with a cost of 10 + 5 + 10 = 25, but the cost is higher than the route through Router C. This higher-cost route will not be included in the Router A's shortest path tree. The resulting tree will look like this:
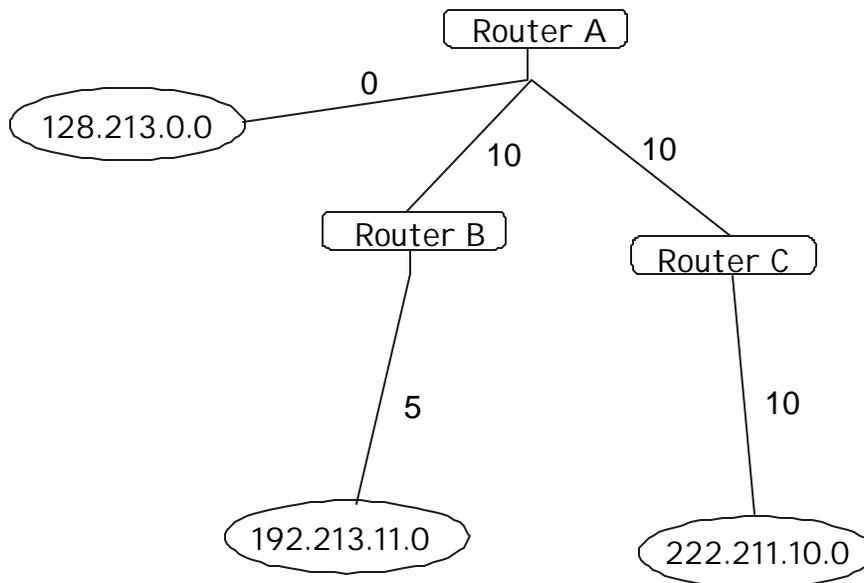

Figure 9 - 15. Constructing a Shortest Path Tree – Completed

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

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

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

Areas and Border Routers

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

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

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

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

Link-State Packets

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

- Router Link-State Updates – These describe a router's links to destinations within an area.

- Summary Link-State Updates – Issued by Border Routers and describe links to networks outside the area but within the Autonomous System (AS).

- Network Link-State Updates – Issued by multi-access areas that have more than one attached router. One router is elected as the Designated Router (DR) and this router issues the network link-state updates describing every router on the segment.

- External Link-State Updates – Issued by an Autonomous System Border Router and describes routes to destinations outside the AS or a default route to the outside AS.

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

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

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

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

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

OSPF Authentication

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

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

Message Digest Authentication (MD-5)

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

Simple Password Authentication

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

Backbone and Area 0

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

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

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

Virtual Links

Virtual links accomplish two purposes:

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

- Patching the backbone in case there is a discontinuity in area 0.

Areas Not Physically Connected to Area 0

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

Partitioning the Backbone

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

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

Neighbors

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

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

- **Area ID** − Two routers having a common segment − their interfaces have to belong to the same area on that segment. Of course, the interfaces should belong to the same subnet and have the same subnet mask.

- **Authentication** − OSPF allows for the configuration of a password for a specific area. Two routers on the same segment and belonging to the same area must also have the same OSPF password before they can become neighbors.

- **Hello and Dead Intervals** − The Hello interval specifies the length of time, in seconds, between the hello packets that a router sends on an OSPF interface. The dead interval is the number of seconds that a router's Hello packets have not been seen before its neighbors declare the OSPF router down. OSPF routers exchange Hello packets on each segment in order to acknowledge each other's existence on a segment and to elect a Designated Router on multi-access segments. OSPF requires these intervals to be exactly the same between any two neighbors. If any of these intervals are different, these routers will not become neighbors on a particular segment.

- **Stub Area Flag** − Any two routers also have to have the same stub area flag in their Hello packets in order to become neighbors.

Adjacencies

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

Designated Router Election

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

Building Adjacency

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

- **Down** − No information has been received from any router on the segment.

- **Attempt** − On non-broadcast multi-access networks (such as Frame Relay or X.25), this state indicates that no recent information has been received from the neighbor. An effort should be made to contact the neighbor by sending Hello packets at the reduced rate set by the Poll Interval.

- **Init** − The interface has detected a Hello packet coming from a neighbor but bi-directional communication has not yet been established.

- **Two-way** − Bi-directional communication with a neighbor has been established. The router has seen its address in the Hello packets coming from a neighbor. At the end of this stage the DR and BDR election would have been done. At the end of the Two-way stage, routers will decide whether to proceed in building an adjacency or not. The decision is based on whether one of the routers is a DR or a BDR or the link is a point-to-point or virtual link.

- **Exstart** − (Exchange Start) Routers establish the initial sequence number that is going to be used in the information exchange packets. The sequence number insures that routers always get the most recent information. One router will become the primary and the other will become secondary. The primary router will poll the secondary for information.

- **Exchange** − Routers will describe their entire link-state database by sending database description packets.

- **Loading** − The routers are finalizing the information exchange. Routers have link-state request list and a link-state retransmission list. Any information that looks incomplete or outdated will be put on the request list. Any update that is sent will be put on the retransmission list until it gets acknowledged.

- **Full** − The adjacency is now complete. The neighboring routers are fully adjacent. Adjacent routers will have the same link-state database.

Adjacencies on Point-to-Point Interfaces

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

OSPF Packet Formats

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

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

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

OSPF Packet Header

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

The format of the OSPP packet header is shown below:

OSPF Packet Header

Octets

0	1	2	3	4

Version No.	Type	Packet Length
Router ID		
Area ID		
Checksum	Authentication Type	
Authentication		
Authentication		
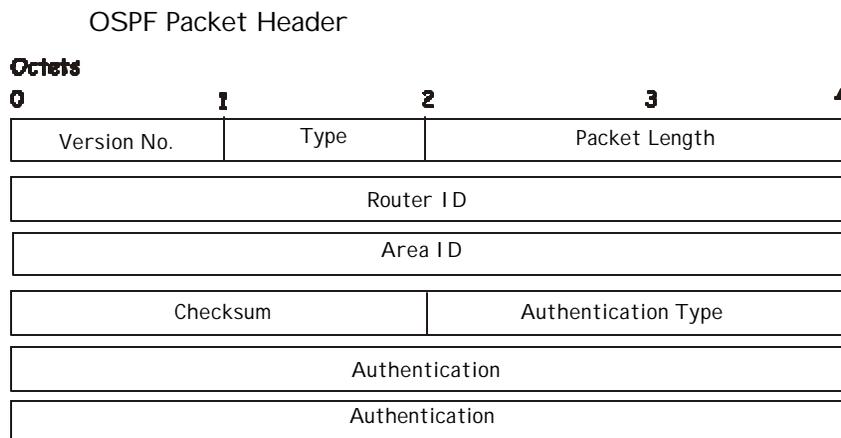
Figure 9 - 16. OSPF Packet Header Format

Field	Description
Version No.	The OSPF version number
Type	The OSPF packet type. The OSPF packet types are as follows: Type Description Hello Database Description Link-State Request Link-State Update Link-State Acknowledgment
Packet Length	The length of the packet in bytes. This length includes the 24-byte header.
Router ID	The Router ID of the packet's source.
Area ID	A 32-bit number identifying the area that this packet belongs to. All OSPF packets are associated with a single area. Packets traversing a virtual link are assigned the backbone Area ID of 0.0.0.0
Checksum	A standard IP checksum that includes all of the packet's contents except for the 64-bit authentication field.
Authentication Type	The type of authentication to be used for the packet.
Authentication	A 64-bit field used by the authentication scheme.

Hello Packet

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

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

The format of the Hello packet is shown below:

Hello Packet
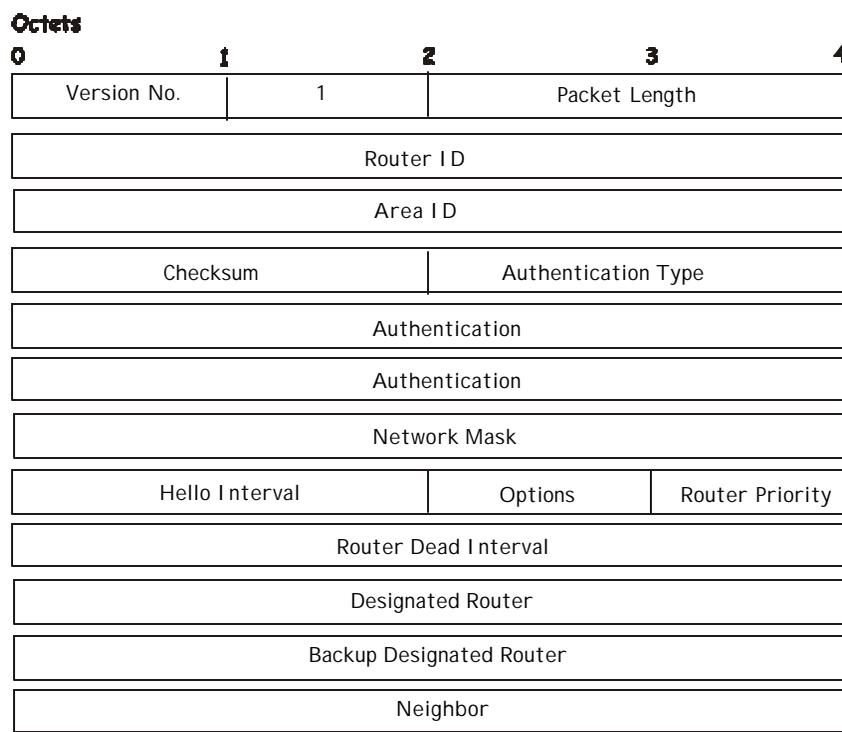
Figure 9 - 17. Hello Packet

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

Database Description Packet

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

Database Description Packet

Octets

0	1	2	3	4

Version No.	2	Packet Length

Router ID

Area ID

Checksum	Authentication Type

Authentication

Authentication

Reserved	I	M	MS	Reserved	Options

DD Sequence No.

Link-State Advertisement Header ...
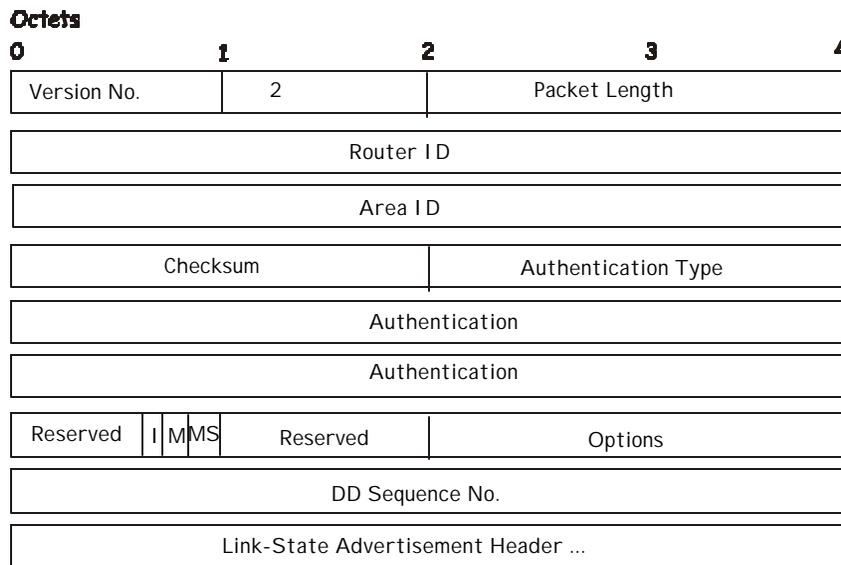
Figure 9 - 18. Database Description Packet

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

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

Link-State Request Packet

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

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

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

Link-State Request Packet

Octets				
0	**1**	**2**	**3**	**4**

Version No.	3	Packet Length

Router I D

Area I D

Checksum	Authentication Type

Authentication

Authentication

Link-State Type

Link-State I D

Advertising Router
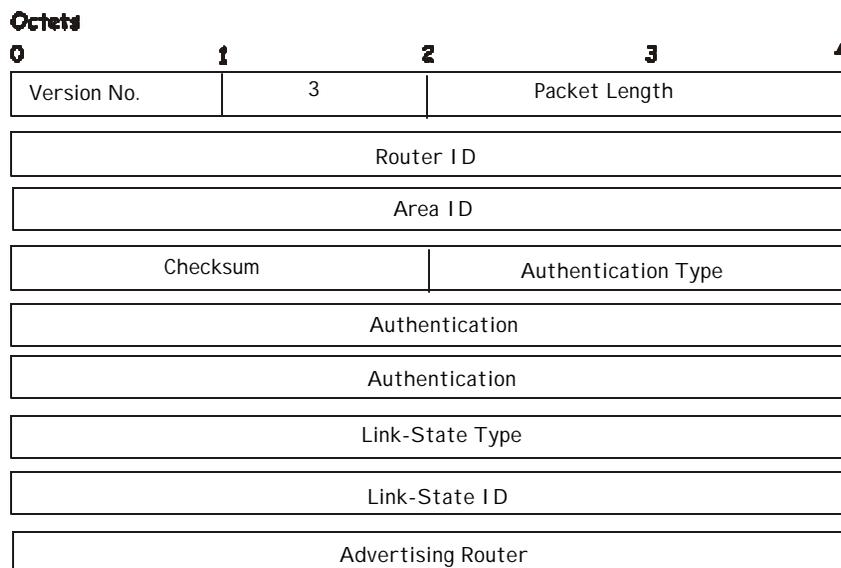
Figure 9 - 19. Link-State Request Packet

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

Link-State Update Packet

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

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

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

Link-State Update Packet

Octets				
0	**1**	**2**	**3**	**4**

Version No.	4	Packet Length

Router I D

Area I D

Checksum	Authentication Type

Authentication

Authentication

Number of Advertisements

Link-State Advertisements ...
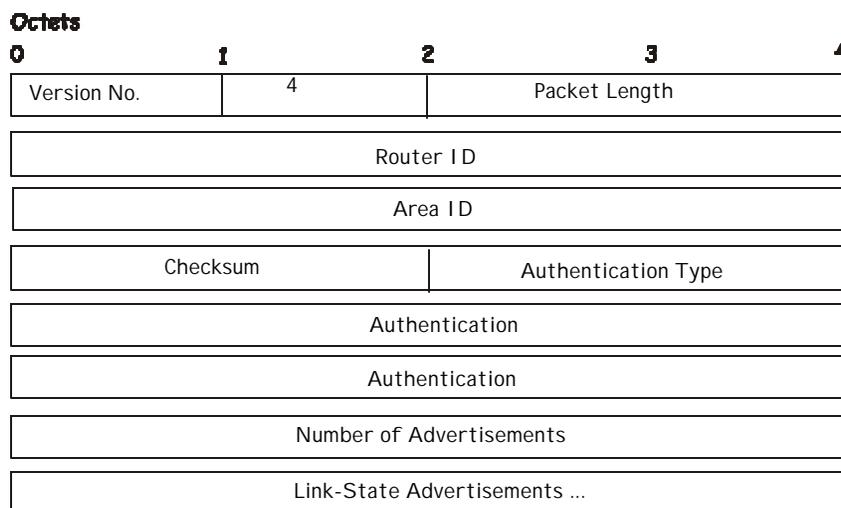
Figure 9 - 20. Link-State Update Packet

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

Link-State Acknowledgment Packet

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

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

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

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

Link-State Acknowledgment Packet

Octets

0	1	2	3	4

Version No.	5	Packet Length		
Router ID				
Area ID				
Checksum		Authentication Type		
Authentication				
Authentication				
Link-State Advertisement Header …				
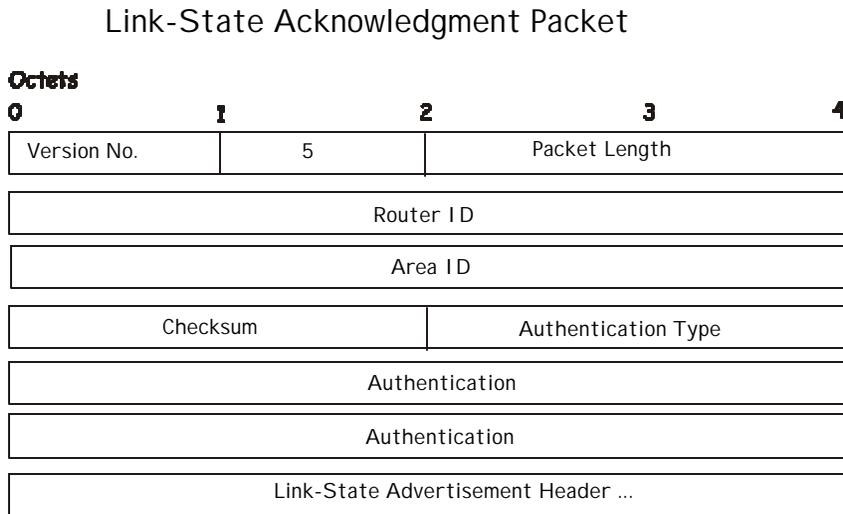
Figure 9 - 21. Link State Acknowledge Packet

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

Link-State Advertisement Formats

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

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

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

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

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

Link State Advertisement Header

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

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

Link-State Advertisement Header

Octets

0	1	2	3	4

Link-State Age		Options	Link-State Type	
Link-State ID				
Advertising Router				
Link-State Sequence Number				
Link-State Checksum		Length		
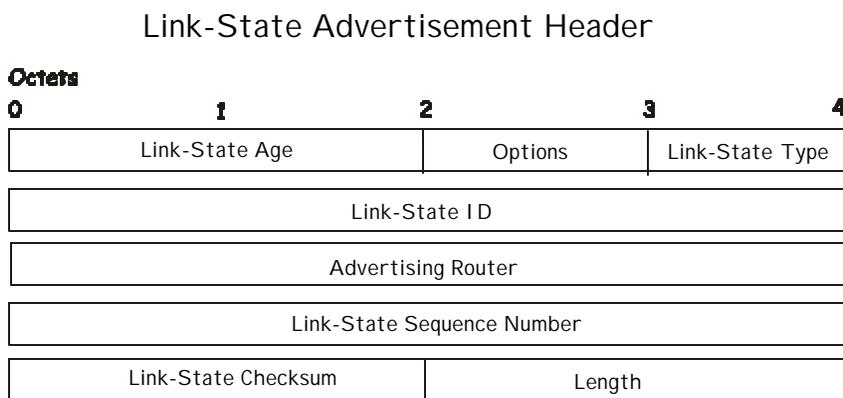
Figure 9 - 22. Link State Advertisement Header

Field	Description
Link State Age	The time is seconds since the link state advertisement was originated.

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

Router Links Advertisements

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

The format of the Router Links Advertisement is shown below:

Routers Links Advertisements
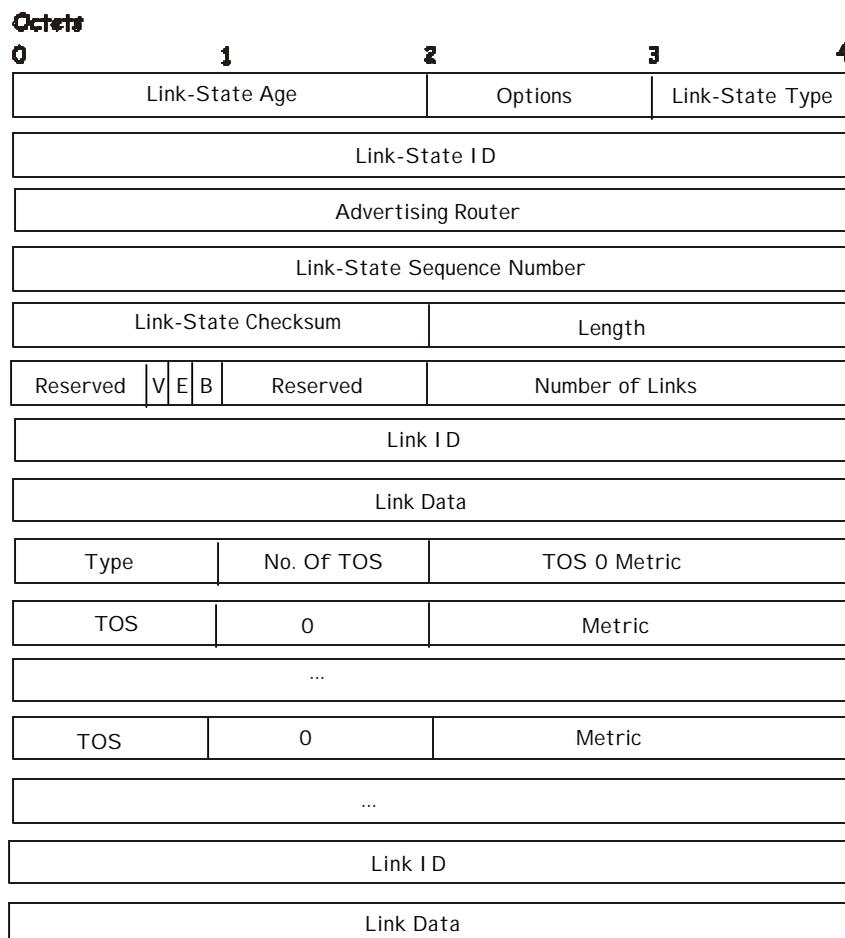
Figure 9 - 23. Routers Links Advertisements

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

Field	Description

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

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

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

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

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

Network Links Advertisements

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

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

The format of the Network Links Advertisement is shown below:

Network Link Advertisements
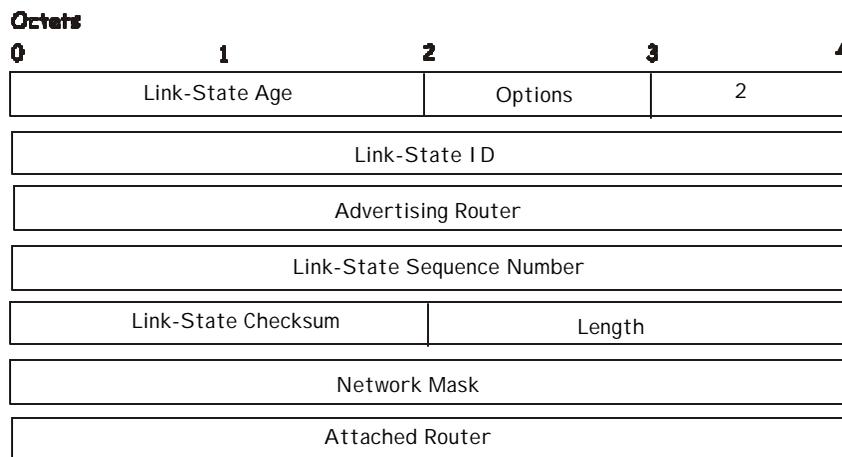
Figure 9 - 24. Network Link Advertisements

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

Summary Link Advertisements

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

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

Summary Link Advertisements
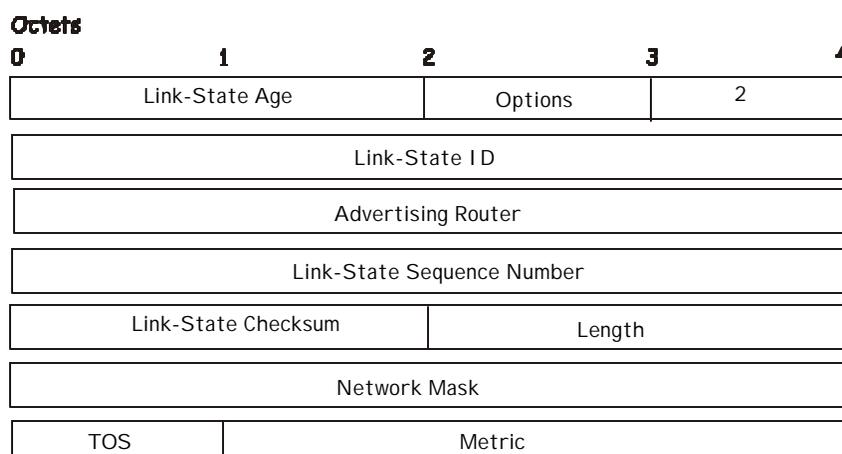
Figure 9 - 25. Summary Link Advertisements

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

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

Field	Description
Network Mask	For Type 3 link state advertisements, this indicates the destination network's IP address mask. For example, when advertising the location of a class A network the value 0xff000000

TOS	The Type of Service that the following cost is relevant to.
Metric	The cost of this route. Expressed in the same units as the interface costs in the router links advertisements.

Autonomous Systems External Link Advertisements

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

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

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

AS External Link Advertisements
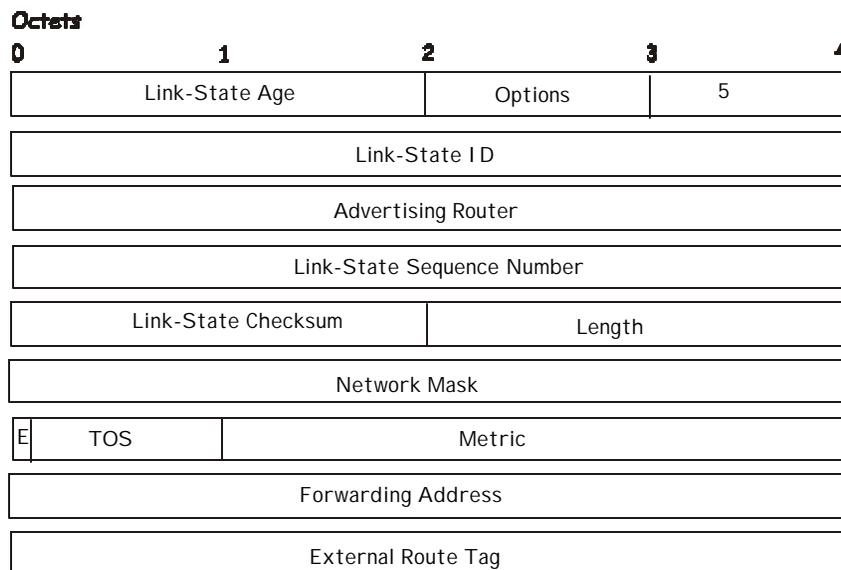
Figure 9 - 26. AS External Link Advertisements

Field	Description
Network Mask	The IP address mask for the advertised destination.
E - bit	The type of external metric. If the E - bit is set, the metric specified is a Type 2 external metric. This means the metric is considered larger than any link state path. If the E - bit is zero, the specified metric is a Type 1 external metric. This means that is comparable directly to the link state metric.
Forwarding Address	Data traffic for the advertised destination will be forwarded to this address. If the Forwarding Address is set to 0.0.0.0, data traffic will be forwarded instead to the advertisement's originator.
TOS	The Type of Service that the following cost is relevant to.
Metric	The cost of this route. The interpretation of this metric depends on the external type indication (the E - bit above).
External Route Tag	A 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

OSPF General Settings

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

To view the following window, click **Configuration > Layer 3 IP Networking > OSPF > OSPF General Settings**. To enable OSPF, first supply an **OSPF Route ID** (see below), select *Enabled* from the **State** drop-down menu and click the **Apply** button.
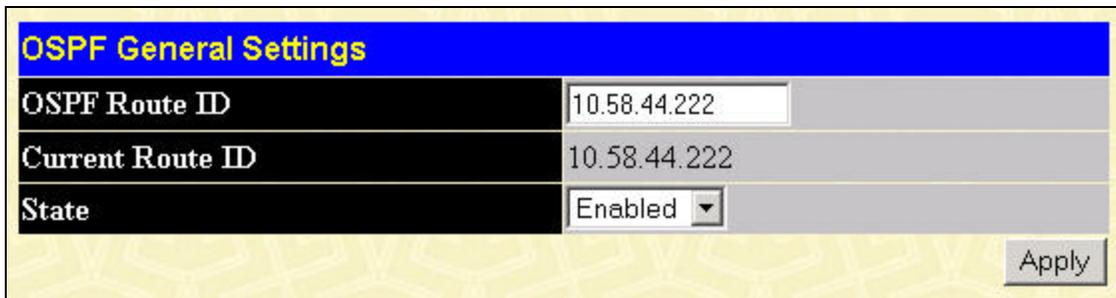
Figure 9 - 27. OSPF General Settings window

The following parameters are used for general OSPF configuration:

Parameter	Description
OSPF Route ID	A 32-bit number (in the same format as an IP address – xxx.xxx.xxx.xxx) that uniquely identifies the Switch in the OSPF domain. It is common to assign the highest IP address assigned to the Switch (router). In this case, it would be 10.53.13.189, but any unique 32-bit number will do. If 0.0.0.0 is entered, the highest IP address assigned to the Switch will become the OSPF Route ID.
Current Route ID	Displays the OSPF Route ID currently in use by the Switch. This Route ID is displayed as a convenience to the user when changing the Switch's OSPF Route ID.
State	Allows OSPF to be enabled or disabled globally on the Switch without changing the OSPF configuration.

OSPF Area Setting

This menu allows the configuration of OSPF Area IDs and to designate these areas as either **Normal** or **Stub**. Normal OSPF areas allow Link-State Database (LSDB) advertisements of routes to networks that are external to the area. Stub areas do not allow the LSDB advertisement of external routes. Stub areas use a default summary external route (0.0.0.0 or Area 0) to reach external destinations.

To set up an OSPF area configuration click **Configuration > Layer 3 IP Networking > OSPF > OSPF Area Settings** link to open the following dialog box:
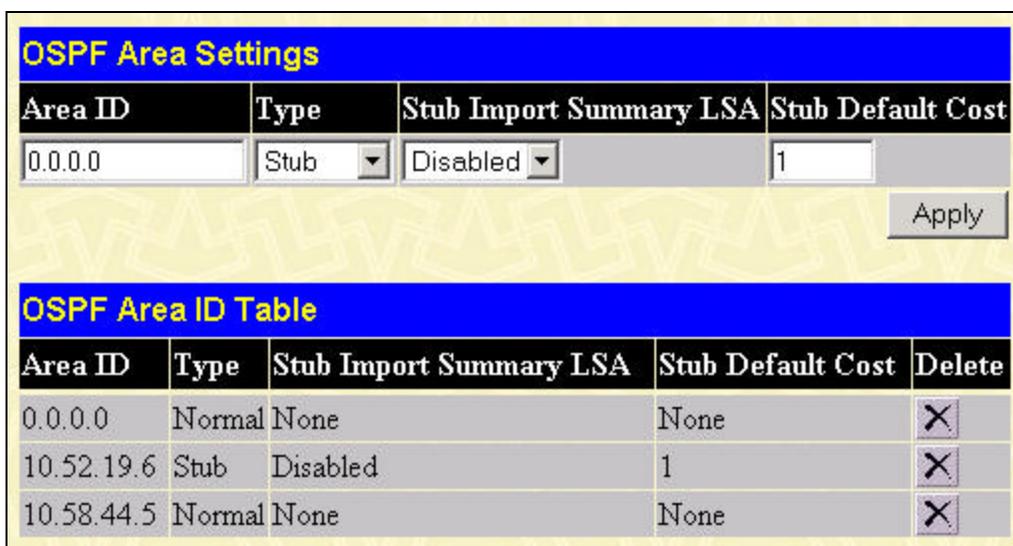
Figure 9 - 28. OSPF Area Settings and Table window

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

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

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

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

The **Area ID** settings are as follows:

Parameters	Description
Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Type	This field can be toggled between *Normal* and *Stub* using the space bar. When it is toggled to *Stub*, additional fields appear – **Stub Import Summary LSA,** and the **Stub Default Cost**.
Stub Import Summary LSA	Displays whether or not the selected Area will allow Summary Link-State Advertisements (Summary LSAs) to be imported into the area from other areas.
Stub Default Cost	Displays the default cost for the route to the stub of between 0 and 65,535. The default is 1.

OSPF Interface Settings

To set up OSPF interfaces, click **Configuration > Layer 3 IP Networking > OSPF > OSPF Interface Settings** to view OSPF settings for existing IP interfaces. If there are no IP interfaces configured (besides the default System interface), only the System interface settings will appear listed. To change settings for in IP interface, click on the hyperlinked name of the interface to see the configuration menu for that interface.

OSPF Interface Settings

Name	IP Address	Area ID	Priority	Hello Time	Dead Time	Auth. Type	State
System	10.58.44.222	0.0.0.0	1	10	40	None	Disabled

Figure 9 - 29. OSPF Interface Settings window

OSPF Interface Configuration-Edit

Interface Name	System
IP Address	10.58.44.222(LinkUp)
Network Medium Type	BROADCAST
Area ID	0.0.0.0
Router Priority	1
Hello Interval(1-65535)	10
Dead Interval(1-65535)	40
State	Disabled
Auth. Type	None
Metric(1-65535)	1
DR State	DOWN
DR Address	0.0.0.0
Backup DR Address	0.0.0.0
Transmit Delay	1
Retransmit Time	5
	Apply

Figure 9 - 30. OSPF Interface Settings - Edit window

Configure each IP interface individually using the **OSPF Interface Settings - Edit** menu. Click the **Apply** button when you have entered the settings. The new configuration appears listed in the **OSPF Interface Settings** table.

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

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

	The highest IP address will be the Designated Router and is determined by the OSPF Hello Protocol of the Switch.
DR Address	The IP address of the aforementioned Designated Router.
Backup DR Address	The IP address of the aforementioned Backup Designated Router.
Transmit Delay	A read only field that denotes the estimated time to transmit a Link State Update Packet over this interface, in seconds.
Retransmit Time	A read only field that denotes the time between LSA retransmissions over this interface, in seconds.

OSPF Virtual Link Settings

Click the **OSPF Virtual Interface Setting**s link to view the current **OSPF Virtual Interface Settings**. There are not virtual interface settings configured by default, so the first time this table is viewed there will be not interfaces listed. To add a new OSPF virtual interface configuration set to the table, click the **Add** button. A new menu appears (see below). To change an existing configuration, click on the hyperlinked **Transit Area ID** for the set you want to change. The menu to modify an existing set is the same as the menu used to add a new one. To eliminate an existing configuration, click the ✕ in the **Delete** column.
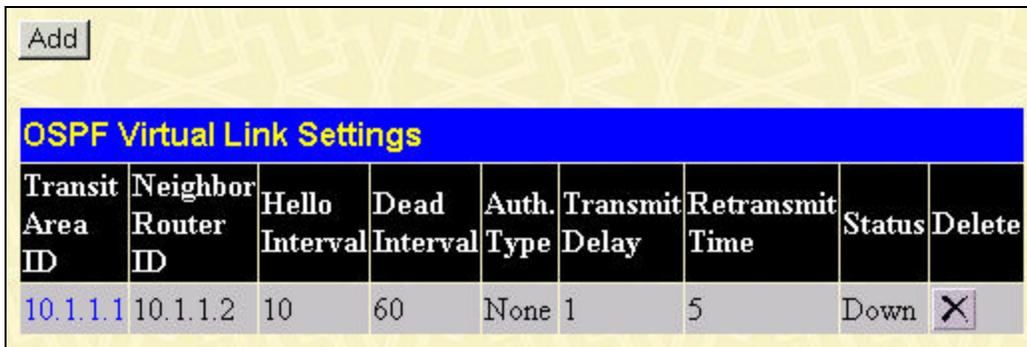
Figure 9 - 31. OSPF Virtual Link Settings table

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

Figure 9 - 32. OSPF Virtual Link Setting –Add

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

Parameters	Description
Transit Area ID	Allows the entry of an OSPF Area ID – previously defined on the Switch – that allows a remote area to communicate with the backbone (area 0). A Transit Area cannot be a Stub Area or a Backbone Area.

Neighbor Router	The OSPF router ID for the remote router. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.
Hello Interval (1-65535)	Specify the interval between the transmission of OSPF Hello packets, in seconds. Enter a value between 1 and 65535 seconds. The **Hello Interval**, **Dead Interval**, **Authorization Type**, and **Authorization Key** should have identical settings for all routers on the same network.
Dead Interval (1-65535)	Specify the length of time between (receiving) Hello packets from a neighbor router before the selected area declares that router down. Again, all routers on the network should use the same setting.
Auth Type	If using authorization for OSPF routers, select the type being used. MD5 key authorization must be set up in the MD5 Key Settings menu.
Password/Auth. Key ID	Enter a case-sensitive password for simple authorization or enter the MD5 key you set in the MD5 Key settings menu.
Transmit Delay	The number of seconds required to transmit a link state update over this virtual link. Transit delay takes into account transmission and propagation delays. This field is fixed at 1 second.
Retransinterval	The number of seconds between link state advertisement retransmissions for adjacencies belonging to this virtual link. This field is fixed at 5 seconds.

Click **Apply** to implement changes made.

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

OSPF Area Aggregation Settings

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

Click **Configuration > Layer 3 IP Networking > OSPF > OSPF Area Aggregation Settings** link to view the current settings. There are no aggregation settings configured by default, so there will not be any listed the first accessing the menu. To add a new **OSPF Area Aggregation** setting, click the **Add** button. A new menu (pictured below) appears. To change an existing configuration, click on the hyperlinked Area ID for the set you want to change. The menu to modify an existing configuration is the same as the menu used to add a new one. To eliminate an existing configuration, click the ✕ in the **Delete** column for the configuration being removed.

Add

OSPF Area Aggregation Settings

Area ID	Network Number	Network Mask	LSDB Type	Advertisement	Delete
10.1.1.1	0.0.0.0	0.0.0.0	Summary	Enabled	✕

Figure 9 - 33. OSPF Area Aggregation Settings table

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

Figure 9 - 34. OSPF Area Aggregation Settings - Add

Specify the OSPF aggregation settings and click the **Apply** button to add or change the settings. The new settings will appear listed in the **OSPF Area Aggregation Configuration** table.

Use the following parameters to configure the following settings for **OSPF Area Aggregation**:

Parameters	Description
Area ID	Allows the entry the OSPF Area ID for which the routing information will be aggregated. This Area ID must be previously defined on the Switch.
Network Number	Sometimes called the Network Address. The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area above.
Network Mask	The corresponding network mask for the Network Number specified above.
LSDB Type	Specifies the type of address aggregation, which is set at *Summary*.
Advertisement	Select *Enabled* or *Disabled* to determine whether the selected OSPF Area will advertise it's summary LSDB (Network-Number and Network-Mask).
Advertisement	Select *Enabled* or *Disabled* to determine whether the selected OSPF Area will advertise it's summary LSDB (Network-Number and Network-Mask).

Click **Apply** to implement changes made.

OSPF Host Route Settings

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

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

Figure 9 - 35. OSPF Host Route Settings table

Use the menu below to set up OSPF host routes.

OSPF Host Route Setting - Add

Host Address	0.0.0.0
Metric	0
Area ID	0.0.0.0
	Apply

Figure 9 - 36. OSPF Host Route Settings - Add

Specify the host route settings and click the **Apply** button to add or change the settings. The new settings will appear listed in the **OSPF Host Route Settings** list. The following fields are configured for OSPF host route.

Parameters	Description
Host Address	**The IP address of the OSPF host.**
Metric	**A value between 1 and 65535 that will be advertised for the route.**
Area ID	**A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.**

DHCP / BOOTP Relay

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

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

DHCP/Bootp Relay Information

Bootp Relay Status	Disabled
Bootp Hops Count Limit(1-16)	4
Bootp Relay Time Threshold(0-65535)	0
	Apply

Figure 9 - 37. DHCP/ BOOTP Relay Global Settings window

The following fields can be set:

Parameters	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 BOOTP/DHCP 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 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 BOOTP/DHCP packet. If

a value of 0 is entered, the Switch will not process the value in the seconds field of the BOOTP or DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given BOOTP or DHCP packet.

DHCP/BOOTP Relay Interface Settings

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

Figure 9 - 38. DHCP/BOOTP Relay Settings and DHCP/BOOTP Relay Table

The following parameters may be configured or viewed.

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

DNS Relay

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

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

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

Mapping Domain Names to Addresses

Name-to-address translation is performed by a program called a Name Server. The client program is called a Name Resolver. A Name Resolver may need to contact several Name Servers to translate a name to an address.

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

Domain Name Resolution

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

When a DNS server receives a query, it checks to see if the name is in its sub domain. If it is, the server translates the name and appends the answer to the query, and sends it back to the client. If the DNS server cannot translate the name, it determines what type of name resolution the client requested. A complete translation is called recursive resolution and requires the server to contact

other DNS servers until the name is resolved. Iterative resolution specifies that if the DNS server cannot supply an answer, it returns the address of the next DNS server the client should contact.

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

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

DNS Relay Information

To configure the DNS function on the Switch, click **Configuration > Layer 3 IP Networking > DNS Relay > DNS Relay Information**, which will open the DNS Relay Global Settings window, as seen below:

Figure 9 - 39. DNS Relay Information window

The following fields can be set:

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

Click **Apply** to implement changes made.

DNS Relay Static Settings

To view the DNS Relay Static Settings, click Configuration > Layer 3 IP Networking > DNS Relay > DNS Relay Static Settings, which will open the DNS Relay Static Settings window, as seen below:

Figure 9 - 40. DNS Relay Static Setting Table

To add an entry into the **DNS Relay Static Table**, simply enter a **Domain Name** with its corresponding IP address and click **Add** under the **Apply** heading. A successful entry will be presented in the table below, as shown in the example above.

IP Multicast Routing Protocol

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

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

IGMP

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP)** is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active.

In the case where there is more than one multicast router on a subnetwork, one router is elected as the 'querier'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given subnetwork or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnetwork. If there are no members on a subnetwork, packets will not be forwarded to that subnetwork.

IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:
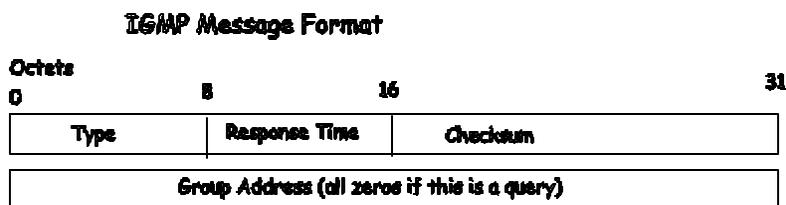
Figure 9 - 41. IGMP Message Format

The IGMP Type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	Membership Report (version 2)
0x17	Leave a Group (version 2)
0x12	Membership Report (version 1)

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective subnetworks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.

1. A host sends an IGMP "report" to join a group

2. A host will never send a report when it wants to leave a group (for version 1).

3. A host will send a "leave" report when it wants to leave a group (for version 2).

4. Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their subnetworks. If there is no response from a particular group, the router assumes that there are no group members on the network.

5. The Time -to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other subnetworks.

6. IGMP version 2 introduces some enhancements such as a method to elect a multicast querier for each LAN, an explicit leave message, and query messages that are specific to a given group.

7. The states a computer will go through to join or to leave a multicast group are shown below:
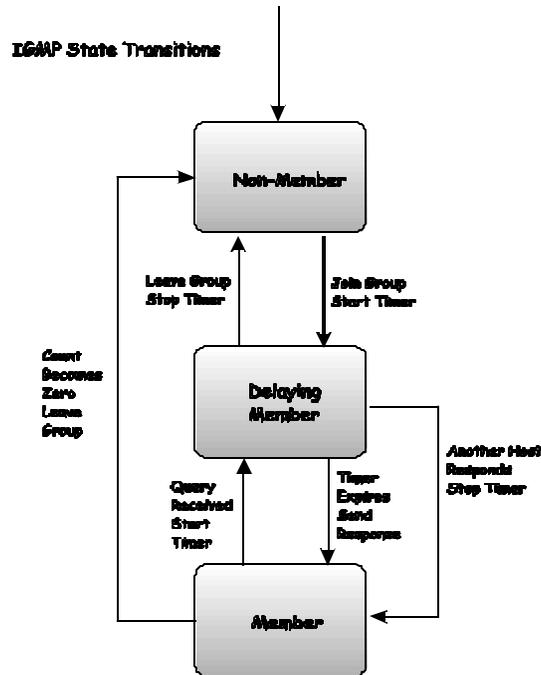
Figure 9 - 42. IGMP State Transitions

IGMP Interface Settings

The Internet Group Multicasting Protocol (IGMP) can be configured on the Switch on a per-IP interface basis. Click **Configuration > Layer 3 IP Networking** > **IP Multicast Routing Protocol > IGMP Interface Settings** to view the window shown below. Each IP interface configured on the Switch is displayed in the below **IGMP Interface Settings** dialog box. To configure IGMP for a particular interface, click the corresponding hyperlink for that IP interface. This will open another **IGMP Interface Settings Edit** window:

Figure 9 - 43. IGMP Interface Table

Figure 9 - 44. IGMP Interface Configuration window

This window allows the configuration of IGMP for each IP interface configured on the Switch. IGMP can be configured as **Version** 1 or 2 by toggling the Version field using the pull-down menu. The length of time between queries can be varied by entering a value between 1 and 31,744 seconds in the **Query Interval** field. The maximum length of time between the receipt of a query and the sending of an IGMP response report can be varied by entering a value in the **Max Response Time** field.

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

The following fields can be set:

Parameters	Description
Interface Name	Displays the name of the IP interface that is to be configured for IGMP. This must be a previously configured IP interface.
IP Address	Displays the IP address corresponding to the IP interface name above.
Version	Enter the IGMP version (1, 2 or 3) that will be used to interpret IGMP queries on the interface.
Query Interval	Allows the entry of a value between *1* and *31744* seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.
Max Response Time	Sets the maximum amount of time allowed before sending an IGMP response report. A value between 1 and 25 seconds can be entered, with a default of 10 seconds.
Robustness Variable	A tuning variable to allow for subnetworks that are expected to lose a large number of packets. A value between 2 and 255 can be entered, with larger values being specified for subnetworks that are expected to lose larger numbers of packets.
Last Member Query Interval	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. A value between 1 and 25. The default is *1* second.
State	This field can be toggled between *Enabled* and *Disabled* and enables or disables IGMP for the IP interface. The default is *Disabled*.

Click **Apply** to implement changes made.

DVMRP Interface Settings

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

DVMRP resembles the Routing Information Protocol (RIP), but is extended for multicast delivery. DVMRP builds a routing table to calculate 'shortest paths' back to the source of a multicast message, but defines a 'route cost' (similar to the hop count in RIP) as a relative number that represents the real cost of using this route in the construction of a multicast delivery tree to be 'pruned' - once the delivery tree has been established.

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

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

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

To enable DVMRP globally on the Switch, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > DVMRP Interface Settings**. This will give the user access to the following screen:

Figure 9 - 45. DVMRP Interface Settings window

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

Figure 9 - 46. DVMRP Interface Settings window

The following fields can be set:

Parameters	Description
Interface Name	Displays the name of the IP interface for which DVMRP is to be configured. This must be a previously defined IP interface.
IP Address	Displays the IP address corresponding to the IP Interface name entered above.
Neighbor Timeout Interval (1-65535)	This field allows an entry between *1* and *65,535* seconds and defines the time period DVMRP will hold Neighbor Router reports before issuing poison route messages. The default is *35* seconds.
Probe Interval (1-65535)	This field allows an entry between 1 – 65535 seconds and defines the interval between probes. The default is ten.
Metric (1-31)	This field allows an entry between *1* and *31* and defines the route cost for the IP interface. The DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hop count in RIP. The default cost is *1.*
State	This field can be toggled between *Enabled* and *Disabled* and enables or disables DVMRP for the IP interface. The default is *Disabled.*

Click **Apply** to implement changes made.

PIM

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

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

PIM-DM has no explicit 'join' messages. It relies upon periodic flooding of multicast messages to all interfaces and then either waiting for a timer to expire (the **Join/Prune Interval**) or for the downstream routers to transmit explicit 'prune' messages indicating that there are no multicast members on their respective branches. PIM-DM then removes these branches ('prunes' them) from the multicast delivery tree.

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

PIM-DM Interface Settings

Click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM > PIM-DM Interface Settings.** This window allows the **PIM-DM** to be configured for each IP interface defined on the Switch. Each IP interface configured on the Switch is displayed in the below **PIM-DM Interface Settings** dialog box. To configure PIM-DM for a particular interface, click the corresponding hyperlink for that IP interface. This will open the **PIM-DM Interface Settings** window:

PIM-DM Interface Settings

Interface Name	IP Address	State
System	10.58.44.222	Disabled

Figure 9 - 47. PIM-DM Interface Table

To view the configuration window for a specific entry, click its hyperlinked name, revealing the following window.

PIM-DM Interface Configuration

Interface Name	System
IP Address	10.58.44.222
Hello Interval(1-18724 sec)	30
Join-Prune Interval(1-18724 sec)	60
State	Disabled

Figure 9 - 48. PIM-DM Interface Configuration window

The following fields can be set or viewed:

Parameters	Description
Interface Name	Allows the entry of the name of the IP interface for which PIM-DM is to be configured. This must be a previously defined IP interface.
IP Address	Displays the IP address for the IP interface named above.
Hello Interval (1-18724)	This field allows an entry of between *1* and *18724* seconds and determines the interval between sending Hello packets to other routers on the network. The default is *30* seconds.
Join/Prune Interval (1-18724)	This field allows an entry of between *1* and *18724* seconds. This interval also determines the time interval the router uses to automatically remove prune information from a branch of a multicast delivery tree and begin to flood multicast messages to all branches of that delivery tree. These two actions are equivalent. The default is *60* seconds.
State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu, and is used to enable or disable PIM-DM for the IP interface. The default is *Disabled*.

Click **Apply** to implement changes made.

<div style="border:1px solid">

Section 10

</div>

Monitoring

> *CPU Utilization*
> *Port Utilization*
> *Packets*
> *Errors*
> *Size*
> *MAC Address*
> *ARP Table*
> *IGMP Snooping Group*
> *IGMP Snooping Forwarding*
> *VLAN Status*
> *Router Port*
> *Port Access Control*

The DES -3350SR provides extensive network monitoring capabilities that can be viewed under the **Monitoring** menu.

CPU Utilization

The CPU Utilization displays the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval. To view the CPU Utilization window, open the Monitoring folder and click the CPU Utilization link.
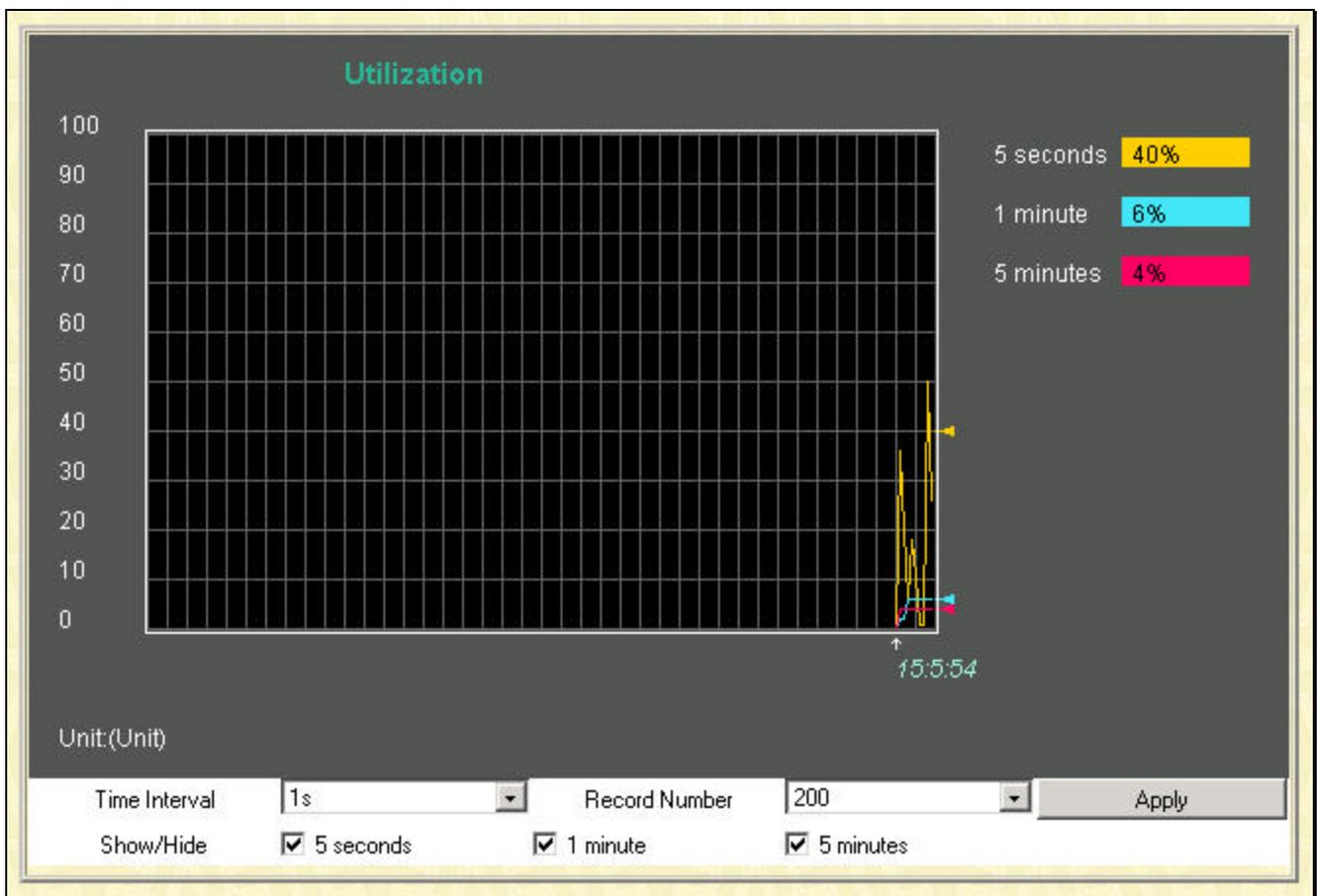
Figure 10 - 1. CPU Utilization window

To select a port to view these statistics for, first select the Switch in the switch stack by using the **Unit** pull-down menu. To view the CPU utilization by port, use the real-time graphic of the Switch and/or switch stack at the top of the web page by simp ly clicking on a port. Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics.

The information is described as follows:

Parameters	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.
Utilization	Check whether or not to display Utilization.

Port Utilization

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

To view port utilization, click on the **Monitoring** folder and then the **Port Utilization** link:
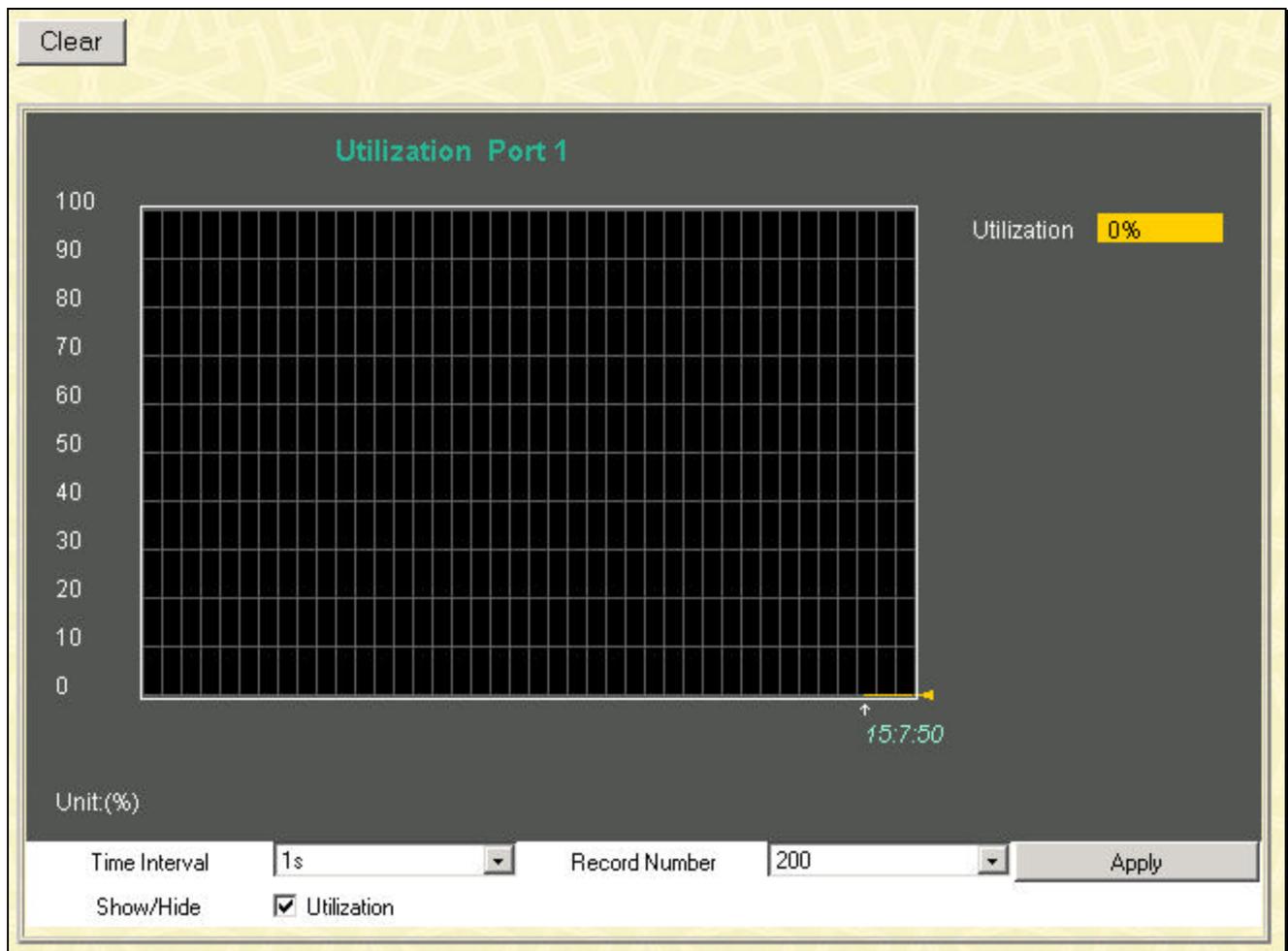
Figure 10 - 2. Utilization window

Click the port on the front panel display that you want to display port utilization.

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 *20*.
Show/Hide	Check to display Utilization.
Clear	Clicking this button clears all statistics counters on this window.

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)

Figure 10 - 3. Rx Packets Analysis window (line graph for Bytes and Packets)

Figure 10 - 4. Rx Packets Analysis window (table for Bytes and Packets)

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 *20*.
Bytes	Counts the number of bytes received on the port.
Packets	Counts the number of packets received on the port.
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)
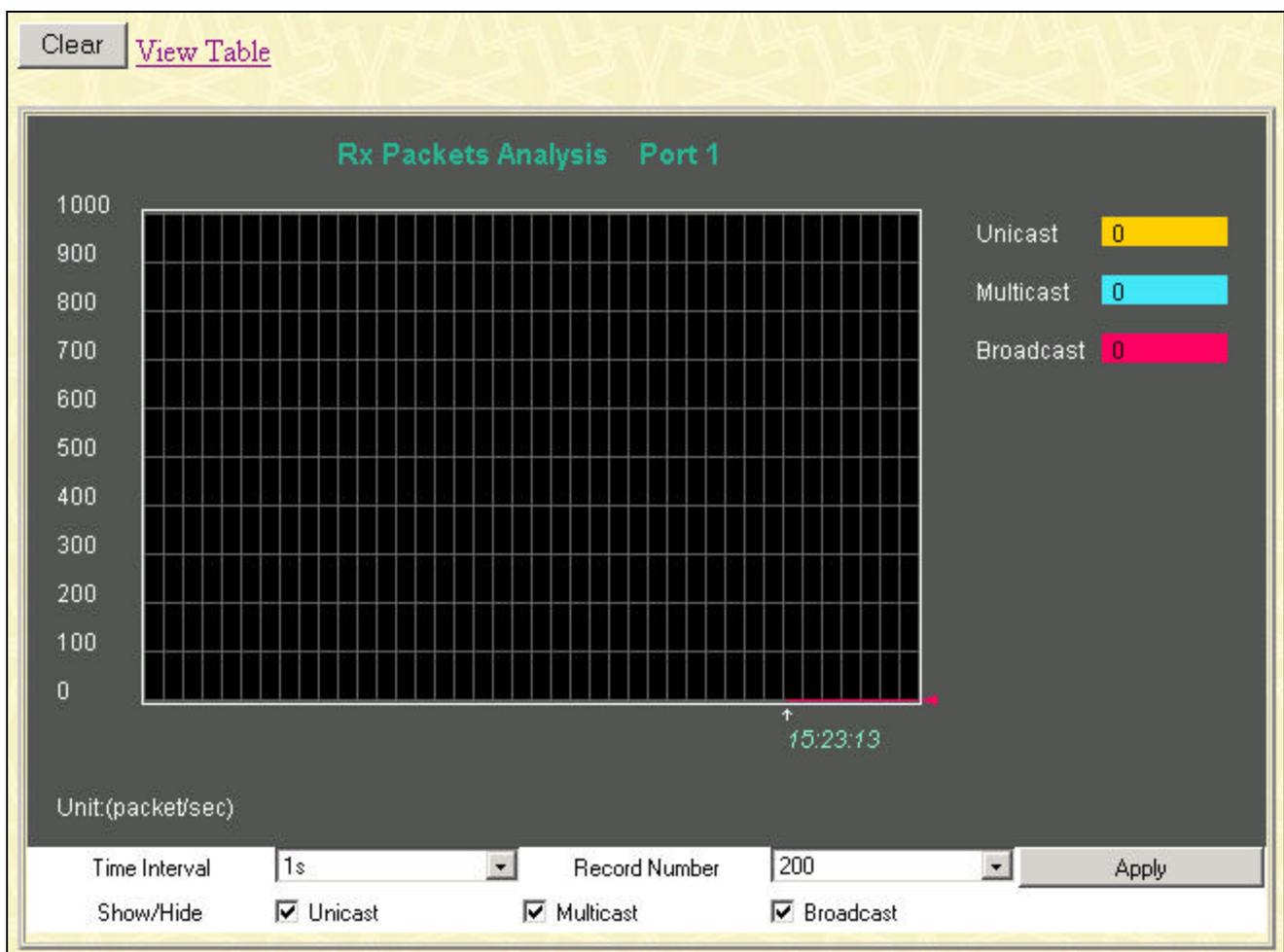
Figure 10 - 5. Rx Packets Analysis window (line graph for Unicast, Multicast, and Broadcast Packets)

128
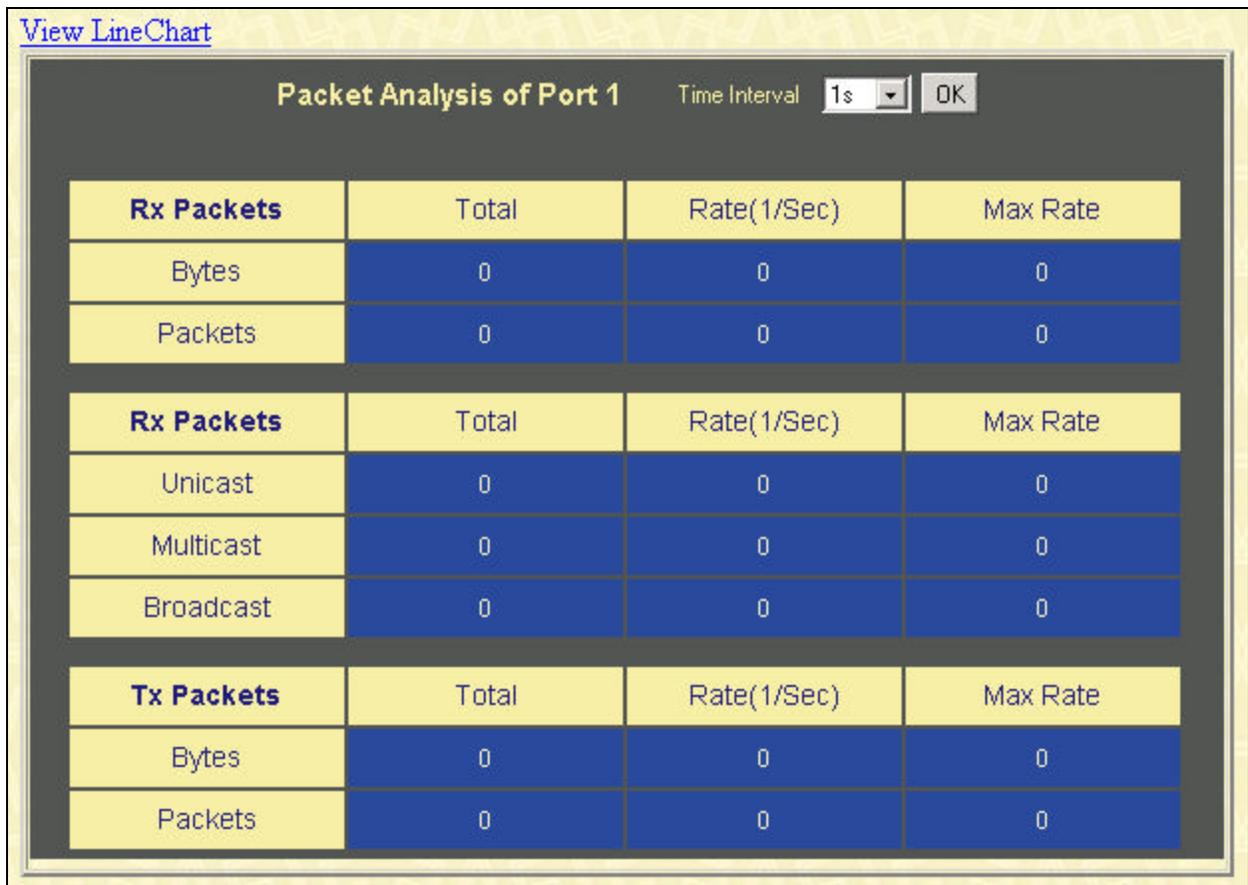
Figure 10 - 6. Rx Packets Analysis window (table for Unicast, Multicast, and Broadcast Packets)

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 *20*.
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)
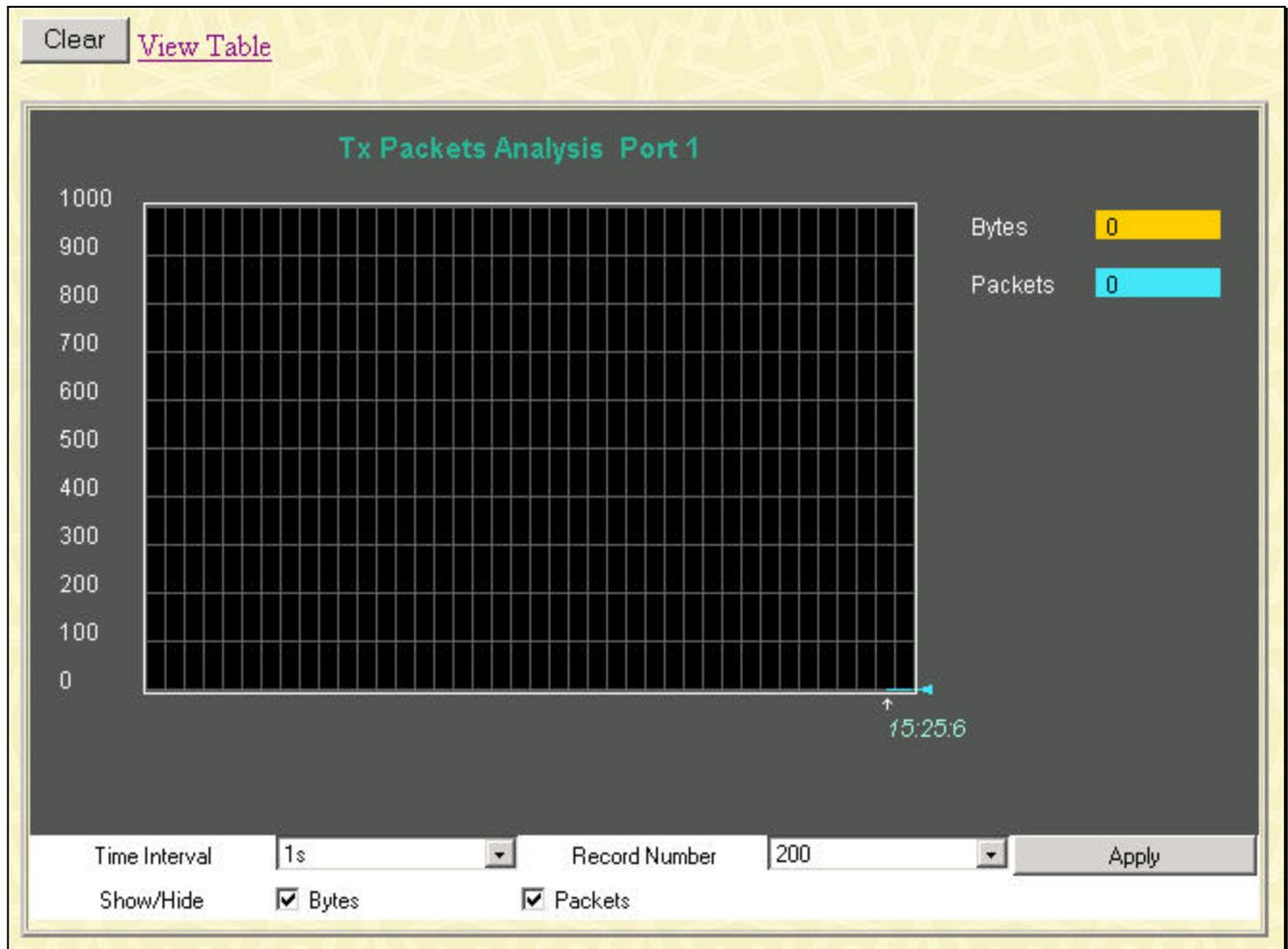
Figure 10 - 7. Tx Packets Analysis window (line graph for Bytes and Packets)

Figure 10 - 8. Tx Packets Analysis window (table for Bytes and Packets)

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

	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 *20*.
Bytes	Counts the number of bytes successfully sent from the port.
Packets	Counts the number of packets successfully sent on the port.
Show/Hide	Check whether or not to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Errors

The Web Manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. Four windows are offered.

Received (RX)
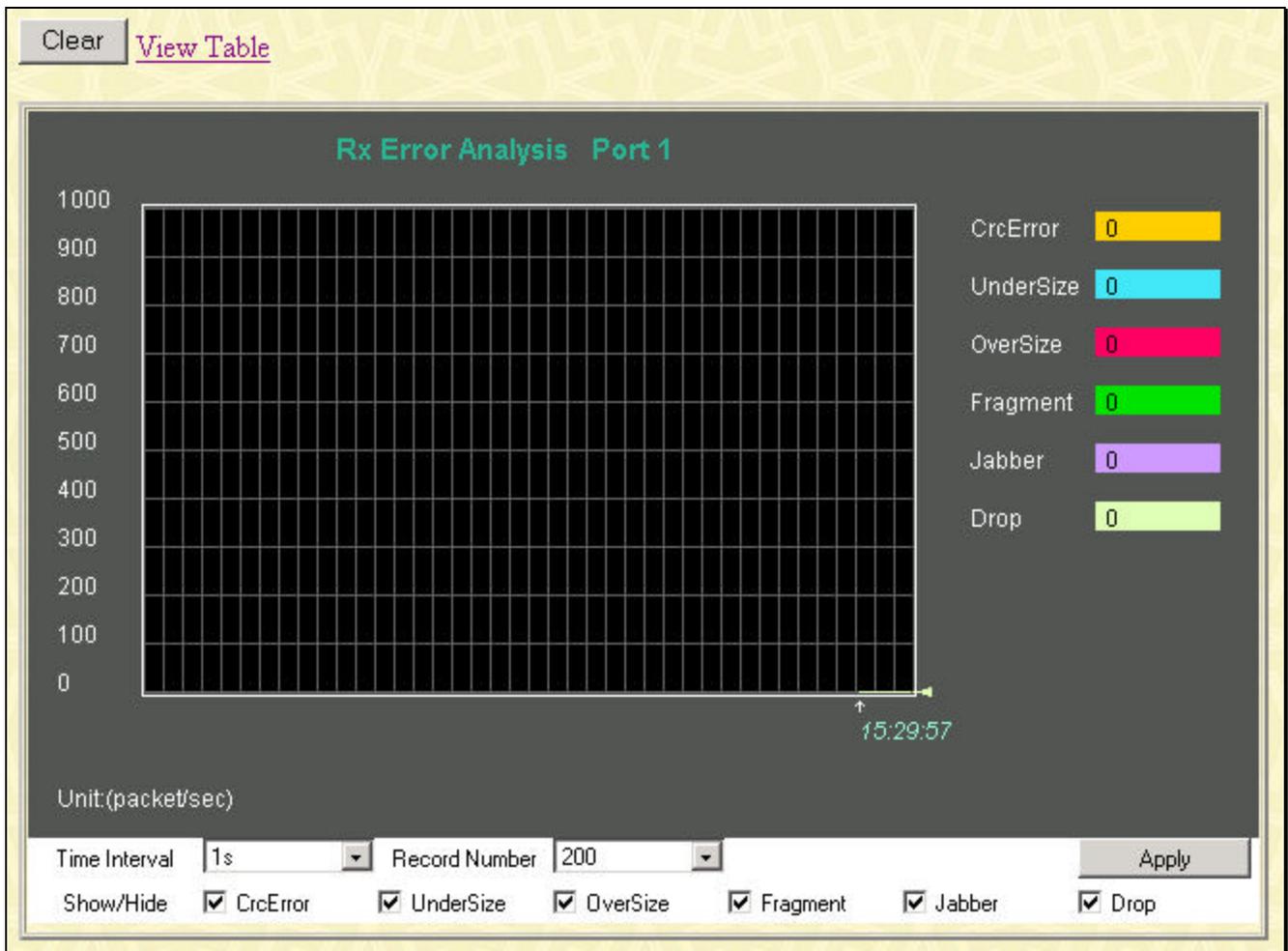
Figure 10 - 9. Rx Error Analysis window (line graph)

View LineChart

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

Packet Analysis of Port 1   Time Interval 1s   OK
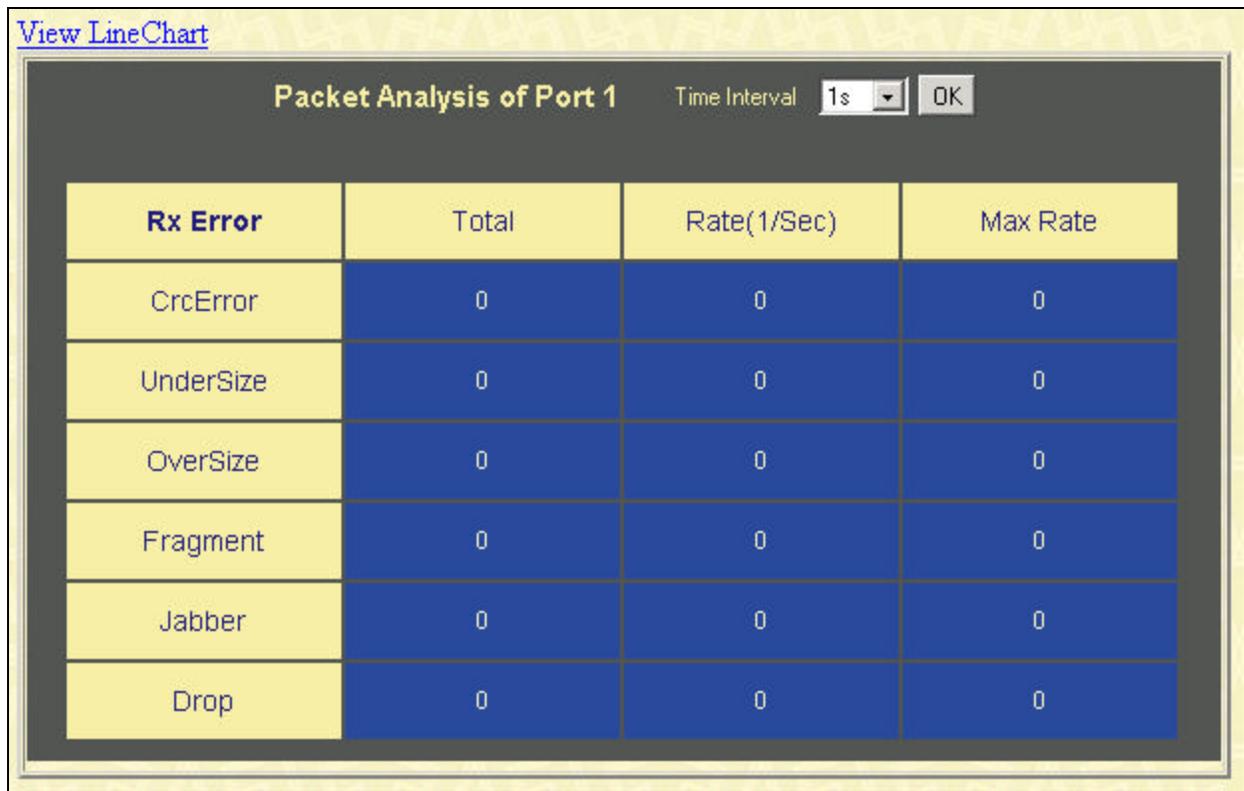
Figure 10 - 10. Rx Error Analysis window (table)

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 *20*.
CrcError	Counts otherwise valid frames that did not end on a byte (octet) boundary.
UnderSize	The number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersize frames usually indicate collision fragments, a normal network occurrence.
OverSize	Counts packets received that were longer than 1518 octets, or if a VLAN frame _1522 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.
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 frames with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522.
Drop	The number of frames that are dropped by this port since the last Switch reboot.
Show/Hide	Check whether or not to display CrcError, UnderSize, OverSize, 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.

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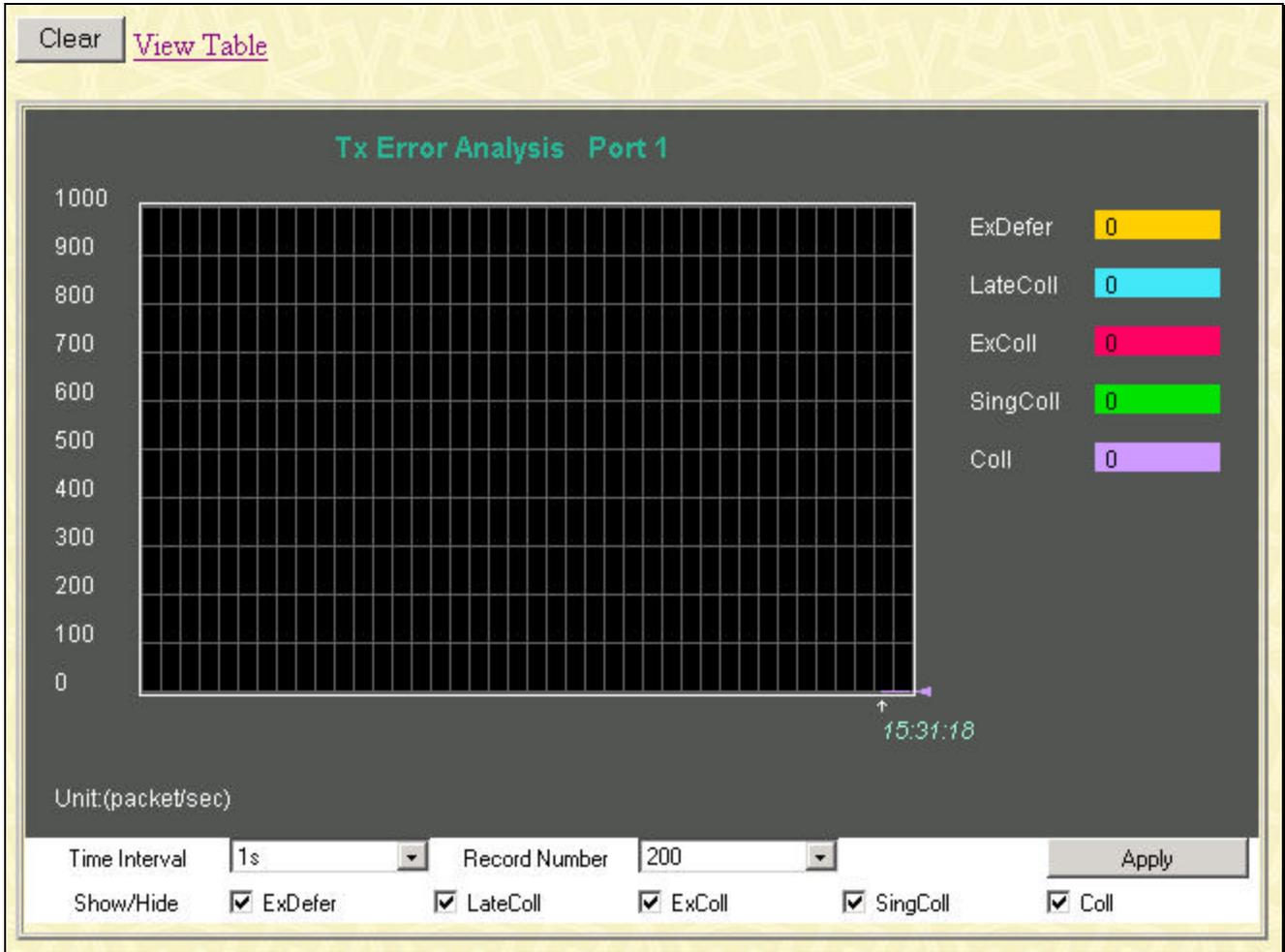
Figure 10 - 11. Tx Error Analysis window (line graph)

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

The following fields can be set:

Parameter	Description

133

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 *20*.
ExDefer	Counts the number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.
LateColl	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
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.

Size

Packet Size

The Web Manager allows packets received by the Switch, arranged in six groups, to be viewed as either a line graph or a table. Two windows are offered.
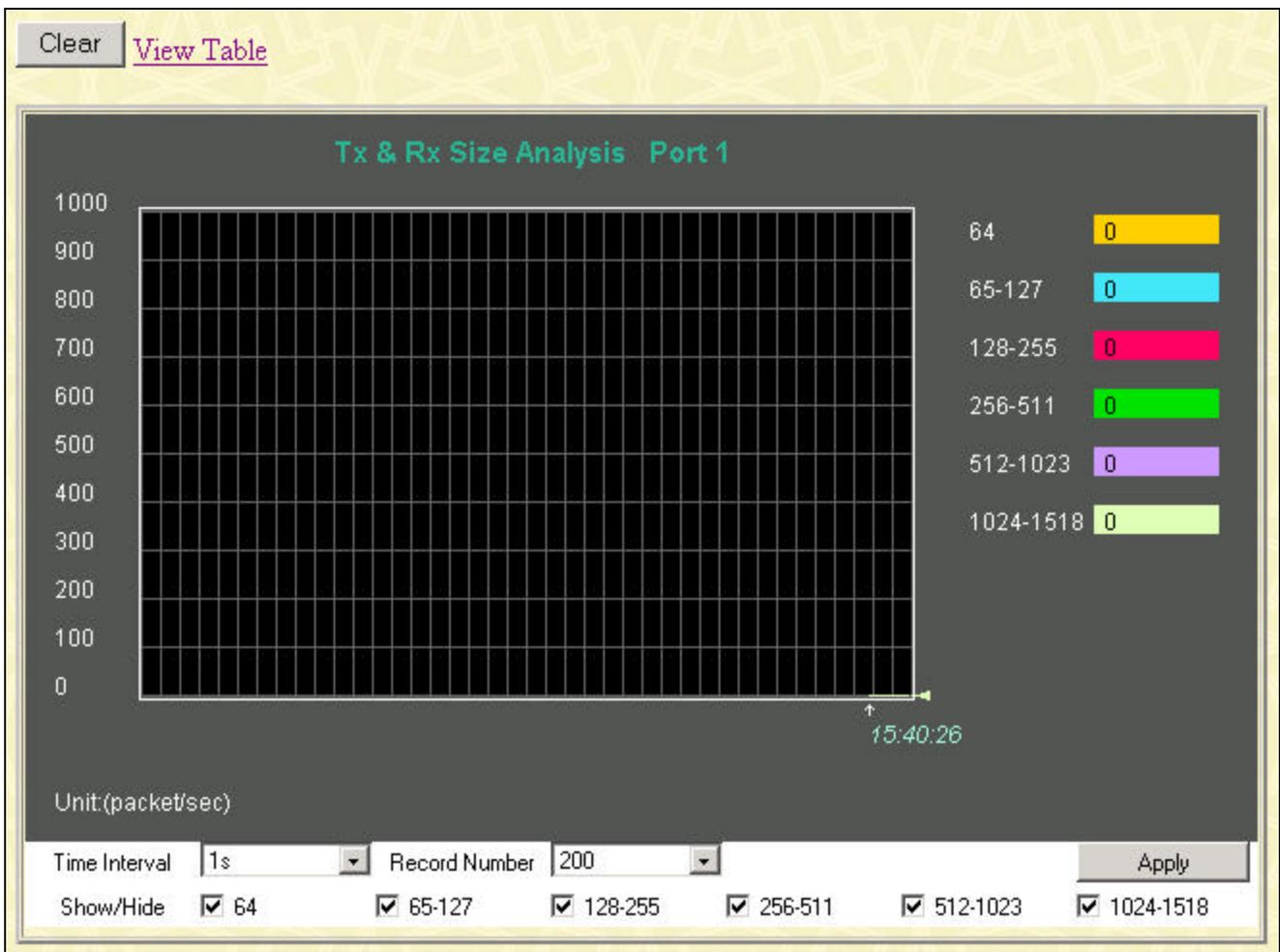
Figure 10 - 13. Rx Size Analysis window (line graph)

134
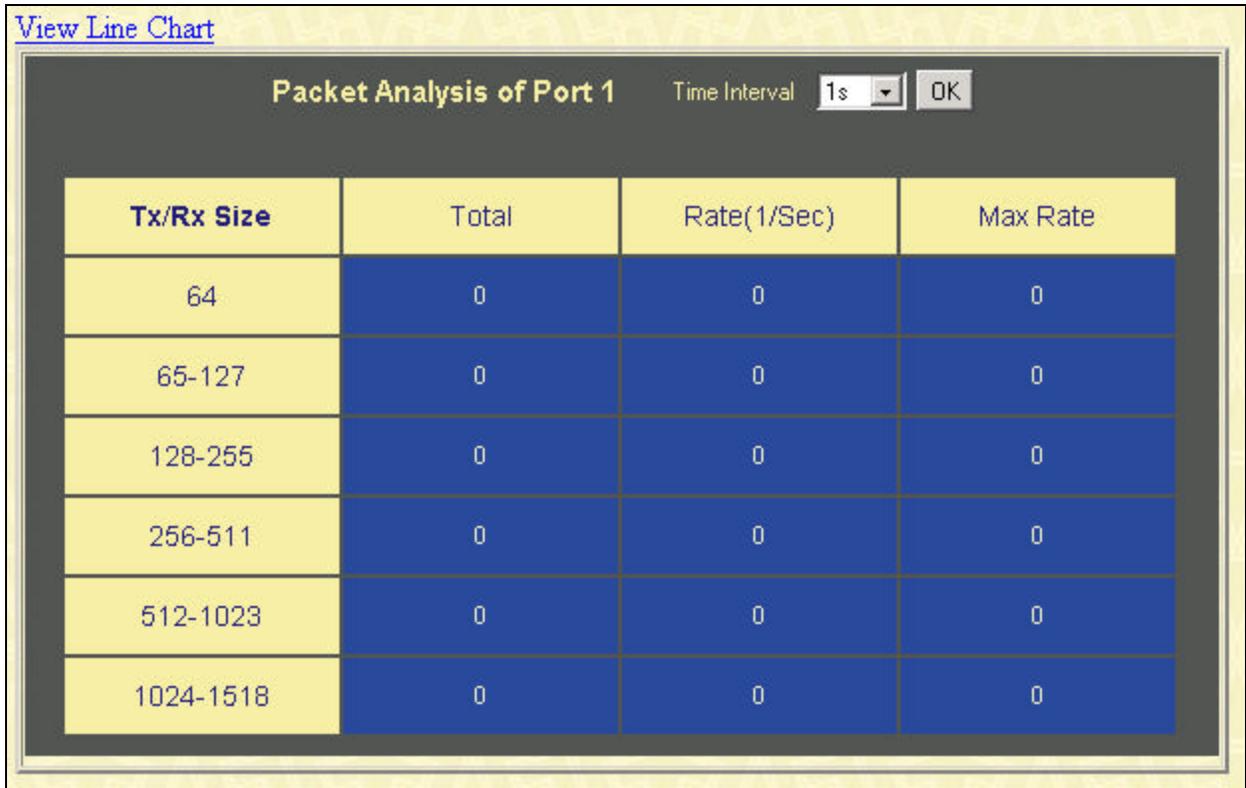
Figure 10 - 14. Rx Size Analysis window (table)

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 *20*.
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 (e xcluding 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.

135

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.

MAC Address

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

To view the MAC address forwarding table, from the **Monitoring** menu, click the **MAC Address** link:

Figure 10 - 15. MAC Address Table window

The following fields can be set:

Parameter	Description
VLAN ID	Enter a VLAN ID for the forwarding table to be browsed by.

MAC Address	Enter a MAC address for the forwarding table to be browsed by.	
Port	Enter a port numb er for the forwarding table to be browsed by.	
Find	Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.	
VID	The VLAN ID of the VLAN the port is a member of.	
MAC Address	The MAC address entered into the address table.	
Port	The port that the MAC address above corresponds to.	
Learned	How the switch discovered the MAC address. The possible entries are *Dynamic*, *Self*, and *Static*.	
Next	Click this button to view the next page of the address table.	

ARP Table

The **ARP Table** window may be found in the **Monitoring** menu in the **Size** folder. This window will show current **ARP** entries on the Switch.

Interface Name			
IP Address	0.0.0.0		Find

ARP Table

Interface Name	IP Address	MAC Address	Type
System	10.0.0.0	ff-ff-ff-ff-ff-ff	Local/Broadcast
System	10.0.0.3	00-03-4b-40-7f-f4	Dynamic
System	10.0.0.4	00-80-2d-39-ff-f4	Dynamic
System	10.0.25.1	00-d0-59-a9-2a-c4	Dynamic
System	10.0.46.1	00-80-c8-91-15-eb	Dynamic
System	10.0.51.12	00-50-ba-da-00-1d	Dynamic
System	10.0.58.4	00-0c-6e-43-13-ae	Dynamic
System	10.1.1.101	00-50-ba-15-48-56	Dynamic
System	10.1.1.103	00-50-ba-97-d7-c9	Dynamic
System	10.1.1.151	00-50-ba-70-d6-d0	Dynamic
System	10.1.1.152	00-13-00-00-00-01	Dynamic
System	10.1.1.154	00-50-ba-97-d9-56	Dynamic
System	10.1.1.157	00-50-ba-71-20-d6	Dynamic
System	10.1.1.161	00-50-ba-70-e4-89	Dynamic
System	10.1.1.164	00-50-ba-70-e4-65	Dynamic
System	10.1.1.166	00-50-ba-70-e4-58	Dynamic
System	10.1.1.167	00-50-ba-70-e4-45	Dynamic
System	10.1.1.168	00-50-ba-70-e4-57	Dynamic
System	10.1.1.169	00-50-ba-70-e4-4e	Dynamic
System	10.1.1.170	00-50-ba-70-e4-7a	Dynamic

Next

Total Entries: 365

Figure 10 - 16. ARP Table window

To search a specific ARP entry, enter an interface name into the **Interface Name** or an **IP address** and click **Find.**

IGMP Snooping Group

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

To view the IGMP Snooping table, click **IGMP Snooping Group** on the **Monitoring** menu:

Figure 10 - 17. IGMP Snooping Table window

The following fields can be set or are displayed.

Parameter	Description
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.

IGMP Snooping Forwarding

To view the IGMP Snooping Forwarding Table, click **IGMP Snooping Forwarding** on the **Monitoring** menu:

Figure 10 - 18. IGMP Snooping Forwarding Table window

Enter the VLAN ID for the desired IGMP Snooping Forwarding Table and click **Search**.

VLAN Status

To view the VLAN Status, click **VLAN Status** on the **Monitoring** menu:

Figure 10 - 19. VLAN Status window

This read-only window displays information about the switch's current VLAN configuration.

Router Port

This displays which of the switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port in the first two rows of the **Router Port** window. A router port that is dynamically configured by the switch is located in the third and fourth rows.

To view the Router Port table, click on the **Router Port** link on the **Monitoring** menu:

Figure 10 - 20. Router Port window

Static router ports are configured by the user and dynamically assigned router ports are configured by the switch.

Power Status

To view the Power Status of the Main Power Supply and the Redundant Power supply, click on **Power Status** in the **Monitoring** menu:

Figure 10 - 21. Power Status table

Port Access Control

Authenticator State

To view the Authenticator Status for Auth PAE State, Backend State, and Port Status, click on the **Authenticator State** link on the **Port Access Control** folder on the **Monitoring** menu:

Figure 10 - 22. Authenticator Status window

Layer 3 Features

IP Address

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

Interface	IP Address	Port	Learned
System	10.0.46.1	5	Dynamic
System	10.0.58.4	5	Dynamic
System	10.1.23.1	5	Dynamic
System	10.1.29.1	5	Dynamic
System	10.1.29.2	5	Dynamic
System	10.1.29.22	5	Dynamic
System	10.1.49.1	5	Dynamic
System	10.1.49.9	5	Dynamic
System	10.1.49.11	5	Dynamic
System	10.1.49.15	5	Dynamic
System	10.1.49.20	5	Dynamic
System	10.1.49.100	5	Dynamic
System	10.1.49.251	5	Dynamic
System	10.1.49.252	5	Dynamic
System	10.1.53.1	5	Dynamic
System	10.2.7.150	5	Dynamic
System	10.2.28.168	5	Dynamic
System	10.2.85.1	5	Dynamic
System	10.2.87.56	5	Dynamic
System	10.3.12.1	5	Dynamic

IP Address [0.0.0.0]   [Find]

IP Address Table

Total Entries: 259

Figure 10 - 23. IP Address Routing Table

Routing Table

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

Destination Address [0.0.0.0]

Netmask [0.0.0.0]   [Find]

Routing Table

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

Total Entries: 1

Figure 10 - 24. Routing Table window

141

IP Multicast Forwarding Table

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

Multicast Group	0.0.0.0	
Source IP	0.0.0.0	Find

IP Multicast Forwarding Table

Multicast Group	Source IP Address	Source Mask	Upstream Neighbor	Expire Time	Protocol

Total Entries: 0

Figure 10 - 25. IP Multicast Forwarding Table

IGMP Group Table

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

Interface Name		
Multicast Group	0.0.0.0	Find

IGMP Group Table

Interface Name	Multicast Group	Last Reporter IP	IP Querier	IP Expire

Total Entries: 0

Figure 10 - 26. IGMP Group Table

To view the specific details for an entry, click the corresponding **View** icon revealing the following window:

This window holds the following information:

Parameter	Description
Interface Name	Defines the interface name of the reporting multicast group.
Multicast Group	The IP address of the reporting Multicast Group.
Last Reporter IP	The IP address of the host member of the multicast group to last report being a member of that group.
IP Querier	The IP Address of a selected multicast router, which is designated to query host interfaces about their multicast reception state.
IP Expire	The length of time, in seconds, until the entry will change filter mode from exclude to include. If the filter is in include mode, this timer will display 0. If the filter is in exclude mode, this timer will be counting down to zero from a pre-calculated figure based on the users implementation of IGMP.

NOTE: All timers within the preceding window can be determined using IGMP configurations to perform the following calculation:

(Group Membership Interval x Robustness Variable) + One Query Response Interval

142

OSPF Monitoring

This section offers windows regarding OSPF (Open Shortest Path First) information on the Switch, including the **OSPF LSDB Table**, **OSPF Neighbor Table** and the **OSPF Virtual Neighbor Table**. To view these tables, open the **Monitoring** folder and click **OSPF Monitoring**.

OSPF LSDB Table

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

Figure 10 - 27. OSPF LSDB Table

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

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

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

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

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

The following fields are displayed in the **OSPF LSDB Table**:

Parameter	Description
Area ID	Allows the entry of an OSPF Area ID. This Area ID will then be used to search the table, and display an entry – if there is one.
LSDB Type	Displays which one of eight types of link advertisements by which the current link was discovered by the Switch: *All*, Router link (*RTRLink*), Network link (*NETLink*), Summary link (*Summary*), Autonomous System link (*ASSummary*), Autonomous System external link (*ASExternal)*, MCGLink (*Multicast Group*), and NSSA (*Not So Stubby Area*)
Adv. Router ID	Displays the Advertising Router's ID.
Link State ID	This field identifies the portion of the Internet environment that is being described by the advertisement. The contents of this field depend on the advertisement's LS type.

LS Type	Link State ID
1	The originating router's Router ID.
2	The IP interface address of the network's Designated Router.
3	The destination network's IP address.
4	The Router ID of the described

	AS boundary router.
Cost	Displays the cost of the table entry.
Sequence	Displays a sequence number corresponding to number of times the current link has been advertised as changed.

OSPF Neighbor Table

This table can be found in the **OSPF Monitoring** folder by clicking on the **OSPF Neighbor Table** link. Routers that are connected to the same area or segment become neighbors in that area. Neighbors are elected via the Hello protocol. IP multicast is used to send out Hello packets to other routers on the segment. Routers become neighbors when they see themselves listed in a Hello packet sent by another router on the same segment. In this way, two-way communication is guaranteed to be possible between any two neighbor routers. This table displays OSPF neighbors of the Switch.

Figure 10 - 28. OSPF Neighbor Table

To search for OSPF neighbors, enter an IP address and click Find. Valid OSPF neighbors will appear in the OSPF Neighbor Table below.

OSPF Virtual Neighbor

This table can be found in the **OSPF Monitoring** folder by clicking on the **OSPF Virtual Neighbor Table** link. This table displays a list of **Virtual OSPF Neighbors** of the Switch. The user may choose specifically search a virtual neighbor by using one of the two search options at the top of the screen, which are:

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

Figure 10 - 29.OSPF Virtual Neighbor Table

DVMRP Monitoring

This menu allows the **DVMRP** (Distance-Vector Multicast Routing Protocol) to be monitored for each IP interface defined on the Switch. This folder, found in the **Monitoring** folder, offers 3 screens for monitoring; **Browse DVMRP Routing Table**, **Browse DVMRP Neighbor Address Table** and **Browse DVMRP Routing Next Hop Table.** Information on DVMRP and its features in relation to the DGS-3324SRi can be found in Section 6, under **IP Multicast Routing Protocol**.

DVMRP Routing Table

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

Figure 10 - 30.DVMRP Routing Table

DVMRP Neighbor Table

This table, found in the **Monitoring** menu under **DVMRP Monitor > Browse DVMRP Neighbor Table** contains information about DVMRP neighbors of the Switch. To search this table, enter either an **Interface Name** or **Neighbor Address** into the respective field and click the **Find** button. DVMRP neighbors of that entry will appear in the **DVMRP Neighbor Table** below.

Figure 10 - 31. DVMRP Neighbor Table

DVMRP Routing Next Hop Table

The **DVMRP Routing Next Hop Table** contains information regarding the next-hop for forwarding multicast packets on outgoing interfaces. Each entry in the **DVMRP Routing Next Hop Table** refers to the next-hop of a specific source to a specific multicast group address. This table is found in the **Monitoring** menu under **DVMRP Monitoring,** with the heading **Browse DVMRP Routing Next Hop Table.** To search this table, enter either an **Interface Name** or **Source IP Address** into the respective field and click the **Find** button. The next hop of that DVMRP Routing entry will appear in the **DVMRP Routing Next Hop Table** below.

Figure 10 - 32. DVMRP Routing Next Hop Table

PIM Monitoring

Multicast routers use **Protocol Independent Multicast (PIM)** to determine which other multicast routers should receive multicast packets. To find out more information concerning PIM and its configuration on the Switch, see the **IP Multicast Routing Protocol** chapter of Section 6, **Configuration**.

PIM Neighbor Table

The **PIM Neighbor Address Table** contains information regarding each of a router's PIM neighbors. This screen may be found in the **Monitoring** folder under the heading **PIM Monitor**. To search this table, enter either an **Interface Name** or **Neighbor Address** into the respective field and click the **Find** button. PIM neighbors of that entry will appear in the **PIM Neighbor Table** below.

PIM Neighbor Address Table		
Interface Name	Neighbor Address	Expire Time
Total Entries: 0		

Figure 10 - 33. PIM Neighbor Table

Section 11

Maintenance

TFTP Services
Switch History
Ping Test
Save Changes
Reboot Services
Logout

A detailed discussion regarding the Simple Network Monitoring Protocol including description of features and a brief introduction to SNMP.

TFTP Utilities

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

Download Firmware from Server

To update the switch's firmware, click on the **Maintenance** folder and then the **TFTP Services** folder and finally click on the **Download Firmware from TFTP Server** link:

Figure 11 - 1. Download Firmware from Server window

Enter the IP address of the TFTP server in the **Server IP Address** field. The TFTP server must be on the same IP subnet as the switch. Enter the path and the filename to the firmware file on the TFTP server. The TFTP server must be running TFTP server software to perform the file transfer. TFTP server software is a part of many network management software packages – such as NetSight, or can be obtained as a separate program. Use the **Save Changes** from the **Maintenance** menu to enter the address into NV-RAM. Click **Start** to initiate the file transfer.

Download Settings from TFTP Server

To download a configuration file for the Switch, click on the **Maintenance** folder and then the **TFTP Services** folder and finally click on the **Download Settings from TFTP Server** link:
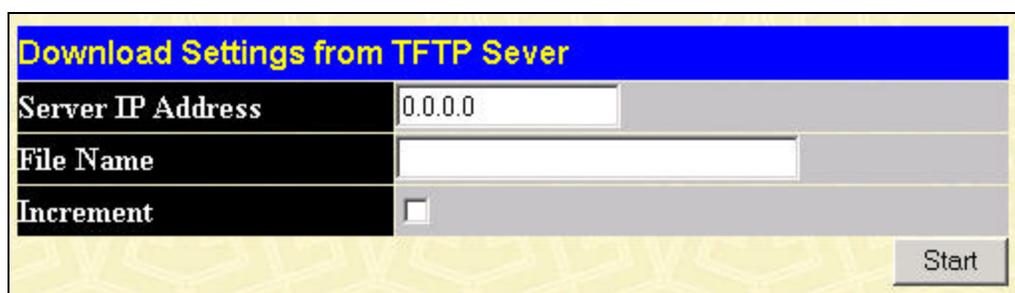
Figure 11 - 2. Download Settings from TFTP Server window

Enter the IP address of the TFTP server and specify the location of the switch configuration file on the TFTP server and click **Start** to initiate the file transfer.

Upload Settings to TFTP Server

To download a configuration file for the switch, click on the **Maintenance** menu and then the **TFTP Services** folder and finally click on the **Upload Settings to TFTP Server** link:

Upload Settings to TFTP Sever

Server IP Address	0.0.0.0
File Name	

Start

Figure 11 - 3. Upload Settings to TFTP Server window

Enter the IP address of the TFTP server and the path and filename of the settings file on the TFTP server and click **Start** to initiate the file transfer.

Upload Log to TFTP Server

To upload the history log for the switch, click on the **Maintenance** folder, the **TFTP Services folder**, and then click on the **Upload log to TFTP Server** link:

Upload log to TFTP Sever

Server IP Address	0.0.0.0
File Name	

Start

Figure 11 - 4. Upload log to TFTP Server window

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

Switch History

This allows the Switch History log to be viewed. The switch records all traps, in sequence, that identify events on the switch. The time since the last cold start of the switch is also recorded.

To view the switch history log, click the **Switch History** link on the **Maintenance** menu:

Switch History

Sequence	Time	Log Text
248	0 days 00:01:19	Successful login through Web (Username: Anonymous)
247	0 days 00:01:10	System started up
246	0 days 00:00:55	Stacking LED is reset(1)
245	0 days 00:00:54	Stacking LED is reset(1)
244	0 days 00:00:53	Stacking LED is reset(1)
243	0 days 00:00:53	Stacking LED is reset(1)
242	0 days 00:00:53	Spanning Tree Protocol is disabled
241	0 days 00:00:52	Stacking LED is reset(1)
240	0 days 00:00:16	Port 50 link down
239	0 days 00:00:16	Port 49 link down
238	0 days 00:00:16	Port 48 link down
237	0 days 00:00:16	Port 47 link down
236	0 days 00:00:16	Port 46 link down
235	0 days 00:00:16	Port 45 link down
234	0 days 00:00:16	Port 44 link down
233	0 days 00:00:16	Port 43 link down
232	0 days 00:00:16	Port 42 link down
231	0 days 00:00:16	Port 41 link down
230	0 days 00:00:16	Port 40 link down
229	0 days 00:00:16	Port 39 link down

Clear   Next

Figure 11 - 5. Switch History window

Ping Test

Ping is a small program that sends data packets to the IP address you specify. The destination node then returns the packets to the switch. This is very useful to verify connectivity between the switch and other nodes on the network.
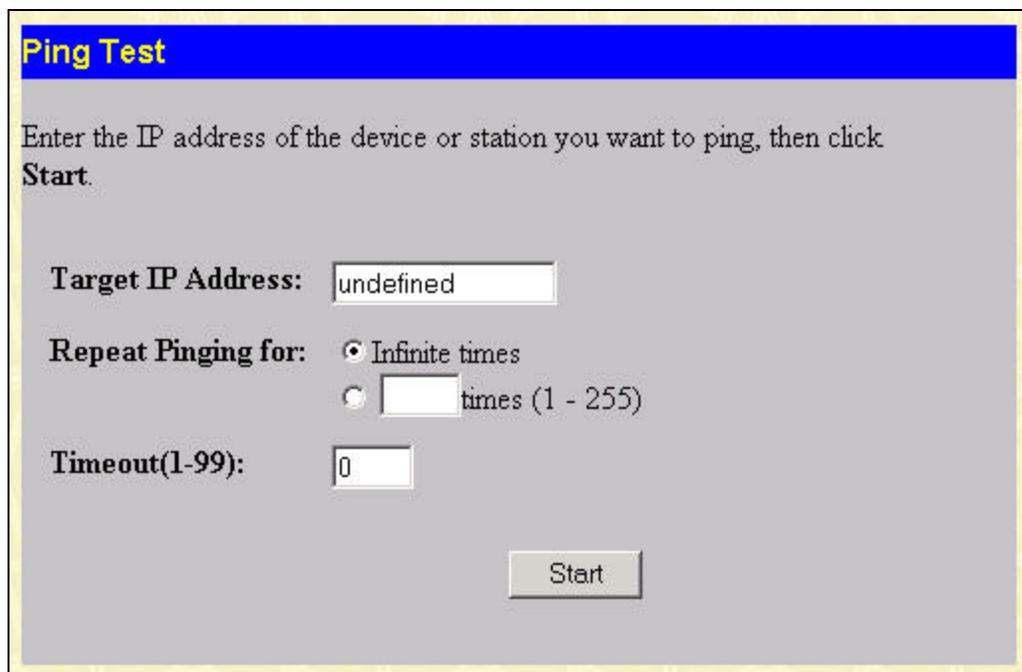
Figure 11 - 6. Ping Test window

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

Save Changes

The DES -3350SR has two levels of memory, normal RAM and non-volatile or NV-RAM.

To retain any configuration changes permanently, highlight **Save Changes** on the **Maintenance** menu. The following screen will appear to verify that your new settings have been saved to NV-RAM.
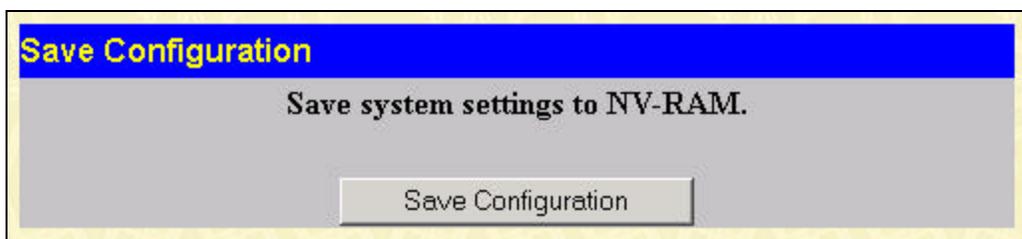
Figure 11 - 7. Save Configuration window

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

Reboot Services

The following folder contains windows that allow you to either **Reboot**, **Reset**, **Reset System**, or **Reset Config**. See the on-screen instructions for the differences among each option.

Note that all changes are kept in normal memory. If a user does not save the result into NV-RAM with the Save Changes function, the switch will recover all the settings the last user configured after the switch is rebooted.
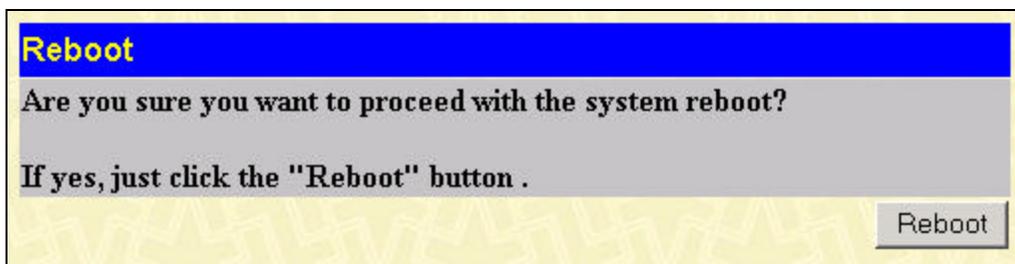
Reboot

Figure 11 - 8. Reboot window

Reset
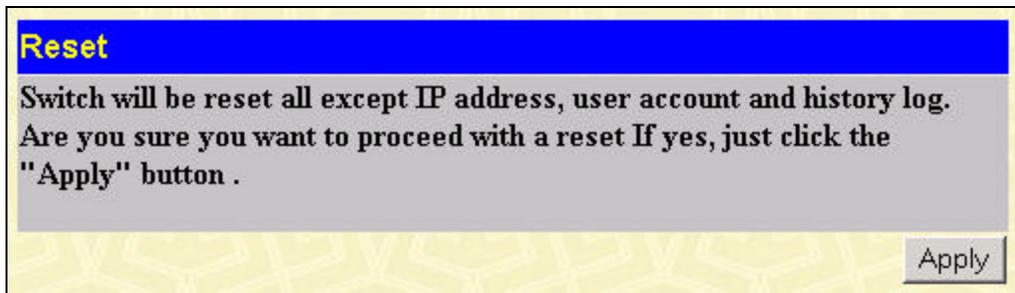
Figure 11 - 9. Reset window

Reset System
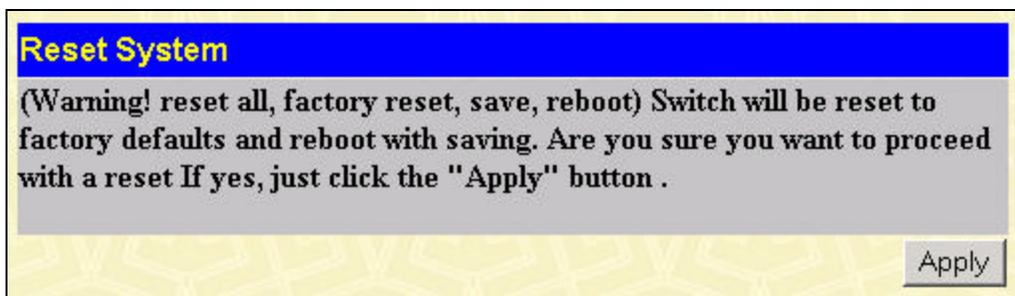
Figure 11 - 10. Reset System window

Reset Config
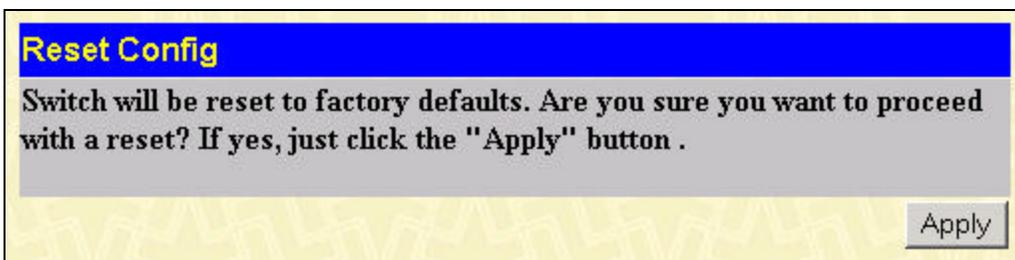
Figure 11 - 11. Reset Config window

Logout
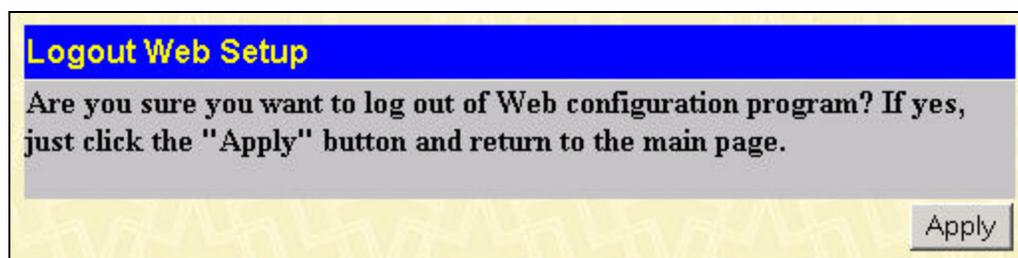
Figure 11 - 12. Logout Web Setup window

Click **Apply** if you want to logout of the Web configuration program and return to the main page.

Appendix A

Technical Specifications

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 P/Q VLAN
	IEEE 802.3x Full-duplex Flow Control
	ANSI/IEEE 802.3 Nway auto-negotiation
Protocols:	CSMA/CD
Data Transfer Rates: Ethernet	Half-duplex Full-duplex
Fast Ethernet	10 Mbps 20Mbps
Gigabit Ethernet	100Mbps 200Mbps
	n/a 2000Mbps
Topology:	Star
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)
Mini GBIC:	IEC 793-2:1992 Type A1a - 50/125um multimode Type A1b - 62.5/125um multimode (SC optical connector)
Number of Ports:	48x 10/100 Mbps NWay ports 2 Gigabit Ethernet ports – 1000BASE-T (included) or Mini GBIC (optional)

Physical and Environmental	
AC Input & External Redundant Power Supply :	100 – 120; 200 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	30 watts maximum
DC Fans:	2 built-in 40 x 40 x10 mm fans
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:	441 mm x 309 mm x 44 mm (1U), 19 inch rack-mount width
Weight:	4.4 kg
EMI:	FCC Class A, CE Class A, C-Tick, VCCI Class A
Safety:	CSA International

Performance

151

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	64M Bytes per device
Filtering Address Table:	8K MAC address per device
Packet Filtering/ Forwarding Rate:	Full-wire speed for all connections. 148,800 pps per port (for 100Mbps) 1,488,000 pps per port (for 1000Mbps)
MAC Address Learning:	Automatic update
Forwarding Table Age Time:	Max age: 10–1,000,000 seconds. Default = 300.
Priority Queues:	4 Priority Queues per port

Appendix B

Understanding and Troubleshooting the Spanning Tree Protocol

When the spanning-tree algorithm determines a port should be transitioned to the forwarding state, the following occurs:

- The port is put into the listening state where it receives BPDUs and passes them to the switch's CPU. BPDU packets from the CPU are processed. If no BPDUs that suggest the port should go to the blocking state are received:

- The port waits for the expiration of the forward delay timer. It then moves to the learning state.

- In the learning state, the port learns station location information from the source address of packets and adds this information to its forwarding database.

- The expiration of the forwarding delay timer moves the port to the forwarding state, where both learning and forwarding are enabled. At this point, packets are forwarded by the port.

Blocking State

A port in the blocking state does not forward packets. When the switch is booted, a BPDU is sent to each port in the switch putting these ports into the blocking state. A switch initially assumes it is the root, and then begins the exchange of BPDUs with other switches. This will determine which switch in the network is the best choice for the root switch. If there is only one switch on the network, no BPDU exchange occurs, the forward delay timer expires, and the ports move to the listening state. All STP enabled ports enter the blocking state following switch boot.

A port in the blocking state does the following:

- Discards packets received from the network segment to which it is attached.

- Discards packets sent from another port on the switch for forwarding.

- Does not add addresses to its forwarding database

- Receives BPDUs and directs them to the CPU.

- Does not transmit BPDUs received from the CPU.

- Receives and responds to network management messages.
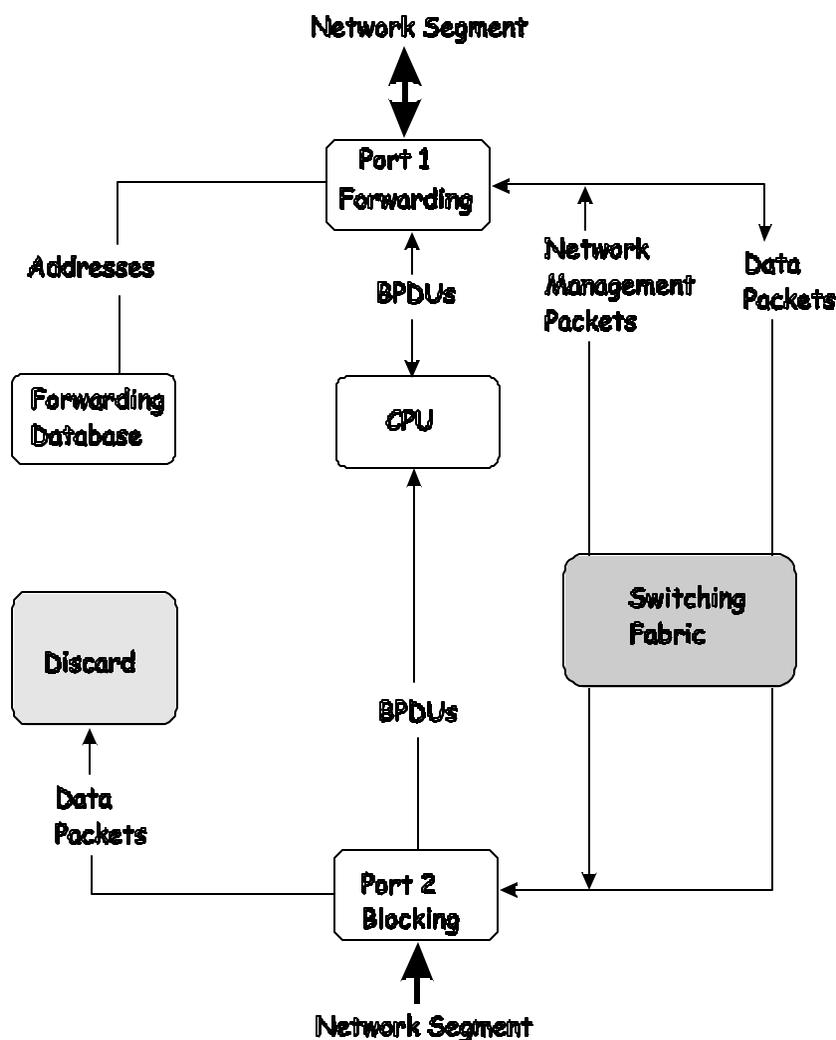
Listening State

The listening state is the first transition for a port from the blocking state. Listening is an opportunity for the switch to receive BPDUs that may tell the switch that the port should not continue to transition to the forwarding state, but should return to the blocking state (that is, a different port is a better choice).

There is no address learning or packet forwarding from a port in the listening state.

A port in the listening state does the following:

- Discards frames received from the network segment to which it is attached.

- Discards packets sent from another port on the switch for forwarding.

- Does not add addresses to its forwarding database

- Receives BPDUs and directs them to the CPU.

- Processes BPDUs received from the CPU.

- Receives and responds to network management messages.
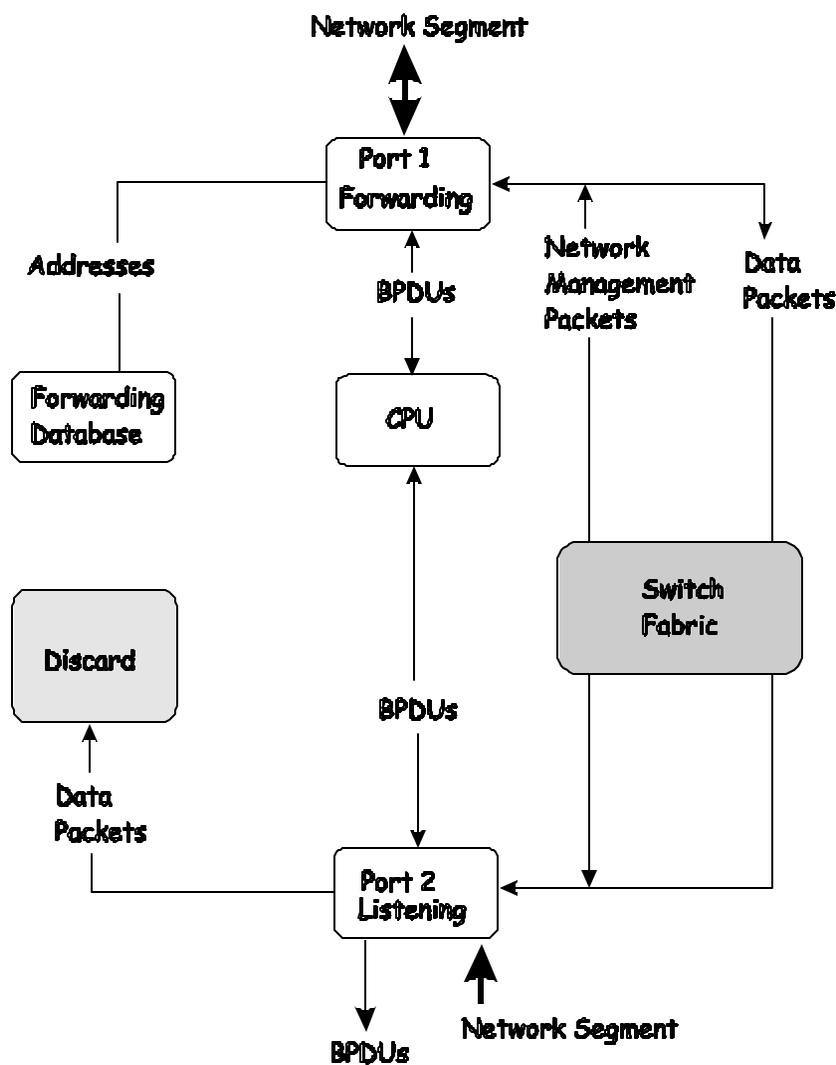
Learning State

A port in the learning state prepares to participate in frame forwarding. The port enters the learning state from the listening state.

A port in the learning state does the following:

- Discards frames received from the network segment to which it is attached.

- Discards packets sent from another port on the switch for forwarding.

- Adds addresses to its forwarding database.

- Receives BPDUs and directs them to the CPU.

- Processes and transmits BPDUs received from the CPU.

- Receives and responds to network management messages .
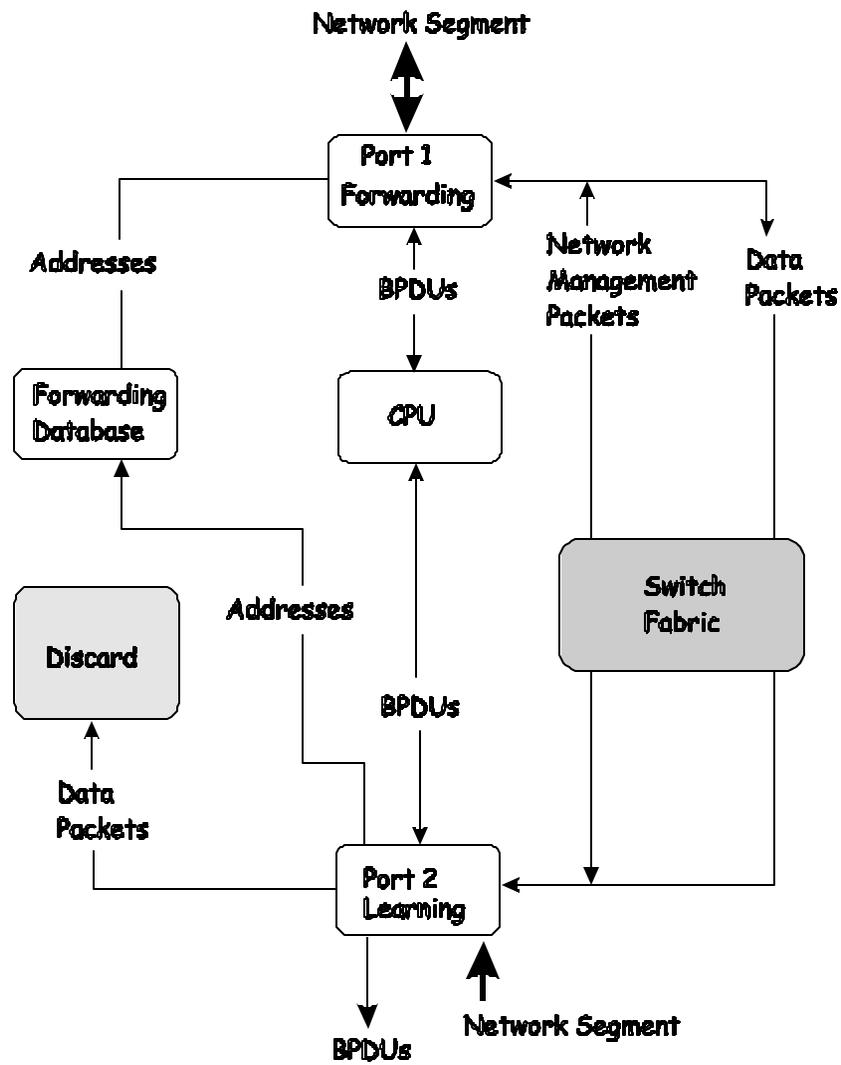
Forwarding State

A port in the forwarding state forwards packets. The port enters the forwarding state from the learning state when the forward delay timer expires.

A port in the forwarding state does the following:

- Forwards packets received from the network segment to which it is attached.
- Forwards packets sent from another port on the switch for forwarding.
- Incorporates station location information into its address database.
- Receives BPDUs and directs them to the system CPU.
- Receives and responds to network management messages.
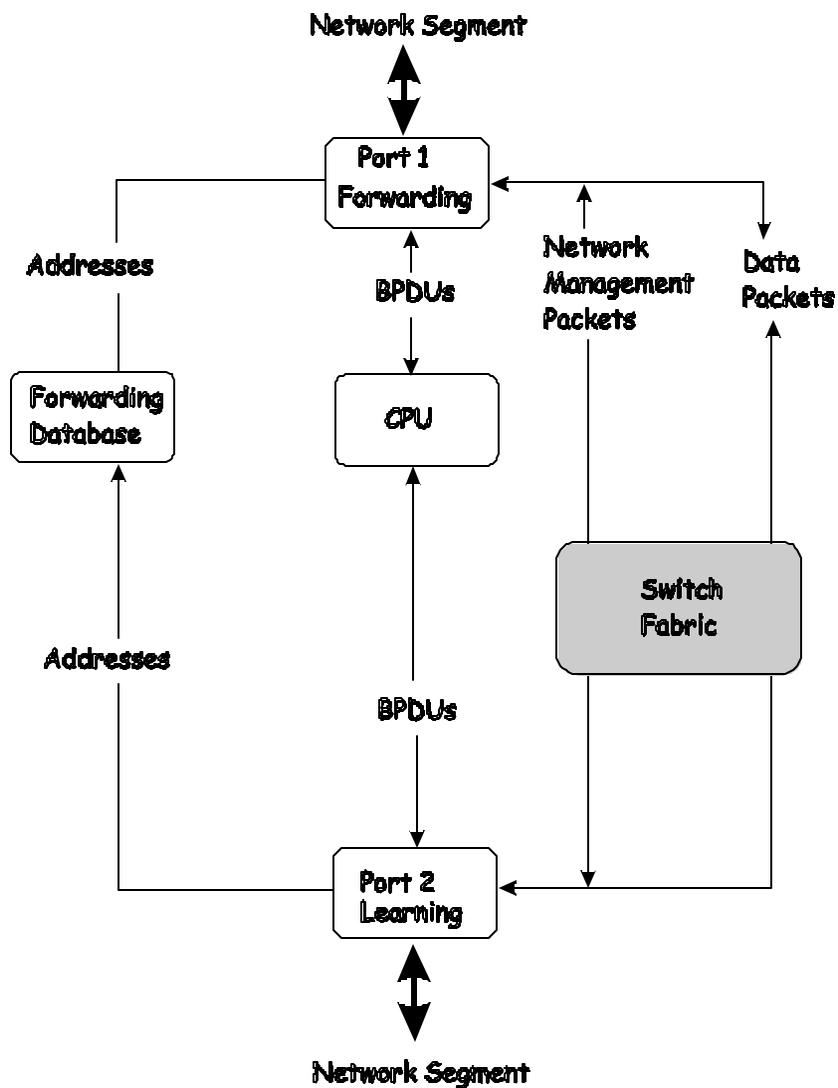
Disabled State

A port in the disabled state does not participate in frame forwarding or STP. A port in the disabled state is virtually non-operational.

A disabled port does the following:

- Discards packets received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database.
- Receives BPDUs, but does not direct them to the system CPU.
- Does not receive BPDUs for transmission from the system CPU.
- Receives and responds to network management messages.
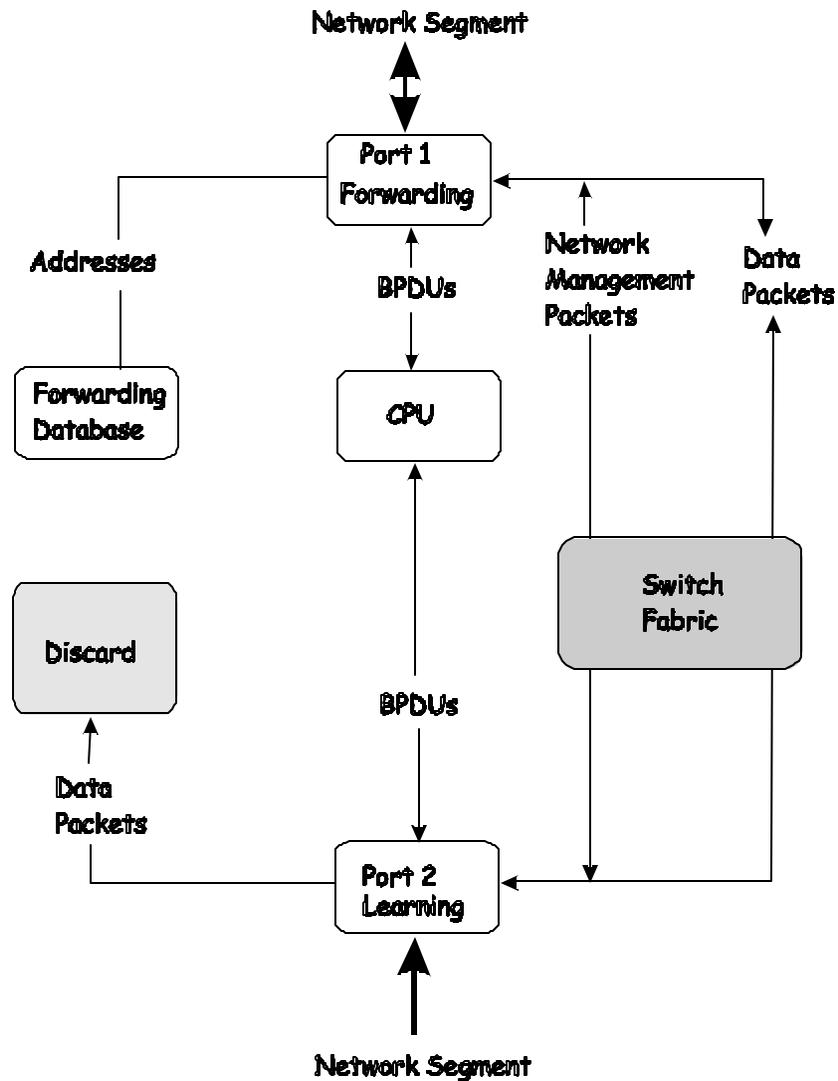
Troubleshooting STP

Spanning Tree Protocol Failure

A failure in the STA generally leads to a bridging loop. A bridging loop in an STP environment comes from a port that should be in the blocking state, but is forwarding packets.
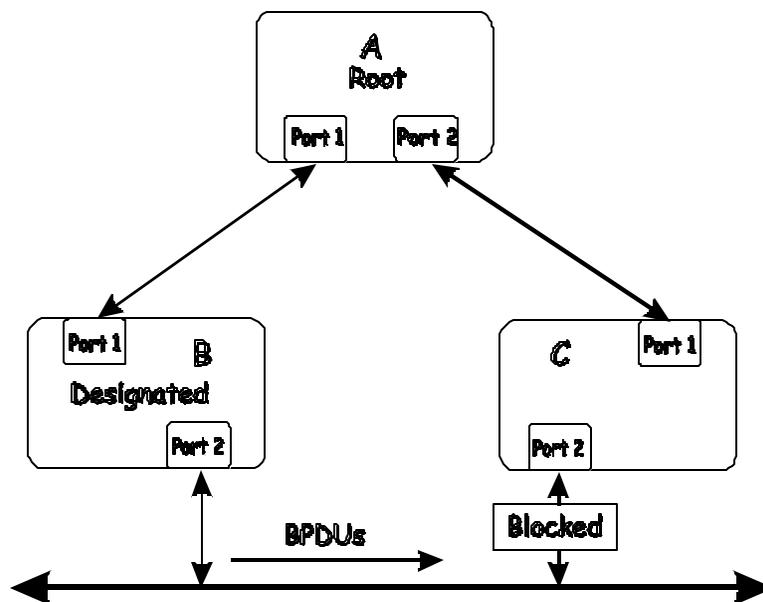
In this example, B has been elected as the designated bridge and port 2 on C is in the blocking state. The election of B as the designated bridge is determined by the exchange of BPDUs between B and C. B had a better BPDU than C. B continues sending BPDUs advertising its superiority over the other bridges on this LAN. Should C fail to receive these BPDUs for longer than the MAX AGE (default of 20 seconds), it could start to transition its port 2 from the blocking state to the forwarding state.

It should be noted: A port must continue to receive BPDUs advertising superior paths to remain in the blocking state.

There are a number of circumstances in which the STA can fail – mostly related to the loss of a large number of BPDUs. These situations will cause a port in the blocking state to transition to the forwarding state.

Full/Half Duplex Mismatch

A mismatch in the duplex state of two ports is a very common configuration error for a point-to-point link. If one port is configured as a full duplex, and the other port is left in auto-negotiation mode, the second port will end up in half-duplex because ports configured as half- or full-duplex do not negotiate.
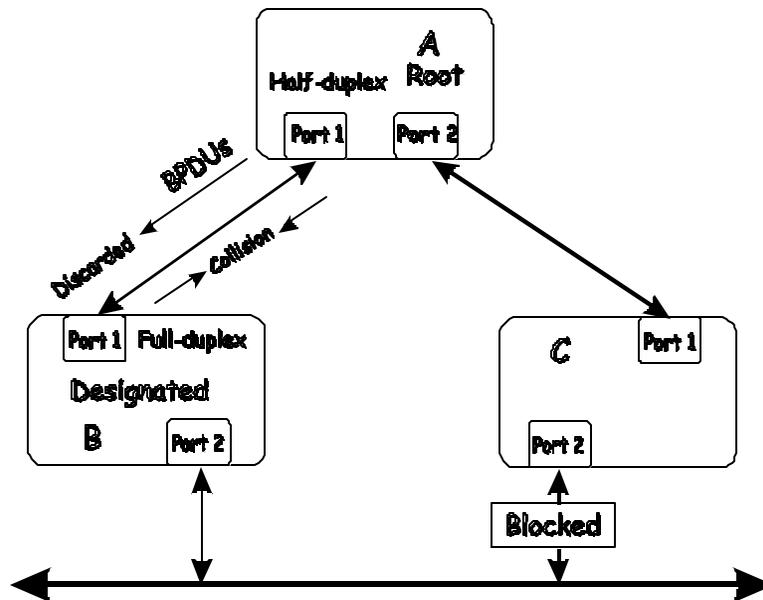
In the above example, port 1 on B is configured as a full-duplex port and port 1 on A is either configured as a half-duplex port, or left in auto-negotiation mode. Because port 1 on B is configured as a full-duplex port, it does not do the carrier sense when accessing the link. B will then start sending packets even if A is using the link. A will then detect collisions and begin to run the flow control algorithm. If there is enough traffic between B and A, all packets (including BPDUs) will be dropped. If the BPDUs sent from A to B are dropped for longer than the MAX AGE, B will lose its connection to the root (A) and will unblock its connection to C. This will lead to a data loop.

Unidirectional Link

Unidirectional links can be caused by an undetected failure in one side of a fiber cable, or a problem with a ports transceiver. Any failure that allows a link to remain up while providing one-way communication is very dangerous for STP.
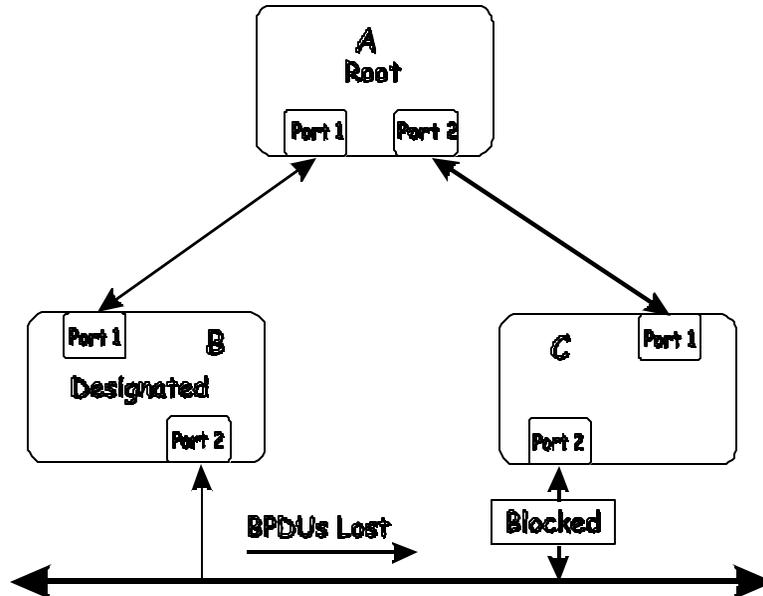
In this example, port 2 on B can receive but not transmit packets. Port 2 on C should be in the blocking state, but since it can no longer receive BPDUs from port 2 on B, it will transition to the forwarding state. If the failure exists at boot, STP will not converge and rebooting the bridges will have no effect. (Note: Rebooting would help temporarily in the previous example).

This type of failure is difficult to detect because the Link-state LEDs for Ethernet links rely on the transmit side of the cable to detect a link. If a unidirectional failure on a link is suspected, it is usually required to go to the console or other management software and look at the packets received and transmitted for the port. A unidirectional port will have many packets transmitted but none received, or vice versa, for example.

Packet Corruption

Packet corruption can lead to the same type of failure. If a link is experiencing a high rate of physical errors, a large number of consecutive BPDUs can be dropped and a port in the blocking state would transition to the forwarding state. The blocking port would have to have the BPDUs dropped for 50 seconds (at the default settings) and a single BPDU would reset the timer. If the MAX AGE is set too low, this time is reduced.

Resource Errors

The DES-3350SR Layer 2 switch performs its switching and routing functions primarily in hardware, using specialized ASICs. STP is implemented in software and is thus reliant upon the speed of the CPU and other factors to converge. If the CPU is over-utilized, it is possible that BPDUs may not be sent in a timely fashion. STP is generally not very CPU intensive and is given priority over other processes, so this type of error is rare.

It can be seen that very low values for the MAX AGE and the FORWARD DELAY can result in an unstable spanning tree. The loss of BPDUs can lead to data loops. The diameter of the network can also cause problems. The default values for STP give a maximum network diameter of about seven. This means that two switches in the network cannot be more than seven hops apart. Part of this diameter restriction is the BPDU age field. As BPDUs are propagated from the root bridge to the leaves of the spanning tree, each bridge increments the age field. When this field is beyond the maximum age, the packet is discarded. For large diameter networks, STP convergence can be very slow.

Identifying a Data Loop

Broadcast storms have a very similar effect on the network to data loops, but broadcast storm controls in modern switches have (along with subnetting and other network practices) have been very effective in controlling broadcast storms. The best way to determine if a data loop exists is to capture traffic on a saturated link and check if similar packets are seen multiple times.

Generally, if all the users of a given domain are having trouble connecting to the network at the same time, a data loop can be suspected. The port utilization data in the switch's console will give unusually high values in this case.

The priority for most cases is to restore connectivity as soon as possible. The simplest remedy is to manually disable all of the ports that provide redundant links. Disabling ports one at a time, and then checking for a restoration of the user's connectivity will identify the link that is causing the problem, if time allows. Connectivity will be restored immediately after disabling a data loop.

Warranty and Registration

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 interfe rence 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.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

BSMI Warning

警告使用者

這是甲類的資訊產品,在居住的環境中使用時,可能會造成射頻干擾,在這種情況下使用者會被要求採取某些適當的對策

Warranty and Registration Information
(All countries and regions excluding USA)
Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am Besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a. Netzkabel oder Netzstecker sint beschädigt.
    b. Flüssigkeit ist in das Gerät eingedrungen.
    c. Das Gerät war Feuchtigkeit ausgesetzt.
    d. Wenn das Gerät nicht der Bedienungsanleitun g ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht großer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

WARRANTIES EXCLUSIVE

IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS.

D-LINK SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY THE CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

LIMITATION OF LIABILITY

IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF A D-LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. IF YOU PURCHASED A D-LINK PRODUCT IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Limited Warranty

Hardware:

D-Link warrants each of its hardware products to be free from defects in workmanship and materials under normal use and service for a period commencing on the date of purchase from D-Link or its Authorized Reseller and extending for the length of time stipulated by the Authorized Reseller or D-Link Branch Office nearest to the place of purchase.

This Warranty applies on the condition that the product Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card.

If the product proves defective within the applicable warranty period, D-Link will provide repair or replacement of the product. D-Link shall have the sole discretion whether to repair or replace, and replacement product may be new or reconditioned. Replacement product shall be of equivalent or better specifications, relative to the defective product, but need not be identical. Any product or part repaired by D-Link pursuant to this warranty shall have a warranty period of not less than 90 days, from dat e of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.

Warranty service may be obtained by contacting a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing/shipping/insurance prepaid. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.

Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

Software:

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system/platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system/platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link product described below ("Hardware") will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below ("Warranty Period"), except as otherwise stated herein.

- Hardware (excluding power supplies and fans): Five (5) Years
- Power supplies and fans: One (1) Year
- Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: The Limited Warranty provided herein by D-Link does not cover: Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law: This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Product Registration:

Register online your D-Link product at http://support.dlink.com/register/

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Trademarks

Copyright statement

CE EMI class A warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

D-Link Europe Limited Product Warranty

General Terms

The Limited Product Warranty set forth below is given by D-LINK (Europe) Ltd. (herein referred to as "D-LINK"). This Limited Product Warranty is only effective upon presentation of the proof of purchase. Upon further request by D-LINK, this warranty card has to be presented, too.

EXCEPT AS EXPRESSLY SET FORTH IN THIS LIMITED WARRANTY, D-LINK MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED IN DURATION TO THE LIMITED WARRANTY PERIOD. SOME STATES OR COUNTRIES DO NOT ALLOW A LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS OR THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS. IN SUCH STATES OR COUNTRIES, SOME EXCLUSIONS OR LIMITATIONS OF THIS LIMITED WARRANTY MAY NOT APPLY TO YOU. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY ALSO HAVE OTHER RIGHTS THAT MAY VARY FROM STATE TO STATE OR FROM COUNTRY TO COUNTRY. YOU ARE ADVISED TO CONSULT APPLICABLE STATE OR COUNTRY LAWS FOR

A FULL DETERMINATION OF YOUR RIGHTS.

This limited warranty applies to D-LINK branded hardware products (collectively referred to in this limited warranty as "D-LINK Hardware Products") sold by from D-LINK (Europe) Ltd., its worldwide subsidiaries, affiliates, authorized resellers, or country distributors (collectively referred to in this limited warranty as "D-LINK") with this limited warranty. The Term "D-LINK Hardware Product" is limited to the hardware components and all its internal components including firmware. The term "D-LINK Hardware Product" DOES NOT include any software applications or programs.

Geographical Scope of the Limited Product Warranty

This Limited Product Warranty is applicable in all European Countries as listed in the addendum "European Countries for D-LINK Limited Product Warranty". The term "European Countries" in this D-LINK Limited Product Warranty only include the countries as listed in this addendum. The Limited Product Warranty will be honored in any country where D-LINK or its authorized service providers offer warranty service subject to the terms and conditions set forth in this Limited Product Warranty. However, warranty service availability and response times may vary from country to country and may also be subject to registration requirements.

Limitation of Product Warranty

D-LINK warrants that the products described below under normal use are free from material defects in materials and workmanship during the Limited Product Warranty Period set forth below ("Limited Product Warranty Period"), if the product is used and serviced in accordance with the user manual and other documentation provided to the purchaser at the time of purchase (or as amended from time to time). D-LINK does not warrant that the products will operate uninterrupted or error-free or that all deficiencies, errors, defects or non-conformities will be corrected.

This warranty shall not apply to problems resulting from: (a) unauthorised alterations or attachments; (b) negligence, abuse or misuse, including failure to operate the product in accordance with specifications or interface requirements; (c) improper handling; (d) failure of goods or services not obtained from D-LINK or not subject to a then-effective D-LINK warranty or maintenance agreement; (e) improper use or storage; or (f) fire, water, acts of God or other catastrophic events. This warranty shall also not apply to any particular product if any D-LINK serial number has been removed or defaced in any way.

D-LINK IS NOT RESPONSIBLE FOR DAMAGE THAT OCCURS AS A RESULT OF YOUR FAILURE TO FOLLOW THE INSTRUCTIONS FOR THE D-LINK HARDWARE PRODUCT.

Limited Product Warranty Period

The Limited Product Warranty Period starts on the date of purchase from D-LINK. Your dated sales or delivery receipt, showing the date of purchase of the product, is your proof of the purchase date. You may be required to provide proof of purchase as a condition of receiving warranty service. You are entitled to warranty service according to the terms and conditions of this document if a repair to your D-LINK branded hardware is required within the Limited Product Warranty Period.

This Limited Product Warranty extends only to the original end-user purchaser of this D-LINK Hardware Product and is not transferable to anyone who obtains ownership of the D-LINK Hardware Product from the original end-user purchaser.

Product Type	Product Warranty Period
Managed Switches (i.e. switches with built in SNMP agent)(including modules and management software)	Five (5) years
All other products	Two (2) years
Spare parts (i.e. External Power Adapters, Fans)	One (1) year

The warranty periods listed above are effective in respect of all D-LINK products sold in European Countries by D-LINK or one of its authorized resellers or distributors from 1st of January 2004. All products sold in European Countries by D-LINK or one of its authorized resellers or distributors before 1st January 2004 carry 5 years warranty, except power supplies, fans and accessories that are provided with 2 year warranty.

The warranty period stated in this card supersedes and replaces the warranty period as stated in the user's manual or in the purchase contract for the relevant products. For the avoidance of doubt, if you have purchased the relevant D-LINK product as a consumer your statutory rights remain unaffected.

Performance of the Limited Product Warranty

If a product defect occurs, D-LINK's sole obligation shall be to repair or replace any defective product free of charge to the original purchaser provided it is returned to an Authorized D-LINK Service Center during the warranty period. Such repair or replacement will be rendered by D-LINK at an Authorized D-LINK Service Center. All component parts or hardware products removed under this limited warranty become the property of D-LINK. The replacement part or product takes on the remaining limited warranty status of the removed part or product. The replacement product need not be new or of an identical make, model or part; D-LINK may in its discretion replace the defective product (or any part thereof) with any reconditioned equivalent (or superior) product in all material respects to the defective product. Proof of purchase may be required by D-LINK.

Warrantor

D-Link (Europe) Ltd.

4th Floor, Merit House

Edgware Road

Colindale

London NW9 5 AB

United Kingdom

Telephone: +44-020-8731-5555

Facsimile: +44-020-8731-5511

www.dlink.co.uk

D-Link Europe Limited Produktgarantie

Allgemeine Bedingungen

Die hierin beschriebene eingeschränkte Garantie wird durch D-LINK (Europe) Ltd. gewährt (im Folgenden: „D-LINK"). Diese eingeschränkte Garantie setzt voraus, dass der Kauf des Produkts nachgewiesen wird. Auf Verlangen von D-LINK muss auch dieser Garantieschein vorgelegt werden.

AUSSER IN DEM HIER AUSDRÜCKLICH BESCHRIEBENEN UMFANG GEWÄHRT D-LINK KEINE WEITEREN GARANTIEN, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND. INSBESONDERE WIRD NICHT STILLSCHWEIGEND EINE GARANTIE FÜR DIE ALLGEMEINE GEBRAUCHSTAUGLICHKEIT ODER DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ERKLÄRT. D-LINK LEHNT AUSDRÜCKLICH JEDE GARANTIE AB, DIE ÜBER DIESE EINGESCHRÄNKTE GARANTIE HINAUSGEHT. JEDE GESETZLICH ANGEORDNETE GARANTIE IST AUF DIE LAUFZEIT DER EINGESCHRÄNKTEN GARANTIE BESCHRÄNKT. IN EINIGEN STAATEN ODER LÄNDERN IST DIE ZEITLICHE BESCHRÄNKUNG EINER STILLSCHWEIGEND ERKLÄRTEN GARANTIE SOWIE AUSSCHLUSS ODER BESCHRÄNKUNG VON SCHADENERSATZ FÜR NEBEN- ODER FOLGESCHÄDEN BEIM VERBRAUCHSGÜTERKAUF UNTERSAGT. SOWEIT SIE IN SOLCHEN STAATEN ODER LÄNDERN LEBEN, ENTFALTEN MÖGLICHERWEISE EINIGE AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN DIESER EINGESCHRÄNKTEN GARANTIE GEGENÜBER IHNEN KEINE WIRKUNG. DIESE EINGESCHRÄNKTE GARANTIE GEWÄHRT IHNEN SPEZIFISCHE RECHTE. DARÜBER HINAUS STEHEN IHNEN MÖGLICHERWEISE NOCH WEITERE RECHTE ZU, DIE SICH JEDOCH VON STAAT ZU STAAT ODER VON LAND ZU LAND UNTERSCHEIDEN KÖNNEN. UM DEN UMFANG IHRER RECHTE ZU BESTIMMEN, WIRD IHNEN EMPFOHLEN, DIE ANWENDBAREN GESETZE DES JEWEILIGEN STAATES ODER LANDES ZU RATE ZU ZIEHEN.

Diese eingeschränkte Garantie ist auf Hardware-Produkte der Marke D-LINK (insgesamt im Folgenden: „D-LINK Hardware-Produkte") anwendbar, die von D-LINK (Europe) Ltd. oder dessen weltweiten Filialen, Tochtergesellschaften, Fachhändlern oder Länderdistributoren (insgesamt im Folgenden: „D-LINK") mit dieser eingeschränkten Garantie verkauft wurden. Der Begriff „D-LINK Hardware-Produkte" beinhaltet nur Hardwarekomponenten und deren Bestandteile einschließlich Firmware. Der Begriff "D-LINK Hardware-Produkte" umfasst KEINE Software-Anwendungen oder -programme.

Räumlicher Geltungsbereich der eingeschränkten Garantie

Diese eingeschränkte Garantie gilt für alle genannten europäischen Staaten gemäß dem Anhang „Eingeschränkte Garantie von D-LINK in europäischen Staaten". Im Rahmen dieser eingeschränkten Garantie sind mit dem Begriff „europäische Staaten" nur die im Anhang genannten Staaten gemeint. Die eingeschränkte Garantie findet überall Anwendung, wo D-LINK oder dessen autorisierte Servicepartner Garantiedienste gemäß den Bestimmungen dieser eingeschränkten Garantie erbringen. Gleichwohl kann sich die Verfügbarkeit von Garantiediensten und die Bearbeitungszeit von Land zu Land unterscheiden und von Registrierungsanforderungen abhängig sein.

Einschränkung der Garantie

D-LINK gewährleistet, dass die nachstehend aufgeführten Produkte bei gewöhnlicher Verwendung für die unten angegebene Laufzeit der eingeschränkten Garantie („Garantielaufzeit") frei von wesentlichen Verarbeitungs- und Materialfehlern sind. Voraussetzung hierfür ist jedoch, dass das Produkt entsprechend dem Benutzerhandbuch und den weiteren Dokumentationen, die der Benutzer beim Kauf (oder später) erhalten hat, genutzt und gewartet wird. D-LINK garantiert nicht, dass die Produkte störungs- oder fehlerfrei arbeiteten oder dass alle Mängel, Fehler, Defekte oder Kompatibilitätsstörungen beseitigt werden können.

Diese Garantie gilt nicht für Probleme wegen: (a) unerlaubter Veränderung oder Hinzufügung, (b) Fahrlässigkeit, Missbrauch oder Zweckentfremdung, einschließlich des Gebrauchs des Produkts entgegen den Spezifikationen oder den durch Schnittstellen gegebenen Vorgaben, (c) fehlerhafter Bedienung, (d) Versagen von Produkten oder Diensten, die nicht von D-LINK stammen oder nicht Gegenstand einer zum maßgeblichen Zeitpunkt gültigen Garantie- oder Wartungsvereinbarung sind, (e) Fehlgebrauch oder fehlerhafter Lagerung oder (f) Feuer, Wasser, höherer Gewalt oder anderer Katastrophen. Diese Garantie gilt ebenfalls nicht für Produkte, bei denen eine D-LINK-Seriennummer entfernt oder auf sonstige Weise unkenntlich gemacht wurde.

D-LINK STEHT NICHT FÜR SCHÄDEN EIN, DIE DADURCH ENTSTEHEN, DASS DIE ANLEITUNG FÜR DAS D-LINK HARDWARE-PRODUKT NICHT BEFOLGT WIRD.

Laufzeit der eingeschränkten Garantie

Die Laufzeit der eingeschränkten Garantie beginnt mit dem Zeitpunkt, zu dem das Produkt von D-LINK gekauft wurde. Als Nachweis für den Zeitpunkt des Kaufs gilt der datierte Kauf- oder Lieferbeleg. Es kann von Ihnen verlangt werden, dass Sie zur Inanspruchnahme von Garantiediensten den Kauf des Produkts nachweisen. Wenn Ihre Hardware-Produkte der Marke D-LINK innerhalb der Laufzeit der eingeschränkten Garantie eine Reparatur benötigen, so sind Sie berechtigt, gemäß den Bedingungen dieser eingeschränkten Garantie Garantiedienste in Anspruch zu nehmen.

Diese eingeschränkte Garantie gilt nur für denjenigen, der das D-LINK Hardware-Produkt ursprünglich als originärer Endbenutzer gekauft hat. Sie ist nicht auf Dritte übertragbar, die das D-LINK-Produkt von dem ursprünglichen originären Endbenutzer erworben haben.

Produkttyp	Gewährleistungslaufzeit
Verwaltete Switches (d. h. Switches mit eingebauten SNMP-Agents) (einschließlich Modulen und Verwaltungssoftware)	Fünf (5) Jahre
Alle weiteren Produkte	Zwei (2) Jahre
Ersatzteile (z.B. externe Netzteile, Lüfter)	Ein (1) Jahr

Die oben aufgeführten Garantielaufzeiten gelten für alle D-LINK-Produkte, die in europäischen Staaten ab dem 1. Januar 2004 von D-LINK oder einem autorisierten Fachhändler oder Distributor verkauft werden. Alle vor dem 1. Januar 2004 von D-LINK oder einem autorisierten Vertragshändler oder Distributor verkauften Produkte haben eine Gewährleistung von 5 Jahren; ausgenommen sind Netzteile, Lüfter und Zubehör, diese haben eine Garantie von 2 Jahren.

Die durch diesen Garantieschein festgelegte Garantielaufzeit tritt an die Stelle der im Benutzerhandbuch oder im Kaufvertrag für das jeweilige Produkt angegebenen Laufzeit. Sollten Sie das betreffende D-LINK-Produkt als Verbraucher erworben haben, so sei klargestellt, dass Ihre gesetzlichen Rechte hiervon unberührt bleiben.

Leistungsumfang der eingeschränkten Garantie

Bei Auftreten eines Produktfehlers besteht die einzige Verpflichtung von D-LINK darin, dem ursprünglichen Käufer das defekte Produkt kostenlos zu reparieren oder es auszutauschen. Voraussetzung hierfür ist, dass das Produkt während der Garantielaufzeit einem autorisierten D-LINK-Servicecenter übergeben wird. Reparatur oder Austausch werden von D-LINK durch ein autorisiertes D-LINK-Servicecenter durchgeführt. Bauteile oder Hardware-Produkte, die gemäß dieser eingeschränkten Garantie entfernt werden, gehen in das Eigentum von D-LINK über. Die verbliebene eingeschränkte Garantie des entfernten Teils oder Produkts wird auf das Ersatzteil oder -produkt übertragen.

Das Austauschprodukt muss weder neu sein noch dem defekten Produkt ganz oder in Teilen entsprechen. D-LINK darf dieses nach eigenem Ermessen gegen ein entsprechendes wiederaufbereitetes Produkt austauschen, welches dem defekten Produkt im Wesentlichen entspricht (oder höherwertig ist). D-LINK kann verlangen, dass der Kauf des Produkts nachgewiesen wird.

DIE VORSTEHENDE GARANTIE WURDE IN DIE DEUTSCHE SPRACHE AUS DEM ENGLISCHEN ÜBERSETZT. BEI ABWEICHUNGEN ZWISCHEN DER ENGLISCHEN VERSION UND DER DEUTSCHEN ÜBERSETZUNG GELTEN DIE BESTIMMUNGEN DER ENGLISCHEN VERSION.

Garantiegeber

D-Link (Europe) Ltd.
4th Floor, Merit House
Edgware Road
Colindale
London NW9 5 AB
Vereinigtes Königreich

Telefon: +44-020-8731-5555

Fax: +44-020-8731-5511
www.dlink.com

D-Link Europe a limité la garantie des produits

Conditions Générales

La Garantie Produit Limitée énoncée ci-dessous émane de D-LINK (Europe) Ltd. (ci-après « D-LINK »). Cette Garantie Produit Limitée n'est valable que sur présentation de la preuve d'achat. D-LINK peut également exiger la présentation du présent bon de garantie.

SAUF INDICATION EXPLICITE DES PRESENTES, D-LINK NE FOURNIT AUCUNE AUTRE GARANTIE, EXPLICITE OU IMPLICITE, Y COMPRIS UNE GARANTIE IMPLICITE DE VALEUR MARCHANDE OU D'ADAPTATION DU PRODUIT A UN USAGE PRECIS. D-LINK DECLINE EXPLICITEMENT TOUTE GARANTIE NON ENONCEE DANS LES PRESENTES. TOUTE GARANTIE IMPLICITE IMPOSEE PAR LA LOI, LE CAS ECHEANT, EST LIMITEE DANS SA DUREE A CELLE DE LA GARANTIE LIMITEE. CERTAINS ETATS OU PAYS NE PERMETTENT PAS DE LIMITER LA DUREE DE LA GARANTIE IMPLICITE OU INTERDISENT D'EXCLURE OU DE LIMITER LA COUVERTURE DES DOMMAGES DIRECTS OU INDIRECTS OCCASIONNES AUX PRODUITS GRAND PUBLIC. DANS LES ETATS OU PAYS EN QUESTION, CERTAINES EXCLUSIONS OU LIMITATIONS DE LA PRESENTE GARANTIE PEUVENT NE PAS S'APPLIQUER A VOTRE CAS. LA PRESENTE GARANTIE LIMITEE VOUS OCTROIE CERTAINS DROITS LEGAUX SPECIFIQUES. VOUS POUVEZ EGALEMENT BENEFICIER D'AUTRES DROITS VARIABLES D'UN ETAT OU D'UN PAYS A L'AUTRE. NOUS VOUS RECOMMANDONS DE CONSULTER LA LEGISLATION EN VIGUEUR DANS VOTRE LIEU DE RESIDENCE POUR CONNAITRE L'ETENDUE DE VOS DROITS.

La présente garantie limitée s'applique aux produits matériels commercialisés sous la marque D-LINK (collectivement ici « les Produits Matériels D-LINK) vendus par D-LINK (Europe) Ltd., ses filiales, sociétés affiliées, revendeurs agréés ou distributeurs locaux à travers le monde (collectivement ici « D-LINK ») avec la présente garantie limitée. Le terme de « Produit Matériel D-LINK » se limite aux composants matériels et à l'ensemble de leurs composants internes, notamment le firmware. Le terme de « Produit Matériel D-LINK » N'englobe PAS les applications ou programmes logiciels.

Etendue géographique de la Garantie Produit Limitée

La présente Garantie Produit Limitée s'applique à tous les pays européens figurant dans l'annexe « Pays européens où s'applique la Garantie Produit Limitée D-LINK ». Le terme de « pays européens » utilisé dans la présente Garantie Produit Limitée D-LINK englobe uniquement les pays figurant dans la liste en annexe. La Garantie Produit Limitée sera honorée dans tout pays où D-LINK ou ses prestataires agréés proposent le service de garantie, sous réserve des modalités énoncées dans la présente Garantie Produit Limitée. Cependant, la disponibilité du service de garantie et les temps de réponse varient d'un pays à l'autre et peuvent également être assujettis à un enregistrement.

Limitation de la Garantie Produit

D-LINK garantit que les produits décrits ci-dessous, dans le cadre d'une utilisation normale, sont dénués de défauts conséquents, tant au niveau de leurs composants matériels que de leur fabrication, et ce pendant toute la Période de Garantie Produit Limitée indiquée ci-dessous (« Période de Garantie Produit Limitée »), sous réserve qu'ils soient utilisés et entretenus conformément au manuel utilisateur et aux autres documents remis au client lors de l'achat (ou amendés de temps à autre). D-LINK ne garantit pas le fonctionnement ininterrompu ou sans erreur de ses produits. D-LINK ne s'engage pas non plus à corriger tous les défauts, erreurs ou non conformités.

La présente garantie ne s'applique pas aux problèmes qui sont la conséquence : (a) d'altérations ou d'ajouts non autorisés ; (b) d'une négligence, d'un abus ou d'une mauvaise utilisation, notamment une utilisation du produit non conforme à ses spécifications ou aux interfaces requises ; (c) d'une mauvaise manipulation ; (d) d'une panne de biens ou de services acquis auprès d'une société tierce (non D-LINK) ou qui ne font pas l'objet d'un contrat D-LINK de garantie ou de maintenance en bonne et due forme ; (e) d'une mauvaise utilisation ou d'un rangement dans des conditions inadaptées ; ou (f) du feu, de l'eau, d'une catastrophe naturelle ou autre. La présente garantie ne s'applique pas non plus à un produit dont le numéro de série D-LINK aurait été retiré ou altéré de quelque manière que ce soit.

D-LINK N'EST NULLEMENT RESPONSABLE DE DOMMAGES RESULTANT DE VOTRE INOBSERVATION DES INSTRUCTIONS FOURNIES POUR L'UTILISATION DE SON PRODUIT MATERIEL.

Période de Garantie Produit Limitée

La Période de Garantie Produit Limitée court à compter de la date d'achat auprès de D-LINK. La date de votre reçu ou bon de livraison correspond à la date d'achat du produit et constitue la date de votre preuve d'achat. Il est possible que le service de garantie ne vous soit accordé que sur production de votre preuve d'achat. Vous avez droit à un service de garantie conforme aux modalités énoncées dans les présentes dès lorsque que votre matériel de marque D-LINK nécessite une réparation pendant la Période de Garantie Produit Limitée.

La présente Garantie Produit Limitée s'applique uniquement à l'acheteur utilisateur final initial du Produit Matériel D-LINK. Elle est non cessible à quiconque se procure le Produit Matériel D-LINK auprès de l'acheteur utilisateur final initial.

Type de produit	Période de Garantie
Switches gérés (switches comportant un agent SNMP intégré)(y compris modules et logiciels de gestion)	Cinq (5) ans
Tous autres produits	Deux (2) ans
Pièces détachées (adaptateurs d'alimentation externes, ventilateurs)	Un (1) an

Les périodes de garantie indiquées ci-dessus s'appliquent à tous les produits D-LINK vendus depuis le 1er janvier 2004 dans les pays européens par D-LINK ou l'un de ses revendeurs ou distributeurs agréés. Tous les produits vendus avant le 1er janvier 2004 dans les pays européens par D-LINK ou l'un de ses revendeurs ou distributeurs agréés bénéficient d'une garantie de 5 ans, excepté les fournitures électriques, ventilateurs et accessoires, qui sont couverts par une garantie de 2 ans.

La période de garantie indiquée sur ce bon annule et remplace celle qui figure dans le manuel utilisateur ou dans le contrat d'achat des produits considérés. Pour éviter le doute, si vous avez acheté votre produit D-LINK en tant que consommateur, vos droits légaux demeurent inchangés.

Exécution de la Garantie Produit Limitée

En cas de défaut ou d'erreur d'un produit, l'unique obligation de D-LINK se limite à la réparation ou au remplacement gratuit du produit défectueux, au bénéfice de l'acheteur initial, sous réserve que le produit soit rapporté à un Centre de Service Agréé D-LINK pendant la période de garantie. D-LINK assure la réparation ou le remplacement dans un Centre de Service Agréé D-LINK. Les composants, pièces ou produits retirés dans le cadre de cette garantie limitée deviennent propriété de D-LINK. La pièce ou le produit de remplacement est couvert par la garantie limitée de la pièce ou du produit d'origine pendant la période restante. Le produit de remplacement n'est pas nécessairement neuf, ni d'une marque ou d'un modèle identique ; D-LINK peut décider, de manière discrétionnaire, de remplacer le produit défectueux (ou ses pièces) par un équivalent (ou un article supérieur) reconditionné ayant toutes les fonctionnalités du produit défectueux. D-LINK peut exiger la preuve d'achat.

Garant

D-Link (Europe) Ltd.
4th Floor, Merit House
Edgware Road
Colindale
London NW9 5 AB
Royaume-Uni
Tél : +44-020-8731-5555
Fax : +44-020-8731-5511
www.dlink.co.uk

Garantí a limitada del producto D-LINK Europa

Condiciones generales

Esta garantí a la ofrece D-LINK (Europe) Ltd. (en este documento, "D-LINK"). La garantí a limitada del producto sólo es válida si se acompaña del comprobante de la compra. También deberá presentarse la tarjeta de garantí a si D-LINK lo solicita.

EXCEPTO EN LO EXPRESAMENTE INDICADO EN ESTA GARANTÍ A LIMITADA, D-LINK NO CONCEDE OTRAS GARANTÍ AS, NI EXPLÍ CITAS NI IMPLÍ CITAS, INCLUIDAS LAS GARANTÍ AS IMPLÍ CITAS DE COMERCIALIDAD Y APTITUD A UN FIN DETERMINADO. D-LINK RECHAZA EXPLÍ CITAMENTE CUALQUIER GARANTÍ A QUE NO FIGURE EN ESTA GARANTÍ A LIMITADA. LA DURACIÓN DE CUALQUIER GARANTÍ A IMPLÍ CITA QUE PUEDA SER IMPUESTA POR LEY QUEDA LIMITADA AL PERÍ ODO DE LA GARANTÍ A LIMITADA. ALGUNOS ESTADOS O PAÍ SES NO PERMITEN QUE EN LA GARANTÍ A LIMITADA DE PRODUCTOS DE CONSUMO SE RESTRINJA LA DURACIÓN TEMPORAL, NI QUE SE EXCLUYAN O LIMITEN LOS DAÑOS INCIDENTALES O RESULTANTES PARA EL CONSUMIDOR DE LOS PRODUCTOS. EN ESTOS ESTADOS O PAÍ SES, A USTED NO LE PUEDEN APLICAR ALGUNAS EXCLUSIONES O LIMITACIONES DE LA GARANTÍ A LIMITADA. ESTA GARANTÍ A LIMITADA LE CONCEDE DETERMINADOS DERECHOS. PUEDE, TAMBIÉN, TENER OTROS DERECHOS, QUE PUEDEN SER DISTINTOS DE UN ESTADO A OTRO O DE UN PAÍ S A OTRO. SE RECOMIENDA QUE CONSULTE LAS LEYES PERTINENTES DE UN ESTADO O PAÍ S A FIN DE QUE CONOZCA SUS DERECHOS.

Esta garantí a limitada se aplica a los productos de hardware de la marca D-LINK (llamados en esta guí a "Productos de hardware D-LINK") comprados a D-LINK (Europe) Ltd., a sus filiales en el mundo, a sus proveedores autorizados o a sus distribuidores locales (llamados en este documento "D-LINK") con esta garantí a limitada. El término "producto de hardware D-LINK" se restringe a los componentes de hardware y a los componentes internos de estos, incluyendo el firmware. El término "producto de hardware D-LINK" NO incluye ni las aplicaciones ni los programas de software.

Cobertura geográfica de la garantí a limitada del producto

Esta garantí a limitada del producto es válida en todos los paí ses europeos que figuran en el apéndice "Paí ses europeos de la garantí a limitada del producto D-LINK". En esta garantí a limitada del producto D-Link, el término "paí ses europeos" sólo incluye los paí ses que figuran en el apéndice. La garantí a limitada del producto será válida en cualquier paí s en el que D-LINK o sus proveedores autorizados de servicios ofrezcan un servicio de garantí a sujeto a los términos y condiciones recogidos en esta garantí a limitada del producto. Sin embargo, la disponibilidad del servicio de garantí a, así como el tiempo de respuesta, pueden variar de un paí s a otro y pueden estar sujetos a requisitos de registro.

Limitación de la garantí a del producto

D-LINK garantiza que los productos descritos más adelante están libres de defectos de fabricación y materiales, en condiciones normales de uso, a lo largo del perí odo de la garantí a limitada del producto que se indica en este documento ("perí odo de la garantí a limitada del producto"), si el producto se ha utilizado y mantenido conforme a lo recogido en el manual del usuario o en otra documentación que se haya proporcionado al comprador en el momento de la compra (o que se haya corregido). D-LINK no garantiza que los productos funcionarán sin interrupciones o sin errores, ni que se corregirán todas las deficiencias, errores, defectos o disconformidades.

Esta garantí a no cubre problemas derivados de: (a) modificaciones o conexiones no autorizadas; (b) negligencia, abuso o mal uso, incluyendo el incumplimiento de las especificaciones y de los requisitos de la interfaz en el funcionamiento del producto; (c) manejo incorrecto; (d) errores en artí culos o servicios ajenos a D-LINK o no sujetos a una garantí a o un contrato de mantenimiento vigentes de D-LINK; (e) uso o almacenamiento incorrecto; o (f) fuego, agua, casos fortuitos u otros hechos catastróficos. Esta garantí a tampoco es válida para aquellos productos a los que se haya eliminado o alterado de algún modo el número de serie D-LINK.

D-LINK NO SE RESPONSABILIZA DE LOS DAÑOS CAUSADOS COMO CONSECUENCIA DEL INCUMPLIMIENTO DE LAS INSTRUCCIONES DEL PRODUCTO DE HARDWARE D-LINK.

Perí odo de la garantí a limitada del producto

El perí odo de la garantí a limitada del producto se inicia en la fecha en que se realizó la compra a D-LINK. Para el comprador, el comprobante de la fecha de la compra es el recibo de la venta o de la entrega, en el que figura la fecha de la compra del producto. Puede ser necesario tener que presentar el comprobante de la compra a fin de que se preste el servicio de garantí a. El comprador tiene derecho al servicio de garantí a conforme a los términos y condiciones de este documento, si requiere una reparación del hardware de la marca D-LINK dentro del perí odo de garantí a limitada del producto.

Esta garantí a limitada del producto cubre sólo al originario comprador-usuario final de este producto de hardware D-LINK, y no es transferible a otras personas que reciban el producto de hardware D-LINK del originario comprador-usuario final.

Tipo de producto	Perí odo de garantí a del producto
Conmutadores gestionados (p. ej., conmutadores con agente SNMP integrado) (incluyendo módulos y software de gestión)	Cinco (5) años
Resto de productos	Dos (2) años
Piezas de repuesto (p. ej., adaptadores de alimentación externos, ventiladores)	Un (1) año

Estos perí odos de garantí a están en vigor para todos los productos D-LINK que hayan sido comprados en paí ses europeos a D-LINK o a alguno de sus proveedores o distribuidores autorizados a partir del 1 de enero del 2004. Todos los productos comprados en paí ses europeos a D-LINK o a uno de sus proveedores o distribuidores autorizados antes del 1 de enero del 2004 cuentan con 5 años de garantí a, excepto las fuentes de alimentación, los ventiladores y los accesorios, que cuentan con 2 años de garantí a.

El perí odo de garantí a que figura en esta tarjeta sustituye y reemplaza al perí odo de garantí a que consta en el manual del usuario o en el contrato de compra de los productos correspondientes. Para evitar dudas: si usted ha comprado el producto D-LINK correspondiente como consumidor, sus derechos legales no se ven afectados.

Uso de la garantí a limitada del producto

Si un producto presenta algún defecto, la obligación exclusiva de D-LINK será reparar o reemplazar, sin coste alguno para el comprador originario, cualquier producto defectuoso siempre y cuando éste sea entregado en un centro autorizado de servicio D-LINK durante el perí odo de garantí a. D-LINK realizará la reparación o sustitución para un centro autorizado de servicio D-LINK. Todos los productos de hardware o componentes que se eliminen bajo esta garantí a limitada serán propiedad de D-LINK. La parte o el producto de repuesto adquiere, para el resto de la garantí a limitada, el estatus de parte o producto eliminado. El producto de repuesto no ha de ser nuevo o de la misma marca, modelo o parte; D-LINK puede sustituir a discreción el producto defectuoso (o cualquier parte) con un producto equivalente reacondicionado (o superior) en cualquier material respecto al producto defectuoso. D-LINK puede pedir el comprobante de compra.

Garante

D-Link (Europe) Ltd.
4th Floor, Merit House
Edgware Road
Colindale
London NW9 5 AB
United Kingdom
Teléfono: +44-020-8731-5555
Fax: +44-020-8731-5511
www.dlink.co.uk

D-Link Europe Termini di Garanzia dei Prodotti

Generalità

La presente Garanzia viene fornita da D-LINK (Europe) Ltd. (di seguito denominata "D-LINK"). Essa viene riconosciuta solo se accompagnata dalla prova di acquisto. D-LINK può richiedere anche l' esibizione della presente cartolina di garanzia.
SALVO QUANTO ESPRESSAMENTE STABILITO NELLA PRESENTE GARANZIA LIMITATA, D-LINK NON FORNISCE NESSUN' ALTRA GARANZIA NE' ESPRESSA NE' IMPLICITA, COMPRESE EVENTUALI GARANZIE DI COMMERCIABILITÀO DI IDONEITÀPER UN PARTICOLARE SCOPO. D-LINK NEGA ESPRESSAMENTE QUALUNQUE ALTRA GARANZIA CHE NON RIENTRI NELLA PRESENTE GARANZIA LIMITATA. QUALSIASI GARANZIA IMPLICITÀ, CHE DOVESSE ESSERE IMPOSTA PER LEGGE, SARÀCIRCOSCRITTA ALLA DURATA DELLA PRESENTE GARANZIA. ALCUNI PAESI VIETANO QUALSIASI LIMITAZIONE DEL PERIODO DI VALIDITÀDELLE GARANZIE IMPLICITE OPPURE L' ESCLUSIONE O LA LIMITAZIONE DEI DANNI INCIDENTALI O CONSEQUENZIALI PER I PRODOTTI. IN TALI PAESI, EVENTUALI ESCLUSIONI O LIMITAZIONI DELLA PRESENTE GARANZIA NON POTRANNO APPLICARSI AL VOSTRO CASO. LA PRESENTE GARANZIA VI CONFERISCE DIRITTI LEGALI SPECIFICI. INOLTRE POTRETE GODERE DI ULTERIORI DIRITTI CHE POSSONO VARIARE A SECONDA DEL PAESE. SIETE INVITATI A CONSULTARE LE LEGGI APPLICABILI DEL VOSTRO PAESE AL FINE DI DETERMINARE CON PRECISIONE I VOSTRI DIRITTI.
La presente garanzia trova applicazione su tutti i prodotti hardware recanti il marchio D-LINK (di seguito denominati collettivamente "Prodotti hardware D-LINK") venduti da D-LINK (Europe) Ltd., dalle sue controllate, dalle sue affiliate, dai rivenditori autorizzati o dai distributori nazionali (di seguito denominati collettivamente "D-LINK"), accompagnati dalla presente garanzia limitata. Il termine "Prodotto hardware D-LINK" si riferisce esclusivamente ai componenti hardware e a tutte le parti interne compreso il firmware. Il termine "Prodotto hardware D-LINK" NON comprende eventuali applicazioni o programmi software.

Ambito geografico della Garanzia limitata

La presente Garanzia è estesa a tutti i Paesi europei elencati nell' appendice "Paesi europei - Garanzia limitata dei prodotti D-LINK". Il termine "Paesi europei" si riferisce esclusivamente ai paesi nominati in questa appendice. La Garanzia verrà riconosciuta in tutti i paesi nei quali D-LINK o i suoi Centri di Assistenza autorizzati offrono assistenza conformemente alle condizioni e ai termini stabiliti nella presente Garanzia. Tuttavia, la disponibilità all' assistenza e i tempi di intervento variano da paese a paese e possono essere soggetti a eventuali requisiti di registrazione.

Limitazione della Garanzia

D-LINK garantisce che i prodotti sotto descritti in condizioni di normale utilizzo non presentano difetti di fabbricazione o vizi di materiale durante il Periodo di garanzia sotto specificato ("Periodo di garanzia"), a condizione che vengano utilizzati e sottoposti a manutenzione in conformità con il manuale d' uso e con ogni altra documentazione fornita all' acquirente all' atto dell' acquisto (e relativi emendamenti). D-LINK non garantisce che il funzionamento del prodotto sarà ininterrotto o esente da errori né tanto meno che tutti gli eventuali errori, carenze, difetti o non conformità potranno essere corretti.
La presente garanzia non copre eventuali problemi derivanti da: (a) alterazioni o aggiunte non autorizzate; (b) negligenza, abuso o utilizzo improprio, compresa l' incapacità di far funzionare il prodotto in conformità con le specifiche e i requisiti di connessione; (c) movimentazione impropria; (d) guasto di prodotti o servizi non forniti da D-LINK o non soggetti a una garanzia successiva di D-LINK o a un accordo di manutenzione; (e) impiego o conservazione impropri; (f) incendio, inondazione, cause di forza maggiore o altro evento catastrofico accidentale. La presente garanzia non si applica altresì ad alcun prodotto particolare qualora il numero di serie di D-LINK sia stato rimosso o reso illeggibile in altro modo.
D-LINK DECLINA OGNI RESPONSABILITÀPER EVENTUALI DANNI RISULTANTI DAL MANCATO RISPETTO DELLE ISTRUZIONI RELATIVE AL PRODOTTO HARDWARE D-LINK.

Periodo di garanzia

Il Periodo di garanzia ha decorrenza dalla data dell' acquisto presso D-LINK. Prova della data di acquisto è il documento fiscale (scontrino fiscale o ricevuta) recante la data di acquisto del prodotto. Per avere diritto alla garanzia può esserVi richiesto di esibire la prova di acquisto. Potete beneficiare delle prestazioni di assistenza previste dalla garanzia in conformità con i termini e le condizioni di cui sotto nel momento in cui il Vostro prodotto hardware D-LINK necessiti di una riparazione durante il Periodo di garanzia.
La presente Garanzia si applica esclusivamente al primo acquirente del Prodotto hardware D-LINK e non può essere trasferita a terzi che abbiano ottenuto la proprietà del Prodotto hardware D-LINK dal primo acquirente.

Tipo di prodotto	Periodo di garanzia
Switch (solo switch dotati di agente SNMP incorporato) (inclusi moduli e software di gestione)	5 (cinque) anni
Tutti gli altri prodotti	2 (due) anni
Pezzi di ricambio (es. adattatori esterni di potenza, alimentatori esterni, ventole)	1 (un) anno

Il periodo di garanzia sopra specificato relativamente a tutti i prodotti D-LINK venduti nei Paesi europei da D-LINK o da qualsiasi suo rivenditore o distributore autorizzato decorre dal 1° gennaio 2004. Tutti i prodotti venduti nei Paesi europei da D-LINK o da uno qualsiasi dei suoi rivenditori o distributori autorizzati prima del 1° gennaio 2004 sono coperti da una garanzia di 5 anni fatto salvo per alimentatori, ventole e accessori che hanno 2 anni di garanzia.

Il periodo di garanzia qui menzionato sostituisce qualsiasi altro periodo di garanzia definito nel manuale d' uso o nel contratto di acquisto del prodotto. Se avete acquistato un prodotto D-LINK in qualità di consumatore i Vostri diritti rimangono invariati.

Prestazioni della Garanzia limitata

Qualora comparisse un difetto o una non conformità, D-LINK avrà l' unico obbligo di riparare o sostituire il prodotto non conforme senza alcun costo per l' acquirente a condizione che il prodotto venga restituito a un Centro di Assistenza autorizzato D-LINK entro il periodo di garanzia. La riparazione o la sostituzione verranno eseguite da D-LINK presso un Centro di Assistenza autorizzato D-LINK. Tutti i componenti o i prodotti hardware rimossi conformemente ai termini e alle condizioni della presente garanzia divengono di proprietà di D-LINK. Il pezzo o il prodotto in sostituzione beneficerà della garanzia per il tempo residuo della parte o del prodotto originale. Il prodotto in sostituzione non deve necessariamente essere nuovo o di identica fattura, modello o composizione; D-LINK può a sua discrezione sostituire il prodotto non conforme (o qualsiasi parte di esso) con un prodotto che risulti essere equivalente (o di valore superiore) al prodotto non conforme. D-LINK può richiedere che venga esibita la prova di acquisto.

Garante
D-Link (Europe) Ltd.
4th Floor, Merit House
Edgware Road
Colindale
Londra NW9 5 AB
Regno Unito
Telefono: +44-020-8731-5555
Fax: +44-020-8731-5511
www.dlink.co.uk

International Offices

U.S.A
17595 Mt. Herrmann Street
Fountain Valley, CA. 92708
TEL: 714-885-6000
Fax 866-743-4905
URL: www.dlink.com

Canada
2180 Winston Park Drive
Oakville, Ontario, L6H 5W1
Canada
TEL: 1-905-8295033
FAX: 1-905-8295223
URL: www.dlink.ca

Europe (U. K.)
4th Floor, Merit House
Edgware Road, Colindale
London NW9 5AB
U.K.
TEL: 44-20-8731-5555
FAX: 44-20-8731-5511
URL: www.dlink.co.uk

Germany
Schwalbacher Strasse 74
D-65760 Eschborn
Germany
TEL: 49-6196-77990
FAX: 49-6196-7799300
URL: www.dlink.de

France
Le Florilege #.2, Allee de la Fresnerie
78330 Fontenay le Fleury
France
TEL: 33-1-30238688
FAX: 33-1-30238689
URL: www.dlink-france.fr

Netherlands
Weena 290
3012 NJ Rotterdam
Netherlands
Tel: +31-10-282-1445
Fax: +31-10-282-1331
URL: www.dlink-benelux.com

Belgium
Rue des Colonies 11
B-1000 Brussels
Belgium
Tel: +32(0)2 517 7111
Fax: +32(0)2 517 6500
URL: www.dlink-benelux.com

Italy
Via Nino Bonnet n. 6/b
20154 – Milano,
Italy
TEL: 39-02-2900-0676
FAX: 39-02-2900-1723
URL: www.dlink.it

Sweden
P.O. Box 15036, S-167 15 Bromma
Sweden
TEL: 46-(0)8564-61900
FAX: 46-(0)8564-61901
URL: www.dlink.se

Denmark
Naverland 2, DK-2600
Glostrup, Copenhagen,
TEL: 45-43-969040
FAX: 45-43-424347
URL:www.dlink.dk

Norway
Karihaugveien 89
1086 Oslo
Norway
TEL: 47-23-897189
FAX: 47-22-309085
URL: www.dlink.no

Finland
Pakkalankuja 7A
01510 Vantaa,
Finland
TEL : +358-9-2707 5080
FAX: + 358-9-2707 5081
URL: www.dlink.fi

Iberia
C/Sabino De Arana,
56 Bajos
08028 Barcelona
TEL: 34 93 4090770
FAX: 34 93 4910795
URL: www.dlinkiberia.es

Singapore
1 International Business Park
#03-12 The Synergy
Singapore 609917
TEL: 65-6774-6233
FAX: 65-6774-6322
URL: www.dlink-intl.com

Australia
1 Giffnock Avenue,
North Ryde, NSW 2113
Australia
TEL: 61-2-8899-1800
FAX: 61-2-8899-1868
URL: www.dlink.com.au

India
D-Link House, Kurla Bandra Complex Road,
Off CST Road, Santacruz (East), Mumbai - 400098.
India
TEL: 91-022-26526696/56902210
FAX: 91-022-26528914
URL: www.dlink.co.in

Middle East (Dubai)
P.O.Box: 500376
Office No.:103, Building:3
Dubai Internet City
Dubai, United Arab Emirates
Tel:+971-4-3916480
Fax:+971-4-3908881
URL: www.dlink-me.com

Turkey
Maslak Ayazaga Yolu
No: 2 Kat :5
Ayazaga-Istanbul
TURKEY
TEL: 0090 212 289 56 59
FAX: 0090 212 289 76 06
URL: www.dlink.com.tr

Egypt
19 El-Shahed Helmy, El Masri
Al-Maza, Heliopolis
Cairo,Egypt.
TEL:+202 414 4295
FAX:+202 415 6704
URL: www.dlink-me.com

Israel
11 Hamanofim Street
Ackerstein Towers, Regus Business Center
P.O.B 2148, Hertzelia-Pituach 46120.
Israel
TEL: +972-9-9715700
FAX: +972-9-9715601
URL: www.dlink.co.il

Latin America
Isidora Goyeechea 2934 of 702,
Las Condes
Santiago – Chile S.A.
TEL: 56-2-232-3185
FAX: 56-2-232-0923
URL: www.dlink.cl

Brasil
Av das Nacoes Unidas,
11857 - 14 - andar - cj 141/142
Brooklin Novo
Sao Paulo - SP - Brazil
CEP 04578-000
TEL: +55 11 55039320
FAX: +55 11 55039322
URL: www.dlinkbrasil.com.br

South Africa
Einstein Park II
Block B
102-106 Witch-Hazel Avenue
Highveld Technopark
Centurion
Gauteng
Republic of South Africa
TEL: 27-12-665-2165
FAX: 27-12-665-2186
URL: www..d-link.co.za

Russia
Grafsky per., 14, floor 6
Moscow
129626 Russia
TEL: 7-095-744-0099
FAX: 7-095-744-0099 #350
URL: www.dlink.ru

China
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
2F, No. 119, Pao-Chung Rd.
Hsin-Tien, Taipei
Taiwan
TEL: 886-2-2910-2626
FAX: 886-2-2910-1515
URL: www.dlinktw.com.tw

Headquarters
2F, No. 233-2, Pao-Chiao Rd.
Hsin-Tien, Taipei
Taiwan
TEL: 886-2-2916-1600
FAX: 886-2-2914-6299
URL:www.dlink.com

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 (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)
Product was purchased from:

Reseller's name:_____

Telephone:_____ Fax:_____

Reseller's full address:_____
_____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?
   □Home □Office □Travel □Company Business □Home Business □Personal Use

2. How many employees work at installation site?
   □1 employee □2-9 □10-49 □50-99 □100-499 □500-999 □1000 or more

3. What network protocol(s) does your organization use ?
   □XNS/IPX □TCP/IP □DECnet □Others_____

4. What network operating system(s) does your organization use ?
   □D-Link LANsmart □Novell NetWare □NetWare Lite □SCO Unix/Xenix □PC NFS □3Com 3+Open
   □Banyan Vines □DECnet Pathwork □Windows NT □Windows 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? _____
_____
_____
_____

TO:

D-Link®