DES-3350SR

Standalone Layer 3 Switch

User's Guide

First Edition (July 2003)

651SR3350015

Printed In Taiwan

RECYCLABLE

D-Link Offices for Registration and Warranty Service

The product's Registration Card, provided at the back of this manual, must be sent to a D-Link office. To obtain an RMA number for warranty service as to a hardware product, or to obtain warranty service as to a software product, contact the D-Link office nearest you. An address/telephone/fax/e-mail/Web site list of D-Link offices is provided in the back of this manual.

For D-Link product users in the United States, registration is also available via the Website of D-Link USA.

Trademarks

Copyright Statement

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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.

VCCI Warning

注意
この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づく第一種情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Table of Contents

1

INTRODUCTION

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

Features

The DES-3350SR Switch was designed for easy installation and high performance in an environment where traffic on the network and the number of users increase continuously.

Switch features include:

Ports

- Forty-eight high-performance NWay ports all operating at 10/100 Mbps for connecting to end stations, servers and hubs. All 48 10/100 UTP ports can auto-negotiate (NWay) between 10Mbps/100Mbps, half-duplex or full duplex.

- One front panel slide-in module interface for a 2-port 1000BASE-T module (provided) and one front panel slide-in module interface for a 2-port Mini GBIC Gigabit Ethernet module (optional). Each Gigabit port supports both operation modes but they cannot be used simultaneously. So if port 50x is used on the Mini GBIC module, port 49x is not available for the 1000BASE-T module, and vice versa.

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

Performance Features

Redundant Power Supply

The DES-3350SR can be equipped with a redundant power supply - the D-Link DPS-200 - to ensure continuation of service if the main power unit fails. An integrated detection circuit continuously monitors the internal power supply. In the event of a power interruption, the redundant power supply is immediately triggered so that the DES-3350SR and connected devices can continue providing service.

This results in a more reliable network infrastructure and protects a network from a single failure of a network device power supply.

The redundant power supply may be purchased with and included in the original system installation, or may be added to an existing system at a later time.

Layer 2 Features

- Store and forward switching scheme.

- Full and half-duplex for both 10Mbps and 100Mbps connections. The front-port Gigabit Ethernet module operates at full duplex only. Full duplex allows the switch port to simultaneously transmit and receive data, and only works with connections to full-duplex capable end stations and switches. Connections to hubs must take place at half-duplex.
- Auto-polarity detection and correction of incorrect polarity on the transmit and receive twisted-pair at each port.
- IEEE 802.3z compliant for Mini GBIC ports (optional module).
- IEEE 802.3ab compliant for 1000BASE-T (Copper) Gigabit ports (optional module).
- Data forwarding rate 14,880 pps per port at 100% of wire-speed for 10Mbps speed.
- Data forwarding rate 148,800 pps per port at 100% of wire-speed for 100Mbps speed.
- Data filtering rate eliminates all error packets, runts, etc. at 14,880 pps per port at 100% of wire-speed for 10Mbps speed.
- Data filtering rate eliminates all error packets, runts, etc. at 148,800 pps per port at 100% of wire-speed for 100Mbps speed.
- 8K active MAC address entry table per device with automatic learning and aging (10 to 1,000,000 seconds).
- 64 MB packet buffer per device.
- Supports Port Mirroring.

- Supports Port Trunking.
- 802.1w Rapid Spanning Tree support.
- 802.1Q Tagged VLAN support – up to 255 VLANs per device (one VLAN is reserved for internal use).
- GVRP – (GARP VLAN Registration Protocol) support for dynamic VLAN registration.
- 802.1p Priority support with four priority queues.
- IGMP Snooping support.

Layer 3 Switch Features

- Wire speed IP forwarding.
- Hardware-based Layer 3 IP switching.
- IP packet forwarding rate of 6.6 Mpps.
- 2K active IP address entry table per device.
- Supports RIP – (Routing Information Protocol) version I and II.
- Supports OSPF – (Open Shortest Path First).
- Supports MD5 and Simple Password OSPF Packet Authentication.
- Supports IP version 4.
- IGMP version 1 and 2 support (RFC 1112 and RFC 2236).
- Supports PIM Dense Mode.

- Supports DVMRP.
- Supports IP packet de-fragmentation.

Traffic Classification and Prioritization

- Based on 802.1p priority bits.
- Four priority queues.

Management

- RS-232 console port for out-of-band network management via a console terminal or PC.
- Rapid Spanning Tree Algorithm Protocol for creation of alternative backup paths and prevention of network loops.
- SNMP V1, V2C, and V3 are supported.
- Fully configurable in-band control for SNMP based software.
- Flash memory for software upgrades. This can be done in-band via TFTP or out-of-band via the console.
- Built-in SNMP management:
    - MIB-II (RFC 1213).
    - MIB (RFC 1215).
    - Bridge MIB (RFC 1493).
    - RMON MIB (RFC 1757) – 4 groups. The RMON specification defines the Counters for the Receive

function only. However, the DES-3350SR implements counters for both receive and transmit functions.

- SNMP V2-MIB (RFC 1907).
- RMON2 (RFC 2021).
- IF MIB (RFC 2233).
- Ether-Like MIB (RFC 2358) – dot3StatsTable.
- 802.1p MIB (RFC 2674).
- Entity MIB (RFC 2737).
- SNMP-Framework (RFC 2571).
- SNMP-MPD (RFC-2572).
- SNMP-Target & SNMP-Notification (RFC 2573).
- SNMP-User-based SM (RFC 2574).
- SNMP-View-based ACM (RFC 2575).
- SNMP-Community (RFC 2576).
- RIPv2 (RFC 1724).
- OSPF (RFC 1850).
- IP-Forward (RFC 2906).
- IPM Route-STD (RFC 2932).
- IGMP-STD (RFC 2933).
- PIM (RFC 2934).
- DVMRP-MIB.

  - IEEE8021-PAE-MIB.
  - RSTP-MIB.
  - DLINK-Agent-MIB.
  - LAG-MIB.
  - DLINK-Time-MIB.
  - DLINK-Equipment-MIB.
  - DLINK-L2MGMT-MIB.
  - DLINK-L3MGMT-MIB.
  - ACL-MGMT-MIB.
- Supports Web-based management.
- CLI management support.
- TFTP support.
- BOOTP support.
- DHCP Client support.
- Password enabled.

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

2

UNPACKING AND SETUP

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 Standalone 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 3 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.

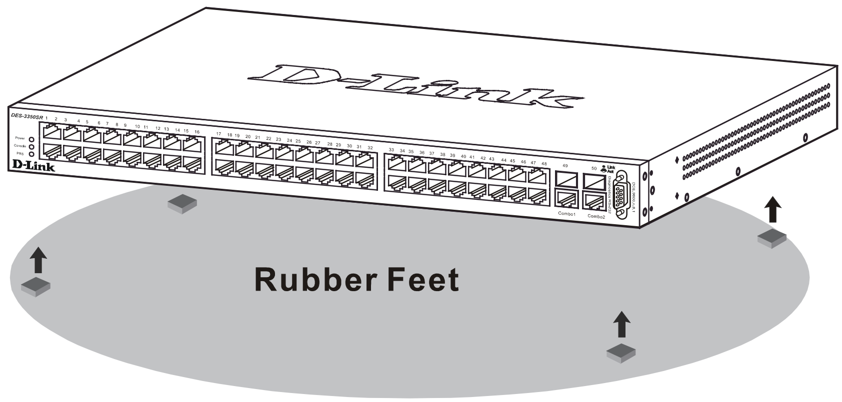


Figure 2-1. Installing rubber feet for desktop installation

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.

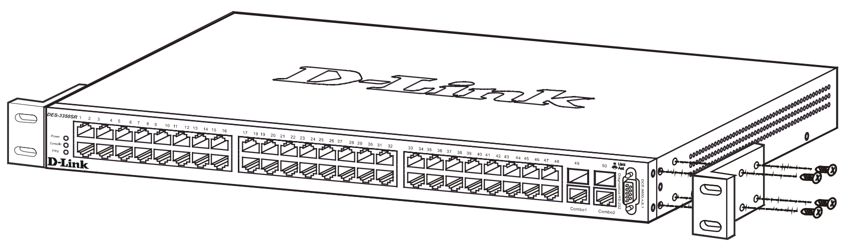


Figure 2-2. Attaching the mounting brackets to the switch

Then, use the screws provided with the equipment rack to mount the switch on the rack.

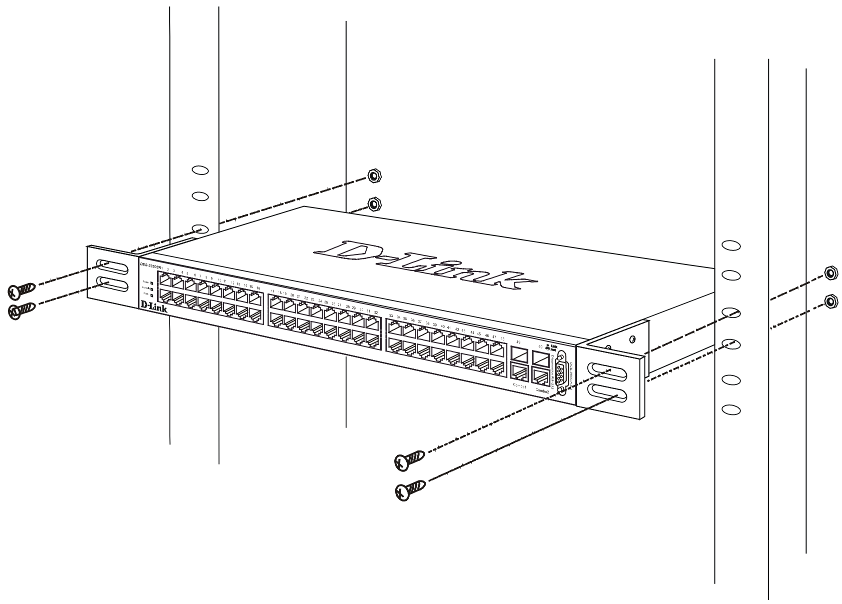


Figure 2-3.   Installing the switch on an equipment rack

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.

Redundant Power Supply

The DES-3350SR can be equipped with a redundant power supply - the D-Link DPS-200 - to ensure continuation of service in a failure of the main power unit. An integrated detection circuit continuously monitors the internal power supply. In the event of a power interruption, the redundant power supply is immediately triggered so that the DES-3350SR and connected devices can continue providing service.

The redundant power supply may be purchased with and included in the original system installation, or may be added to an existing system at a later time.

3

IDENTIFYING EXTERNAL COMPONENTS

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).

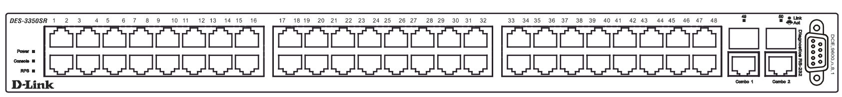


Figure 3-1. Front panel view of the Switch

- 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.

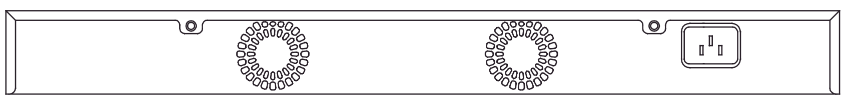


Figure 3-2. Rear panel view of the Switch

The 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.

Between the fan outlet and the power cord is the outlet for the redundant power supply. Using the DPS-200 14-pin DC power cable, connect the DES-3350SR to the DPS-200 redundant power supply. The redundant power supply ensures that service will not be interrupted in the event of an internal power supply failure.

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.

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 diagrams below to view the two Mini-GBIC port modules being plugged into the Switch.

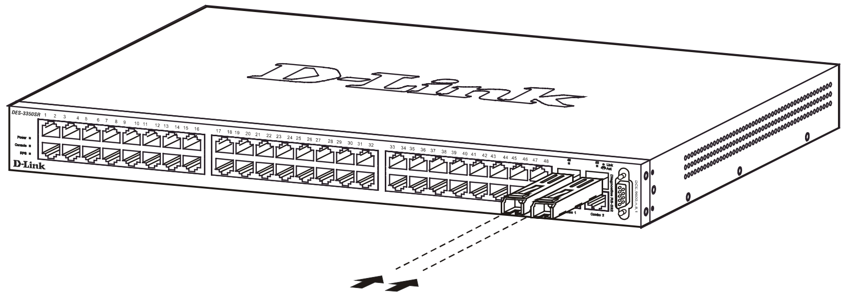


Figure 3-4. Step One: Plug the empty Mini-GBIC module outer casings into the upper slots for ports 49x and 50x

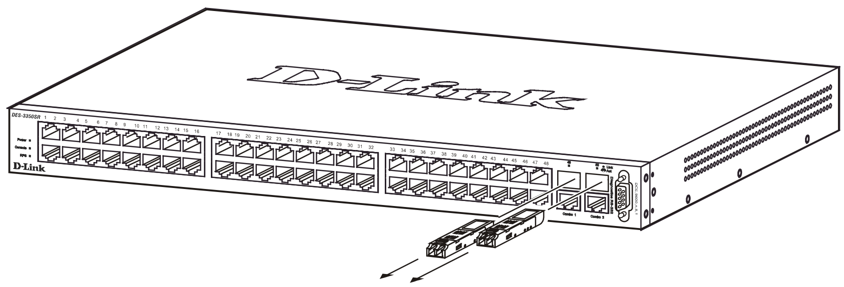


Figure 3-5. Step Two: Insert the Mini-GBIC modules into the upper slots above Combo 1 and Combo 2 on the Switch

Mini-GBIC Installation Instructions

Insert the Mini-GBIC module(s) into the empty Mini-GBIC slot(s) in the top row of the pair of ports for 49x and 50x. Make sure the modules are properly aligned with the slots, and that the electrical connectors on the rear of the modules face downward, for the two Mini-GBIC fiber optic module slots on top of the group of four. Make sure the electrical connectors on the Mini-GBIC fiber optic modules are facing upward for the two Mini-GBIC fiber optic module slots on the bottom of the group of four. The Mini-GBIC fiber optic module can only be installed one way, so if it does not fit, do not force it.

When the electrical contacts at the rear of the Mini-GBIC modules have seated against the contacts in the Mini-GBIC slot on the Switch, gently press the modules into the slot until you feel a slight click.

There are two methods of removing a Mini-GBIC module, depending upon the module type. One method requires moving a small lever from the top of the module down across the front where the fiber optic cable connections are, and then using this lever to gently pull the module out of the Mini-GBIC slot on the Switch. You cannot remove this type of module without first disconnecting the fiber optic cable from the module because the fiber optic cables block the movement of the lever.

Removing the other type of Mini-GBIC module requires using a small tool, such as a ballpoint pen, to press a small slider at the bottom of the front of the module, where the fiber optic cable connectors are. Pressing this slider forces it against the edge of the Mini-GBIC slot on the Switch, and will gently release the Mini-GBIC module from the slot.

The connector on the fiber optic cable must also be properly aligned. This connector can also be inserted only one way, so if it does not fit, do not force it.

The Mini-GBIC module fiber optic cable connectors have two small tabs, similar to the tabs on copper Cat 5 Ethernet cable or a telephone cable connector. This tab is used to retain the connector in the Mini-GBIC module so that it cannot be accidentally pulled out and the link lost.

To remove the Mini-GBIC module fiber optic cable connector from the Mini-GBIC module, press the retaining tabs on the fiber optic cable connectors down and gently pull the outer plastic casing back away from the Mini-GBIC module. Many Mini-GBIC fiber optic cables have their connectors grouped into pairs, with a small plastic tab that will press both connector tabs at the same time, so you can remove both cable connectors as a group.

Note: Each Gigabit port supports both operation modes but they cannot be used simultaneously. So if port 49x is used on the Mini GBIC module, port 50x is not available for the 1000BASE-T module, and vice versa.

LED Indicators

The LED indicators of the Switch include Power, Console, RPS in use, and Link/Act. The following shows the LED indicators for the Switch along with an explanation of each indicator.

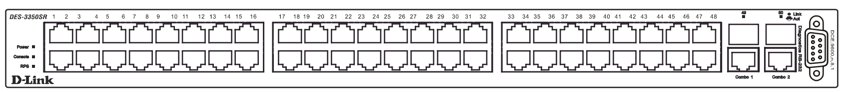


Figure 3-6. The LED Indicators

- **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.
- **RPS in use** – The bottom LED on the left-hand side of the switch, the Redundant Power Supply (RPS) indicator will show steady amber when in standby mode. When the RPS is triggered, the LED will show steady green.
- **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.

4

CONNECTING THE SWITCH

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 twisted-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.

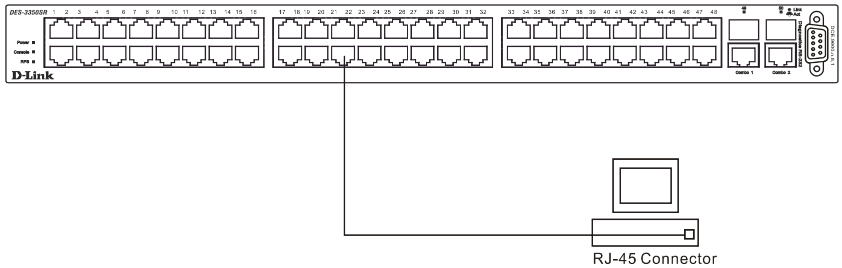


Figure 4-1. Switch connected to an End Node

- 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 twisted-pair Category 3, 4 or 5 UTP/STP cable.
- A 100BASE-TX hub or switch can be connected to the Switch via a twisted-pair Category 5 UTP/STP cable.

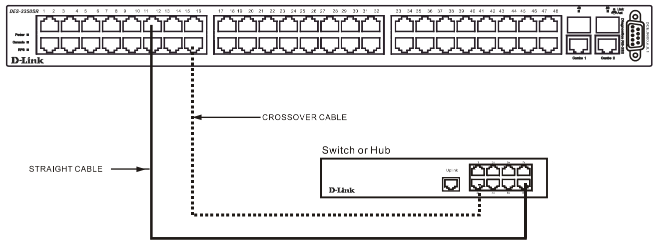


Figure 4-2. Switch connected to a port on a hub or switch using a straight or crossover cable

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*.

5

SWITCH MANAGEMENT AND OPERATING CONCEPTS

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. Further, this chapter explains many important points regarding these features.

Configuring the switch to implement these concepts and make use of its many features is discussed in detail in the next chapters.

Local Console Management

A local console is a terminal or a workstation running a terminal emulation program that is connected directly to the switch via the RS-232 serial console port on the front of the switch. A console connection is referred to as an 'Out-of-Band' connection, meaning that console is connected to the switch using a different circuit than that used for normal network communications. So, the console can be used to set up and manage the switch even if the network is down.

Local console management uses the terminal connection to operate the console program built-in to the switch. A network administrator can manage, control, and monitor the switch from the console program.

The DES-3350SR contains a CPU, memory for data storage, flash memory for configuration data, operational programs, and SNMP agent firmware. These components allow the switch to be actively managed and monitored from either the console port or the network itself (out-of-band, or in-band).

Diagnostic (console) port (RS-232 DCE)

Out-of-band management requires connecting a terminal, such as a VT-100 or a PC running a terminal emulation program (such as HyperTerminal, which is automatically installed with Microsoft Windows) a to the RS-232 DCE console port of the Switch. Switch management using the RS-232 DCE console port is called *Local Console Management* to differentiate it from management performed via management platforms, such as D-View, HP OpenView, etc. *Web-based Management* describes management of the switch performed over the network (in-band) using the switch's built-in Web-based management program). The operations to be performed and the facilities provided by these two built-in programs are identical.

The console port is set at the factory for the following configuration:

- Baud rate: 9,600
- Data width: 8 bits
- Parity: none
- Stop bits: 1
- Flow Control None

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. If you still don't see anything, try hitting <Ctrl> + r to refresh the screen.

Switch IP Address

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

The switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found from the initial boot console screen – shown below.

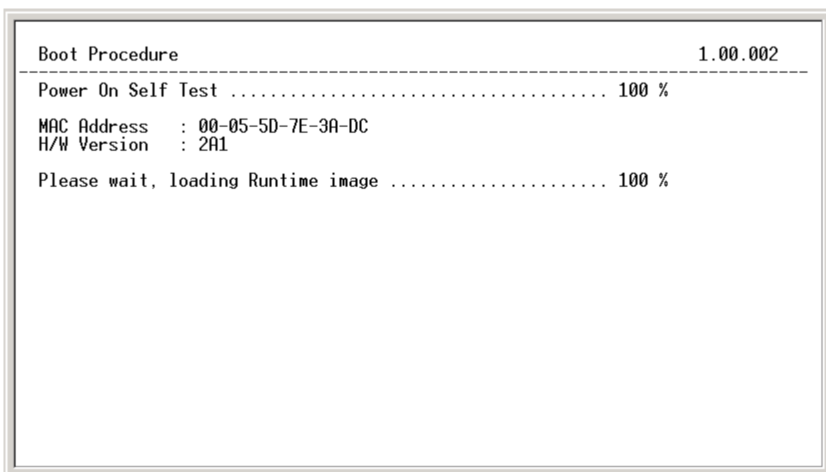


Figure 5- 1. Console Boot Screen

The switch's MAC address can also be found under the **Switch Information (Basic Settings)** window in the Web manager.

Setting an IP Address

The IP address for the switch must be set before it can be managed with the web-based manager. The switch IP address may 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 alternatively be set using the Command Line Interface (CLI) over the console serial port as follows:

1. Starting at the command line prompt **local>**, 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.

2. Alternatively, you can enter the commands **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.

Using this method, 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 Web-based management agent.

SNMP

The Simple Network Management Protocol (SNMP) is an OSI layer 7 (the application layer) protocol for remotely monitoring and configuring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. SNMP can be used to perform many of the same functions as a directly connected console, or can be used within an integrated network management software package such as DView.

SNMP performs the following functions:

- Sending and receiving SNMP packets through the IP protocol.
- Collecting information about the status and current configuration of network devices.
- Modifying the configuration of network devices.

The DES-3350SR has a software program called an 'agent' that processes SNMP requests, but the user program that makes the requests and collects the responses runs on a management station (a designated computer on the network). The SNMP agent and the user program both use the UDP/IP protocol to exchange packets.

Authentication

The authentication protocol ensures that both the router SNMP agent and the remote user SNMP application program discard packets from unauthorized users. Authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the router SNMP must use the same community string.

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).

Trap recipients are special users of the network who are given certain rights and access in overseeing the maintenance of the network. Trap recipients will receive traps sent from the Switch; they must immediately take certain actions to avoid future failure or breakdown of the network.

You can also specify which network managers may receive traps from the Switch by entering a list of the IP addresses of authorized network managers. Up to four trap recipient IP addresses, and four corresponding SNMP community strings can be entered.

SNMP community strings function like passwords in that the community string entered for a given IP address must be used in the management station software, or a trap will be sent.

The following are trap types the switch can send to a trap recipient:

- **Authentication Failure** – This trap signifies that someone has tried to logon to the switch using an invalid SNMP community string. The switch automatically stores the source IP address of the unauthorized user.

- **Cold Start** – This trap signifies that the Switch has been powered up and initialized such that software settings are reconfigured and hardware systems are rebooted. A cold start is different from a factory reset in that configuration settings saved to non-volatile RAM used to reconfigure the switch.

- **File Transfer Status Change** – This trap indicates file transfer status change notification.
- **Link Change Event** – This trap is sent whenever the link of a port changes from link up to link down or from link down to link up.
- **Power Failure** – This trap is sent to notify power failure.
- **Power Recover** – This trap is sent to notify power recovery.
- **Power Status Change** – As part of the Switch's built-in Redundant Power Supply, a trap is sent to notify power status change.
- **Save to NV-RAM** – This trap is sent whenever "Save all configuration of device to NV-RAM" has been processed.
- **Set to Factory Default** – The trap is sent whenever the "Set factory to default setting has been processed."
- **System Restart** – This trap contains the reboot information.
- **Topology Change** – A Topology Change trap is sent by the Switch when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a new root trap is sent for the same transition.

MIBs

Management and counter information are stored in 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. These MIBs may also be retrieved by specifying the MIB's Object-Identity (OID) at the network manager. MIB values can be either read-only or read-write.

Read-only MIBs variables can be either constants that are programmed into the Switch, or variables that change while the Switch is in operation. Examples of read-only constants are the number of port and type of ports. Examples of read-only variables are the statistics counters such as the number of errors that have occurred, or how many kilobytes of data have been received and forwarded through a port.

Read-write MIBs are variables usually related to user-customized configurations. Examples of these are the Switch's IP Address, Spanning Tree Algorithm parameters, and port status.

If you use a third-party vendors' SNMP software to manage the Switch, a diskette listing the Switch's propriety enterprise MIBs can be obtained by request. If your software provides functions to browse or modify MIBs, you can also get the MIB values and change them (if the MIBs' attributes permit the write operation). This process however can be quite involved, since you must know the MIB OIDs and retrieve them one by one.

Packet Forwarding

The Switch enters the relationship between destination MAC or IP addresses and the Ethernet port or gateway router the destination resides on into its forwarding table. This information is then used to forward packets. This reduces the traffic congestion on the network, because packets, instead of being transmitted to all ports, are transmitted to the destination port only. Example: if Port 1 receives a packet destined for a station on Port 2, the Switch transmits that packet through Port 2 only, and transmits nothing through the other ports. This process is referred to as 'learning' the network topology.

MAC Address Aging Time

The Aging Time affects the learning process of the Switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time.

The aging time can be from 10 to 1,000,000 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the switch.

If the Aging Time is too short however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the switch will broadcast the packet to all ports, negating many of the benefits of having a switch.

Static forwarding entries are not affected by the aging time.

Filtering

The switch uses a filtering database to segment the network and control communication between segments. It can also filter packets off the network for intrusion control. Static filtering entries can be made by MAC Address filtering.

Each port on the switch is a unique collision domain and the switch filters (discards) packets whose destination lies on the same port as where it originated. This keeps local packets from disrupting communications on other parts of the network.

For intrusion control, whenever a switch encounters a packet originating from or destined to a MAC address entered into the filter table, the switch will discard the packet.

Some filtering is done automatically by the switch:

- Dynamic filtering – automatic learning and aging of MAC addresses and their location on the network. Filtering occurs to keep local traffic confined to its segment.

- Filtering done by the Spanning Tree Protocol, which can filter packets based on topology, making sure that signal loops don't occur.

- Filtering done for VLAN integrity. Packets from a member of a VLAN (VLAN 2, for example) destined for a device on another VLAN (VLAN 3) will be filtered.

Some filtering requires the manual entry of information into a filtering table:

- MAC address filtering – the manual entry of specific MAC addresses to be filtered from the network. Packets sent from one manually entered MAC address can be filtered from the network. The entry may be specified as a source, a destination, or both.

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

Table 5- 1. Comparing Port States

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

Edge Port

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

P2P Port

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

802.1d/802.1w Compatibility

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

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.

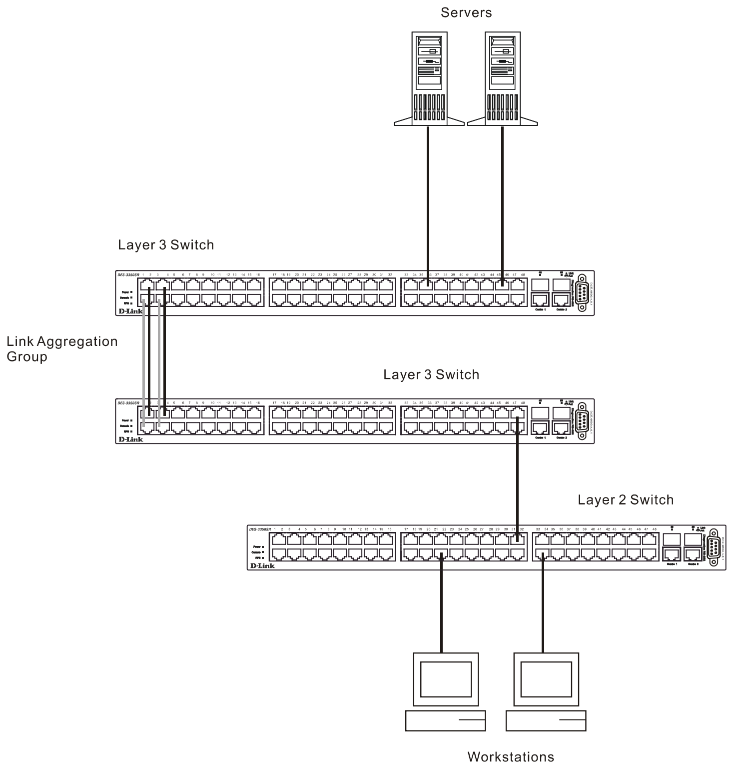


Figure 5- 2. Link Aggregation Group

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.

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.

Notes About VLANs on the DES-3350SR

1. 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).

2. 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 3 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.

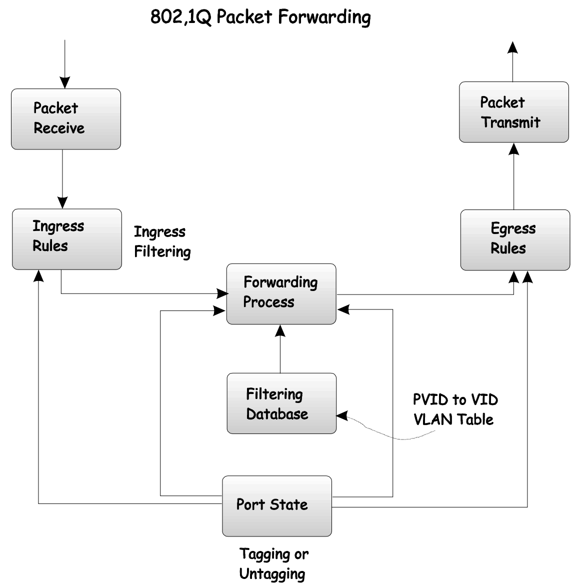


Figure 5- 3. IEEE 802.1Q Packet Forwarding

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 4 octets. All of the information contained in the packet originally is retained.

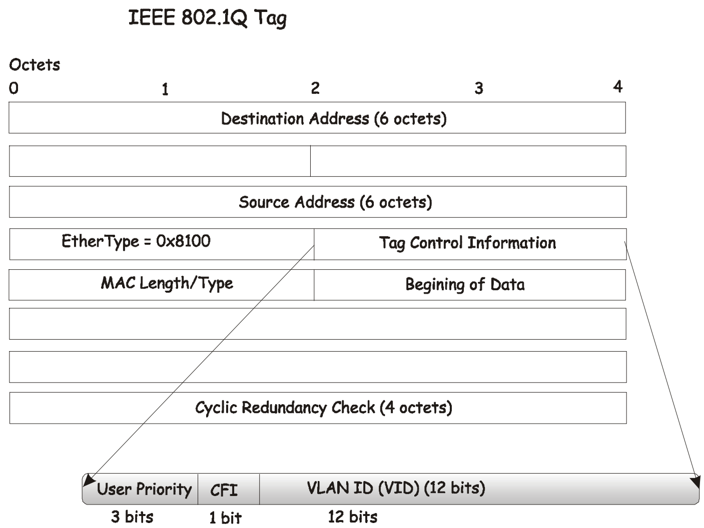


Figure 5- 4. IEEE 802.1Q Tag

The EtherType and VLAN ID are inserted after the MAC source address, but before the original EtherType/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

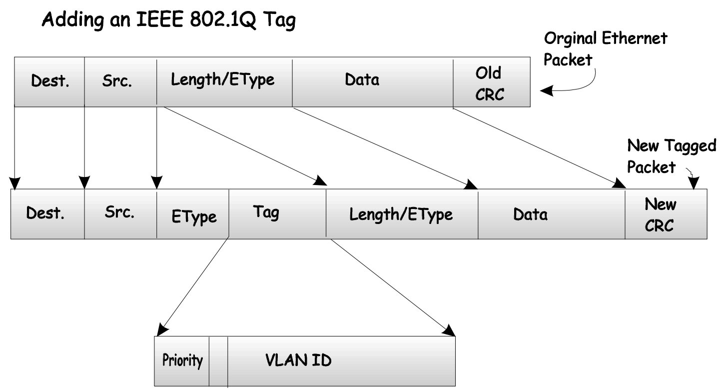


Figure 5- 5. Adding an IEEE 802.1Q Tag

Port VLAN ID

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

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

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

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

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLANs are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, 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 Filtering

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

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

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

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

VLANs in Layer 2 Only Mode

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 the switch is in **Layer 2 Only** mode. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

When the switch is in **Layer 2 Only** mode, 802.1Q VLANs are supported.

If no VLANs are configured on the switch and the switch is in **Layer 2 Only** mode, then all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.

A VLAN that does not have a corresponding IP interface defined for it, will function as a **Layer 2 Only** VLAN – regardless of the **Switch Operation** mode.

Layer 3-Based VLANs

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

The DES-3350SR allows an IP subnet to be configured for each 802.1Q VLAN that exists on the switch.

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

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

IP Addressing and Subnetting

This section gives basic information needed to configure your Layer 3 switch for IP routing. The information includes how IP addresses are broken down and how subnetting works. You will learn how to assign each interface on the router an IP address with a unique subnet.

Definitions

- **IP Address** – The unique number ID assigned to each host or interface on a network. IP addresses have the form xxx.xxx.xxx.xxx.
- **Subnet** – A portion of a network sharing a particular network address.
- **Subnet mask** – A 32-bit number used to describe which portion of a Network Address refers to the subnet and which portion refers to the host. Subnet masks have the form xxx.xxx.xxx.xxx.
- **Interface** – A network connection
- **IP Interface** – Another name for subnet.
- **Network Address** – The resulting 32-bit number from a bitwise logical AND operation performed between an IP address and a subnet mask.
- **Subnet Address** – Another name for network address.

IP Addresses

The Internet Protocol (IP) was designed for routing data between network sites. Later, it was adapted for routing between networks (referred to as "subnets") within a site. The IP defines a way of generating a unique number that can be assigned each network in the Internet and each of the computers on each of those networks. This number is called the IP address.

IP addresses use a "dotted decimal" notation. Here are some examples of IP addresses written in this format:

1. 210.202.204.205
2. 189.21.241.56
3. 125.87.0.1

This allows IP address to be written in a string of 4 decimal (base 10) numbers. Computers can only understand binary (base 2) numbers, and these binary numbers are usually grouped together in bytes, or eight bits. (A bit is a binary digit – either a "1" or a "0"). The dots (periods) simply make the IP address easier to read. A computer sees an IP address not as four decimal numbers, but as a long string of binary digits (32 binary digits or 32 bits, IP addresses are 32-bit addresses).

The three IP addresses in the example above, written in binary form are:

1. 11010010.11001010.11001100.11001101
2. 10111101.00010101.11110001.00111000
3. 01111101.01010111.00000000.00000001

The dots are included to make the numbers easier to read.

Eight binary bits are called a 'byte' or an 'octet'. An octet can represent any decimal value between '0' (00000000) and '255' (11111111). IP addresses, represented in decimal form, are four numbers whose value is between '0' to '255'. The total range of IP addresses are then:

Lowest possible IP address -	0.0.0.0
Highest possible IP address -	255.255.255.255

To convert decimal numbers to 8-bit binary numbers (and vice-versa), you can use the following chart:

Binary Octet Digit	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal Equivalent	128	64	32	16	8	4	2	1
Binary Number 128+64+32+16+8+4+2+1= 255	1	1	1	1	1	1	1	1

Table 5- 2. Binary to Decimal Conversion

Each digit in an 8-bit binary number (an octet) represents a power of two. The left-most digit represents 2 raised to the 7th power (2x2x2x2x2x2x2=128) while the right-most digit represents 2 raised to the 0th power (any number raised to the 0th power is equal to one, by definition).

IP addresses actually consist of two parts, one identifying the network and one identifying the destination (node) within the network.

The IP address discussed above is one part and a second number called the Subnet mask is the other part. To make this a bit more confusing, the subnet mask has the same numerical form as an IP address.

Address Classes

Address classes refer to the range of numbers in the subnet mask. Grouping the subnet masks into classes makes the task of dividing a network into subnets a bit easier.

There are five address classes. The first four bits in the IP address determine which class the IP address falls in.

- Class A addresses begin with 0xxx, or 1 to 126 decimal.
- Class B addresses begin with 10xx, or 128 to 191 decimal.
- Class C addresses begin with 110x, or 192 to 223 decimal.
- Class D addresses begin with 1110, or 224 to 239 decimal.
- Class E addresses begin with 1111, or 240 to 254 decimal.

Addresses beginning with 01111111, or 127 decimal, are reserved. They are used for internal testing on a local machine (called loopback). The address 127.0.0.1 can always be pinged from a local node because it forms a loopback and points back to the same node.

Class D addresses are reserved for multicasting.

Class E Addresses are reserved for future use. They are not used for node addresses.

The part of the IP address that belongs to the network is the part that is 'hidden' by the '1's in the subnet mask. This can be seen below:

- Class A NETWORK.node.node.node
- Class B NETWORK.NETWORK.node.node
- Class C NETWORK.NETWORK.NETWORK.node

For example, the IP address 10.42.73.210 is a Class A address, so the Network part of the address (called the *Network Address*) is the first octet (10.x.x.x). The node part of the address is the last three octets (x.42.73.210).

To specify the network address for a given IP address, the node part is set to all "0"s. In our example, 10.0.0.0 specifies the network address for 10.42.73.210. When the node part is set to all "1"s, the address specifies a broadcast address. So, 10.255.255.255 is the broadcast address for the network 10.0.0.0.

Subnet Masking

A subnet mask can be applied to an IP address to identify the network and the node parts of the address. A bitwise logical AND operation between the IP address and the subnet mask results in the *Network Address.*

For example:

00001010.00101010.01001001.11010010	10.42.73.210	Class A IP address
11111111.00000000.00000000.00000000	255.0.0.0	Class A Subnet Mask

00001010.00000000.00000000.00000000	10.0.0.0	Network Address

The Default subnet masks are:

- Class A – 11111111.00000000.00000000.00000000
  255.0.0.0
- Class B – 11111111.11111111.00000000.00000000
  255.255.0.0
- Class C – 1111111.11111111.11111111.00000000
  255.255.255.0

Additional bits can be added to the default subnet mask for a given Class to further subnet a network. When a bitwise logical AND operation is performed between the subnet mask and the IP address, the result defines the *Subnet Address*.

Some restrictions apply to subnet addresses. Addresses of all "0"s and all "1"s are reserved for the local network (when a host does not know it's network address) and for all hosts on the network (the broadcast address). This also applies to subnets. A subnet address cannot be all "0"s or all "1"s. A 1-bit subnet mask is also not allowed.

Calculating the Number of Subnets and Nodes

To calculate the number of subnets and nodes, use the formula ($2^n - 2$) where n = the number of bits in either the subnet mask or the node portion of the IP address. Multiplying the number of subnets by the number of nodes available per subnet gives the total number of nodes for the entire network.

Example

00001010.00101010.01001001.11010010	10.42.73.210	Class A IP address
11111111.11100000.00000000.00000000	255.224.0.0	Subnet Mask
00001010.00100000.00000000.00000000	10.32.0.0	Network Address
00001010.00101010.11111111.11111111	10.32.255.255	Broadcast Address

This example uses an 11-bit subnet mask. (There are 3 additional bits added to the default Class A subnet mask). So the number of subnets is:

$$2^3 - 2 = 8 - 2 = 6$$

Subnets of all "0"s and all "1"s are not allowed, so two subnets are subtracted from the total.

The number of bits used in the node part of the address is 24 – 3 = 21 bits, so the total number of nodes is:

$$2^{21} - 2 = 2{,}097{,}152 - 2 = 2{,}097{,}150$$

Multiplying the number of subnets times the number of nodes gives 12,582,900 possible nodes.

Note that this is less than the 16,777,214 possible nodes that an unsubnetted class A network would have.

Subnetting reduces the number of possible nodes for a given network, but increases the segmentation of the network.

Classless InterDomain Routing – CIDR

Under CIDR, the subnet mask notation is reduced to a simplified shorthand. Instead of specifying all of the bits of the subnet mask, it is simply listed as the number of contiguous "1"s (bits) in the network portion of the address. Look at the subnet mask of the above example in binary - 11111111.11100000.00000000.00000000 – and you can see that there are 11 "1"s or 11 bits used to mask the network address from the node address. Written in CIDR notation this becomes:

10.32.0.0/11

# of Bits	Subnet Mask	CIDR Notation	# of Subnets	# of Hosts	Total Hosts
2	255.192.0.0	/10	2	419430	8388604

				2	
3	255.224.0.0	/11	6	209715 0	12582900
4	255.240.0.0	/12	14	104857 4	14680036
5	255.248.0.0	/13	30	524286	15728580
6	255.252.0.0	/14	62	262142	16252804
7	255.254.0.0	/15	126	131070	16514820
8	255.255.0.0	/16	254	65534	16645636
9	255.255.128.0	/17	510	32766	16710660
10	255.255.192.0	/18	1022	16382	16742404
11	255.255.224.0	/19	2046	8190	16756740
12	255.255.240.0	/20	4094	4094	16760836
13	255.255.248.0	/21	8190	2046	16756740
14	255.255.252.0	/22	16382	1022	16742404
15	255.255.254.0	/23	32766	510	16710660
16	255.255.255.0	/24	65534	254	16645636
17	255.255.255.1 28	/25	131070	126	16514820
18	255.255.255.1 92	/26	262142	62	16252804
19	255.255.255.2 24	/27	525286	30	15728580
20	255.255.255.2 40	/28	104857 4	14	14680036
21	255.255.255.2 48	/29	209715 0	6	12582900
22	255.255.255.2 52	/30	419430 2	2	8388604

Table 5-9. Class A Subnet Masks

# of Bits	Subnet Mask	CIDR Notation	# of Subnets	# of Hosts	Total Hosts
2	255.255.192	/18	2	16382	32764
3	255.255.224.0	/19	6	8190	49140
4	255.255.240.0	/20	14	4094	57316
5	255.255.248.0	/21	30	2046	61380
6	255.255.252.0	/22	62	1022	63364
7	255.255.254.0	/23	126	510	64260
8	255.255.255.0	/24	254	254	64516
9	255.255.255.128	/25	510	126	64260

10	255.255.255.192	/26	1022	62	63364
11	255.255.255.224	/27	2046	30	61380
12	255.255.255.240	/28	4094	14	57316
13	255.255.255.248	/29	8190	6	49140
14	255.255.255.252	/30	16382	2	32764

Table 5-10. Class B Subnet Masks

# of Bits	Subnet Mask	CIDR Notation	# of Subnets	# of Hosts	Total Hosts
2	255.255.255.192	/26	2	62	124
3	255.255.255.224	/27	6	30	180
4	255.255.255.240	/28	14	14	196
5	255.255.255.248	/29	30	6	180
6	255.255.255.252	/30	62	2	124

Table 5-11. Class C Subnet Masks

Internet Protocols

This is a brief introduction to the suite of Internet Protocols frequently referred to as TCP/IP. It is intended to give the reader a reasonable understanding of the available facilities and some familiarity with terminology. It is not intended to be a complete description.

Protocol Layering

The Internet Protocol (IP) divides the tasks necessary to route and forward packets across networks by using a layered approach. Each layer has clearly defined tasks, protocol, and interfaces for communicating with adjacent layers, but the exact way these tasks are accomplished is left to individual software designers. The Open Systems Interconnect (OSI) seven-layer model has been adopted as the reference for the description of modern networking, including the Internet.

A diagram of the OSI model is shown below (note that this is not a complete listing of the protocols contained within each layer of the model):

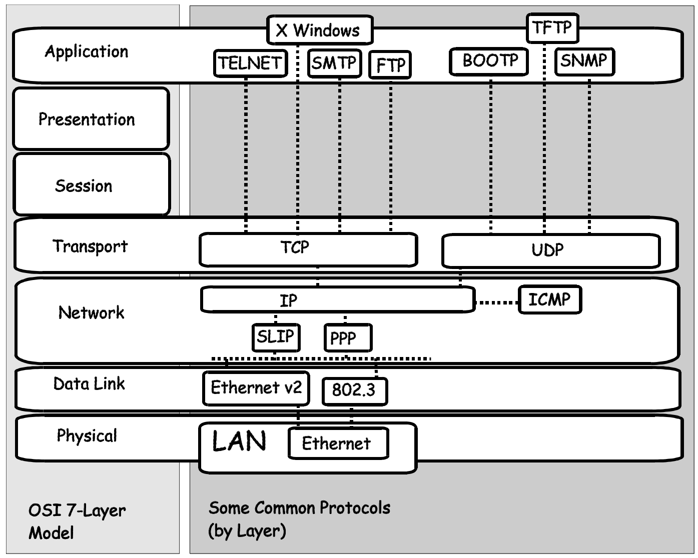


Figure 5- 6. OSI Seven Layer Network Model

Each layer is a distinct set of programs executing a distinct set of protocols designed to accomplish some necessary tasks. They are separated from the other layers within the same system or network, but must communicate and interoperate. This requires very well defined and well-known methods for transferring messages and data. This is accomplished through the protocol stack.

Protocol layering as simply a tool for visualizing the organization of the necessary software and hardware in a network. In this view, Layer 2 represents switching and Layer 3 represents routing. Protocol layering is actually a set of guidelines used in writing programs and designing hardware that delegate network functions and allow the layers to communicate. How these layers communicate within a stack (for example, within a given computer) is left to the operating system programmers.

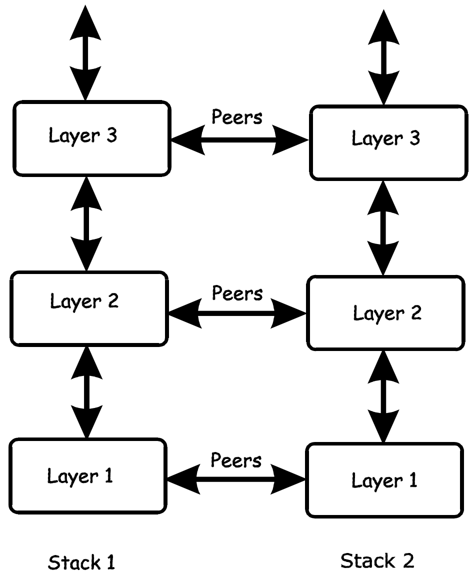


Figure 5- 7. The Protocol Stack

Between two protocol stacks, members of the same layer are known as peers and communicate by well-known (open and published) protocols. Within a protocol stack, adjacent layers communicate by an internal interface. This interface is usually not publicly documented and is frequently proprietary. It has some of the same characteristics of a protocol and two stacks from the same software vendor may communicate in the same way. Two stacks from different software vendors (or different products from the same vendor) may communicate in completely different ways. As long as peers can communicate and interoperate, this has no impact on the functioning of the network.

The communication between layers within a given protocol stack can be both different from a second stack and proprietary, but communication between peers on the same OSI layer is open and consistent.

A brief description of the most commonly used functional layers is helpful to understand the scope of how protocol layering works.

Layer 1

This is referred to as the physical layer. It handles the electrical connections and signaling required to make a physical link from one point in the network to another. It is on this layer that the unique Media Access Control (MAC) address is defined.

Layer 2

This layer, commonly called the switching layer, allows end station addressing and the establishment of connections between them.

Layer 2 switching forwards packets based on the unique MAC address of each end station and offers high-performance, dedicated-bandwidth of Fast or Gigabit Ethernet within the network.

Layer 2 does not ordinarily extend beyond the intranet. To connect to the Internet usually requires a router and a modem or other device to connect to an Internet Service Provider's WAN. These are Layer 3 functions.

Layer 3

Commonly referred to as the routing layer, this layer provides logical partitioning of networks (subnetting), scalability, security, and Quality of Service (QoS).

The backbone of the Internet is built using Layer 3 functions. IP is the premier Layer 3 protocol.

IP is itself, only one protocol in the IP protocol suite. More extensive capabilities are found in the other protocols of the IP suite. For example, the Domain Name System (DNS) associates IP addresses with text names, the Dynamic Host Configuration Protocol (DCHP) eases the administration of IP addresses, and routing protocols such as the Routing Information Protocol (RIP), the Open Shortest Path First (OSPF), and the Border Gateway Protocol (BGP) enable Layer 3 devices to direct data traffic to the intended destination. IP security allows for authentication and encryption. IP not only allows for user-to-user communication, but also for transmission from point-to-multipoint (known as IP multicasting).

Layer 4

This layer, known as the transport layer, establishes the communication path between user applications and the network infrastructure and defines the method of communicating. TCP and UDP are well-known protocols in the transport layer. TCP is a "connection-oriented" protocol, and requires the establishment of parameters for transmission prior to the exchange of data. Web technology is based on TCP. UDP is "connectionless" and requires no connection setup. This is important for multicast traffic, which cannot tolerate the overhead and latency of TCP. TCP and UDP also differ in the amount of error recovery provided and whether or not it is visible to the user application. Both TCP and UDP are layered on IP, which has minimal error recovery and detection. TCP forces retransmission of data that was lost by the lower layers, UDP does not.

Layer 7

This layer, known as the application layer, provides access to either the end user application software such as a database. Users communicate with the application, which in turn delivers data to the transport layer. Applications do not usually communicate directly with lower layers. They are written to use a specific communication library, like the popular WinSock library.

Software developers must decide what type of transport mechanism is necessary. For example, Web access requires reliable, error-free access and would demand TCP. Multimedia, on the other hand, requires low overhead and latency and commonly uses UDP.

TCP/IP

The TCP/IP protocol suite is a set of protocols that allow computers to share resources across a network. TCP and IP are only two of the Internet suite of protocols, but they are the best known and it has become common to refer the entire family of Internet protocols as TCP/IP.

TCP/IP is a layered set of protocols. An example, such as sending e-mail, can illustrate this. There is first a protocol for sending and receiving e-mail. This protocol defines a set of commands to identify the sender, the recipient, and the content of the e-mail. The e-mail protocol will not handle the actual communication between the two computers, this is done by TCP/IP. TCP/IP handles the actual sending and receiving of the packets that make up the e-mail exchange.

TCP makes sure the e-mail commands and messages are received by the appropriate computers. It keeps track of what is sent and what is received, and retransmits any packets that are lost or dropped. TCP also handles the division of large messages into several Ethernet packets, and makes sure these packets are received and reassembled in the correct order.

Because these functions are required by a large number of applications, they are grouped into a single protocol, rather than being the part of the specifications for just sending e-mail. TCP is then a library of routines that application software can use when reliable network communications are required.

IP is also a library of routines, but with a more general set of functions. IP handles the routing of packets from the source to the destination. This may require the packets to traverse many different networks. IP can route packets through the necessary gateways and provides the functions required for any user on one network to communicate with any user on another connected network.

The communication interface between TCP and IP is relatively simple. When IP received a packet, it does not know how this packet is related to others it has sent (or received) or even which connection the packet is part of. IP only knows the address of the source and the destination of the packet, and it makes its best effort to deliver the packet to its destination.

The information required for IP to do its job is contained in a series of octets added to the beginning of the packet called headers. A header contains a few octets of data added to the packet by the protocol in order to keep track of it.

Other protocols on other network devices can add and extract their own headers to and from packets as they cross networks. This is analogous to putting data into an envelope and sending the envelope to a higher-level protocol, and having the higher-level protocol put the entire envelope into its own, larger envelope. This process is referred to as encapsulation.

Many levels of encapsulation are required for a packet to cross the Internet.

Packet Headers

TCP

Most data transmissions are much longer that a single packet. The data must then be divided up among a series of packets. These packets must be transmitted, received and then reassembled into the original data. TCP handles these functions.

TCP must know how large a packet the network can process. To do this, the TCP protocols at each end of a connection state how large a packet they can handle and the smaller of the two is selected.

The TCP header contains at least 20 octets. The source and destination TCP port numbers are the most important fields. These specify the connection between two TCP protocols on two network devices.

The header also contains a sequence number that is used to ensure the packets are received in the correct order. The packets are not numbered, but rather the octets the packets contain are. If there are 100 octets of data in each packet, the first packet is numbered 0, the second 100, the third 200, etc.

To insure that the data in a packet is received uncorrupted, TCP adds the binary value of all the octets in the packet and writes the sum in the checksum field. The receiving TCP recalculates the checksum and if the numbers are different, the packet is dropped.

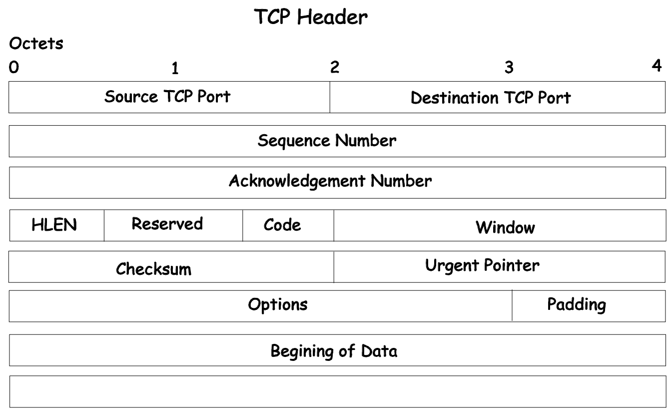


Figure 5- 8. TCP Packet Header

When packets have been successfully received, TCP sends an acknowledgement. This is simply a packet that has the acknowledgement number field filled in.

An acknowledgement number of 1000 indicates that all of the data up to octet 1000 has been received. If the transmitting TCP does not receive an acknowledgement in a reasonable amount of time, the data is resent.

The window field controls the amount of data being sent at any one time. It would require too much time and overhead to acknowledge each packet received. Each end of the TCP connection declares how much data it is able to receive at any one time by writing this number of octets in the window field.

The transmitting TCP decrements the number in the window field and when it reaches zero, the transmitting TCP stops sending data. When the receiving TCP can accept more data, it increases the number in the window field. In practice, a single packet can acknowledge the receipt of data and give permission for more data to be sent.

IP

TCP sends its packets to IP with the source and destination IP addresses. IP is only concerned with these IP addresses. It is not concerned with the contents of the packet or the TCP header.

IP finds a route for the packet to get to the other end of the TCP connection. IP adds its own header to the packet to accomplish this.

The IP header contains the source and destination addresses, the protocol number, and another checksum.

The protocol number tells the receiving IP which protocol to give the packet to. Although most IP traffic uses TCP, other protocols can be used (such as UDP).

The checksum is used by the receiving IP in the same way as the TCP checksum.

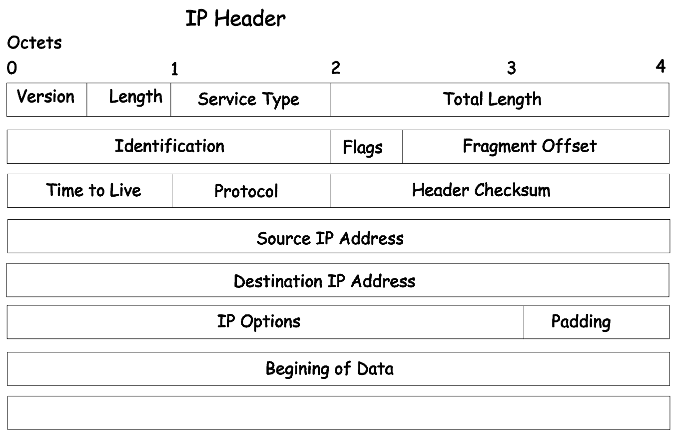


Figure 5- 9. IP Packet Header

The flags and fragment offset are used to keep track of packets that must be divided among several smaller packets to cross networks for which they are too large.

The Time-to-Live (TTL) is the number of gateways the packet is allowed to cross between the source and destination. This number is decremented by one when the packet crosses a gateway and when the TTL reaches zero, the packet is dropped. This helps reduce network traffic if a loop develops.

Ethernet

Every active Ethernet device has its own Ethernet address (commonly called the MAC address) assigned to it by the manufacturer. Ethernet uses 48 bit addresses.

The Ethernet header is 14 octets that include the source and destination MAC address and a type code.

There is no relationship between the MAC address of a network node and its IP address. There must be a database of Ethernet addresses and their corresponding IP addresses.

Different protocol families can be in use on the same network. The type code field allows each protocol family to have its own entry.

A checksum is calculated and when the packet is received, the checksum is recalculated. If the two checksums are different, the packet is dropped.

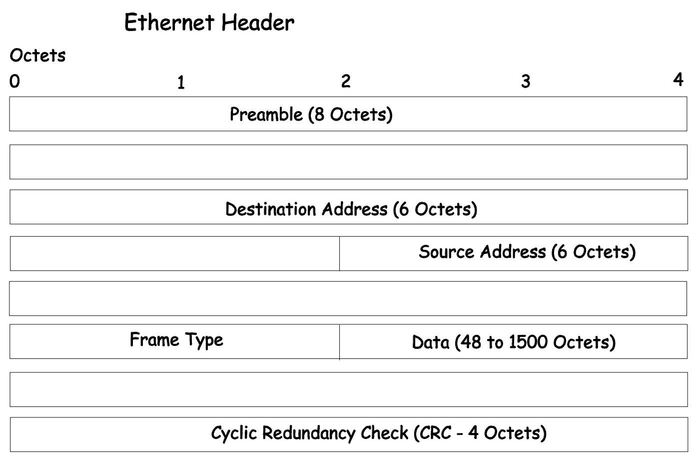


Figure 5- 10. Ethernet Packet Header

When a packet is received, the headers are removed. The Ethernet Network Interface Card (NIC) removes the Ethernet header and checks the checksum. It then looks at the type code. If the type code is for IP, the packet is given to IP. IP then removes the IP header and looks at its protocol field. If the protocol field is TCP, the packet is sent to TCP. TCP then looks at the sequence number and uses this number and other data from the headers to reassemble the data into the original file.

TCP and UDP Well-Known Ports

Application protocols run 'on top of' TCP/IP. When an application wants to send data or a message, it gives the data to TCP. Because TCP and IP take care of the networking details, the application can look at the network connection as a simple data stream.

To transfer a file across a network using the File Transfer Protocol (FTP), a connection must first be established. The computer requesting the file transfer must connect specifically to the FTP server on the computer that has the file.

This is accomplished using sockets. A socket is a pair of TCP port numbers used to establish a connection from one computer to another. TCP uses these port numbers to keep track of connections. Specific port numbers are assigned to applications that wait for requests. These port numbers are referred to as 'well-known' ports.

TCP will open a connection to the FTP server using some random port number, 1234 for example, on the local computer. TCP will specify port 21 for the FTP server. Port 21 is the well-known port number for FTP servers. Note that there are two different FTP programs running in this example – an FTP client that requests the file to be transferred, and an FTP server that sends the file to the FTP client. The FTP server accepts commands from the client, so the FTP client must know how to connect to the server (must know the TCP port number) in order to send commands. The FTP Server can use any TCP port number to send the file, so long as it is sent as part of the connection setup.

A TCP connection is then described by a set of four numbers – the IP address and TCP port number for the local computer, and the IP address and TCP port number for the remote computer. The IP address is in the IP header and the TCP port number is in the TCP header.

No two TCP connection can have the same set of numbers, but only one number needs to be different. It is possible, for example, for two users to send files to the same destination at the same time. This could give the following connection numbers:

	Internet addresses	TCP ports
Connection 1	10.42.73.23, 10.128.12.1	1234, 21
Connection 2	10.42.73.23, 10.128.12.1	1235, 21

The same computers are making the connections, so the IP addresses are the same. Both computers are using the same well-known TCP port for the FTP server. The local FTP clients are using different TCP port numbers.

FTP transfers actually involve two different connections. The connection begins by the FTP sending commands to send a particular file. Once the commands are sent, a second connection is opened for the actual data transfer. Although it is possible to send data on the same connection, it is very convenient for the FTP client to be able to continue to send commands (such as 'stop sending this file').

UDP and ICMP

There are many applications that do not require long messages that cannot fit into a single packet. Looking up computer names is an example. Users wanting to make connections to other computers will usually use a name rather than the computer's IP or MAC address. The user's computer must be able to determine the remote computer's address before a connection can be made. A designated computer on the network will contain a database of computer names and their corresponding IP and MAC addresses. The user's computer will send a query to the name database computer, and the database computer will send a response. Both the query and the response are very short. There is no need to divide the query or response between multiple packets, so the complexity of TCP is not required. If there is no response to the query after a period of time, the query can simply be resent.

The User Datagram Protocol (UDP) is designed for communications that do not require division among multiple packets and subsequent reassembly. UDP does not keep track of what is sent.

UDP uses port numbers in a way that is directly analogous to TCP. There are well-known UDP port numbers for servers that use UDP.

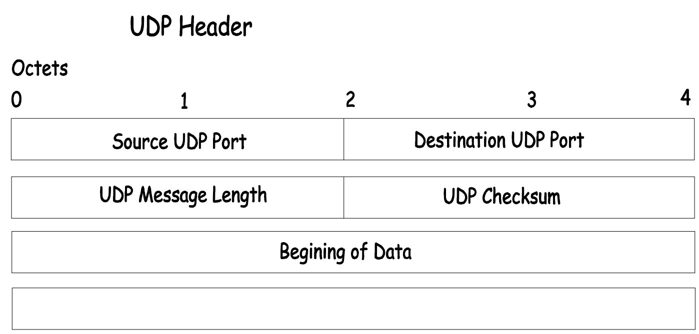


Figure 5- 11. UDP Packet Header

The UDP header is shorter than a TCP header. UDP also uses a checksum to verify that data is received uncorrupted.

The Internet Control Message Protocol (ICMP) is also a simplified protocol used for error messages and messages used by TCP/IP. ICMP, like UDP, processes messages that will fit into a single packet. ICMP does not, however use ports because its messages are processed by the network software.

The Domain Name System

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

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

For two DNS servers to communicate across different subnets, the **DNS Relay** of the DES-3350SR 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 subdomain. 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 DCHP or BOOTP server, or can be entered manually and configured into the operating system at startup.

DHCP Servers

The Dynamic Host Configuration Protocol (DHCP) is used to dynamically assign a TCP/IP network configuration to network devices and computers on the network. It also ensures that IP address conflicts do not occur.

IP addresses are assigned from a pool of free addresses. Each IP address assigned has a 'lease' and a 'lease expiration period'. The lease must be periodically renewed. If the lease is expires, the IP address is returned to the pool of available IP addresses.

Usually, it is a network policy to assign the same IP address to a given network device or computer each time.

If the IP address lease expires, the network device sends a message to the DHCP server requesting a lease renewal. The DHCP server can send an acknowledgement containing a new lease and updated configuration information.

If an IP address lease cannot be renewed, the network device or computer sends a request to all local DHCP servers attempting to renew the lease. If the DHCP returns a negative acknowledgement, the network device must release its TCP/IP configuration and reinitialize.

When a new TCP/IP configuration is received from a DHCP server, the network device checks for a possible IP address conflict by sending an Address Resolution Protocol (ARP) request that contains its new IP address.

IP Routing

IP handles the task of determining how packets will get from their source to their destination. This process is referred to as routing.

For IP to work, the local system must be attached to a network. It is safe to assume that any system on this network can send packets to any other system, but when packets must cross other networks to reach a destination on a remote network, these packets must be handled by gateways (also called routers).

Gateways connect a network with one or more other networks. Gateways can be a computer with two network interfaces or a specialized device with multiple network interfaces. The device is designed to forward packets from one network to another.

IP routing is based on the network address of the destination IP address. Each computer has a table of network addresses. For each network address, a corresponding gateway is listed. This is the gateway to use to communicate with that network. The gateway does not have to be directly connected to the remote network, it simply needs to be the first place to go on the way to the remote network.

Before a local computer sends a packet, it first determines whether the destination address is on the local network. If it is, the packet can be sent directly to the remote device. If it is not, the local computer looks for the network address of the destination and the corresponding gateway address. The packet is then sent to the gateway leading to the remote network. There is often only one gateway on a network.

A single gateway is usually defined as a default gateway, if that gateway connects the local network to a backbone network or to the Internet. This default gateway is also used whenever no specific route is found for a packet, or when there are several gateways on a network.

Local computers can use default gateways, but the gateways themselves need a more complete routing table to be able to forward packets correctly. A protocol is required for the gateways to be able to communicate between themselves and to keep their routing tables updated.

Packet Fragmentation and Reassembly

TCP/IP can be used with many different types of networks, but not all network types can handle the same length packets.

When IP is transmitting large files, large packets are much more efficient than small ones. It is preferable to use the largest possible packet size, but still be able to cross networks that require smaller packets.

To do this, IP can 'negotiate' packet size between the local and remote ends of a connection. When an IP connection is first made, the IPs at both ends of the connection state the largest packet they can handle. The smaller of the two is selected.

When an IP connection crosses multiple networks, it is possible that one of the intermediate networks has a smaller packet size limit than the local or remote network. IP is not able to determine the maximum packet size across all of the networks that may make up the route for a connection. IP has, therefore, a method to divide packets into multiple, smaller packets to cross such networks. This division of large packets into smaller packets is referred to as fragmentation.

A field in the IP header indicates that a packet has been fragmented, and other information aids in the reassembly of the packets into the original data.

Gateways that connect networks of different packet size limits split the large packets into smaller ones and forward the smaller packets on their attached networks.

ARP

The Address Resolution Protocol (ARP) determines the MAC address and IP address correspondence for a network device.

A local computer will maintain an ARP cache that is a table of MAC addresses and the corresponding IP addresses. Before a connection with another computer is made, the local computer first checks its ARP cache to determine whether the remote computer has an entry. If it does, the local computer reads the remote computer's MAC address and writes it into the destination field of the packets to be sent.

If the remote computer does not have an ARP cache entry, the local computer must send an ARP request and wait for a reply.

When the local computer receives the ARP reply packet, the local ARP reads the IP MAC address pair, and then checks the ARP cache for this entry. If there is an entry, it is updated with the new information. If there is no entry, a new entry is made.

There are two possible cases when an ARP packet is received by a local computer. First, the local computer is the target of the request. If it is, the local ARP replies by sending its MAC IP address pair back to the requesting system. Second, if the local computer is not the target of the request, the packet is dropped.

Multicasting

Multicasting is a group of protocols and tools that enable a single source point to send packets to groups of multiple destination points with persistent connections that last for some amount of time. The main advantage to multicasting is a decrease in the network load compared to broadcasting.

Multicast Groups

Class D IP addresses are assigned to groups of network devices that comprise a multicast group. The four most significant four bits of a Class D address are set to "1110". The following 28 bits is referred to as the 'multicast group ID'. Some of the range of Class D addresses are registered with the Internet Assigned Numbers Authority (IANA) for special purposes. For example, the block of multicast addresses ranging from 224.0.0.1 to 224.0.0.225 is reserved for use by routing protocols and some other low-level topology discovery and maintenance protocols.

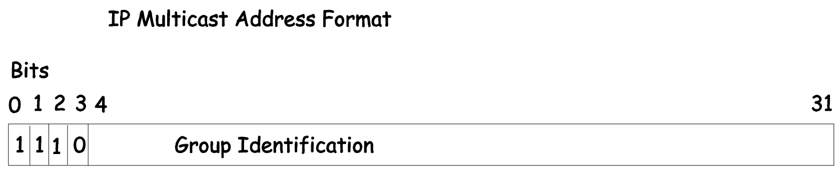


Figure 5- 12. Class D Multicast Address

Some of the reserved IP multicast addresses are as follows:

Address	Assignment
224.0.0.0	Base Address (reserved)
224.0.0.1	All Systems on this subnet
224.0.0.2	All Routers on this subnet
224.0.0.3	Unassigned
224.0.0.4	DVMRP Routers
224.0.0.5	OSPF IGP Routers
224.0.0.6	OSPF IGP Designated Routers
224.0.0.7	ST Routers
224.0.0.8	ST Hosts
224.0.0.9	All RIP2 Routers
224.0.0.10	All IGRP Routers
224.0.0.11	Mobile Agents
224.0.0.12	DHCP Servers and Relay Agents
224.0.0.13	All PIM Routers
224.0.0.14	RSVP Encapsulation
224.0.0.15	All CBT Routers
224.0.0.16	Designated Sbm
224.0.0.17	All Sbms
224.0.0.18	VRRP
224.0.0.19	Unassigned

through	
224.0.0.225	
224.0.0.21	DVMRP on MOSPF

Table 5- 3. Reserved Multicast Address Assignment

Internet Group Management Protocol (IGMP)

End users that want to receive multicast packets must be able to inform nearby routers that they want to become a multicast group member of the group these packets are being sent to. The Internet Group Management Protocol (IGMP) is used by multicast routers to maintain multicast group membership. IGMP is also used to coordinate between multiple multicast routers that may be present on a network by electing one of the multicast routers as the 'querier'. This router then keep track of the membership of multicast groups that have active members on the network. IGMP is used to determine whether the router should forward multicast packets it receives to the subnetworks it is attached to or not. A multicast router that has received a multicast packet will check to determine if there is at least one member of a multicast group that has requested to receive multicast packets from this source. If there is one member, the packet is forwarded. If there are no members, the packet is dropped.

IGMP Versions 1 and 2

Users that want to receive multicast packets need to be able to join and leave multicast groups. This is accomplished using IGMP.

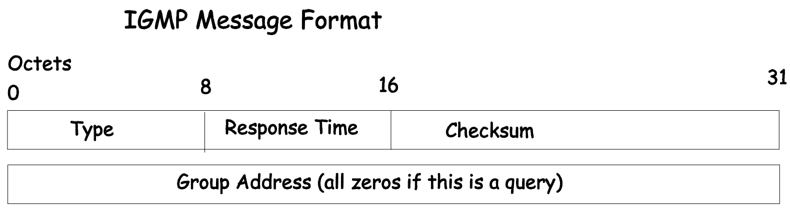


Figure 5- 13. IGMP Message Format

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)

Table 5- 4. IGMP Type Codes

Multicast routers use IGMP to manage multicast group memberships:

- An IGMP "report" is sent by a user's computer to join a group
- IGMP version 1 does not have an explicit 'leave' message. Group members have an expiration timer, and if this timer expires before a query response is returned, the member is dropped from the group.
- IGMP version 2 introduces an explicit "leave" report. When a user wants to leave a group, this report is sent to the multicast router (for IGMP version 2).

- 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, and multicast packets are not forwarded.

The TTL field of query messages is set to 1 so that the queries do not get forwarded to other subnetworks.

IGMP version 2 introduces a few extensions to IGMP version 1 such as, the election of a single multicast querier for each network, explicit 'leave' reports, and queries that are specific to a particular multicast group.

The router with the lowest IP address is elected as the querier. The explicit group leave message is added to decrease latency, and routers can ask for membership reports from a particular multicast group ID.

The transition states a host will go through to join or leave a multicast group are shown in the diagram below.

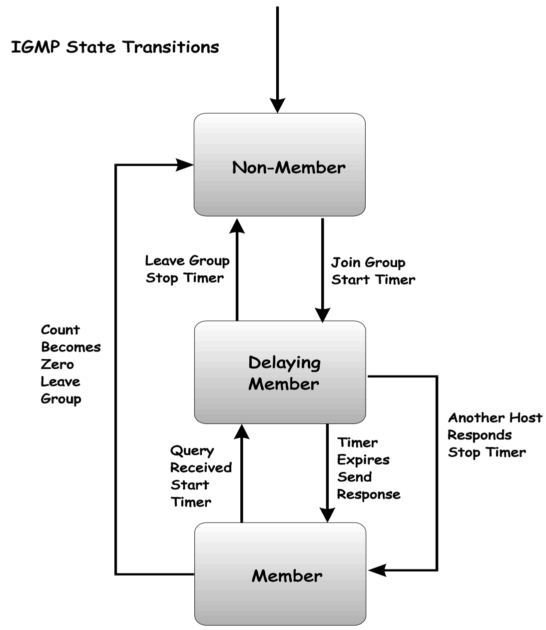


Figure 5- 14. IGMP State Transitions

Multicast Routing Algorithms

An algorithm is not a program. An algorithm is a statement of how a problem can be solved. A program is written to implement an algorithm.

Multicast packets are delivered by constructing multicast trees where the multicast router is the trunk, the branches are the various subnetworks that may be present, and the leaves are end recipients of the multicast packets. Several algorithms have been developed to construct these trees and to prune branches that have no active mulitcast group members

Flooding

The simplest algorithm for the delivery of multicast packets is for the multicast router to forward a multicast packet to all interfaces. This is referred to as flooding. An equally simple refinement of flooding is to have the router check to determine if a given multicast packet has been received before (in a certain amount of time). If it has, then the packet does not need to be forwarded at all and can be dropped. If the packet is being received for the first time, it should be flooded to all interface, except the interface on which it was received. This will ensure that all routers on the network will receive at least one copy of the multicast packet.

There are some obvious disadvantages to this simple algorithm. Flooding duplicates a lot of packets and uses a lot of network bandwidth. A multicast router must also keep a record of the multicast packets it has received (for a period of time) to determine if a given packet has been previously received. So flooding uses a lot of router memory.

Multicast Spanning Trees

A multicast delivery tree that spans the entire network with a single active link between routers (or subnetwork) is called a multicast spanning tree. Links (or branches) are chosen such that there is only one active path between any two routers. When a router receives a multicast packet, it forwards the packet on all links except the one on which it was received. This guarantees that all routers in the network will receive a copy of the packet. The only information the router needs to store is whether a link is a part of the spanning tree (leads to a router) or not.

Multicast spanning trees do not use group membership information when deciding to forward or drop a given multicast packet.

Reverse Path Broadcasting (RPB)

The Reverse Path Broadcasting (RPB) algorithm is an enhancement of the multicast spanning tree algorithm. RPB constructs a spanning tree for each multicast source. When the router receives a multicast packet, it then checks to determine if the packet was received on the shortest path back from the router to the source. If the packet was received on the shortest path back to the source, the packet is forwarded on all links except the link on which the packet was received. If the packet was not received on the shortest link back to the source, the packet is dropped.

If a link-state routing protocol is in use, RPB on a local router can determine if the path from the source through the local router to an immediately neighboring router. If it is not, the packet will be dropped at the next router and the packet should not be forwarded.

If a distance-vector routing protocol is in use, a neighboring router can either advertise its previous hop for the source as part of its routing update messages. This will 'poison-reverse' the route (or have the local router prune the branch from the multicast source to the neighboring router because the neighboring router has a better route from the source to the next router or subnetwork).

Since multicast packets are forwarded through the shortest route between source and destination, RPB is fast. A given router also does not need information about the entire spanning tree, nor does it need a mechanism to stop the forwarding of packets.

RPB does not use multicast group membership information in its forwarding decisions.

Reverse Path Multicasting (RPM)

Reverse Path Multicasting (RPM) introduces an enhancement to RPB – an explicit method to prune branches of the spanning tree that have on active multicast group members for the source. RPM constructs a tree that spans only subnetworks with multicast group member and routers along the shortest path between the source and the destinations.

When a multicast router receives a multicast packet, it is forwarded using the RPB constructed spanning tree. Subsequent routers in the tree that have no active path to another router are referred to as leaf routers. If the multicast packet if forwarded to a leaf router that has no active multicast group members for the source, the leaf router will send a prune message to the previous router. This will remove the leaf router's branch from the spanning tree, and no more multicast packets (from that source) will be forwarded to it. Prune messages have a TTL equal to one, so they can be sent only one hop (one router) back toward the source. If the previous router receives prune messages from all of its branch and leaf routers, the previous router will then send it's own prune message back one router toward the multicast source, and the process will repeat. In this way, multicast group membership information can be used to prune the spanning tree between a given multicast source and the corresponding multicast group.

Since the membership of any given multicast group can change and the network topology can also change, RPM periodically removes all of the pruning information it has gathered from its memory, and the entire process repeats. This gives all subsequent routers on the network a chance to receive multicast packets from all multicast sources on the network. It also gives all users a chance to join a given multicast group.

Multicast Routing Protocols

This section contains an overview of two multicast routing protocols – Distance Vector Multicast Routing Protocol

(DVMRP), and Protocol Independent Multicast-Dense Mode (PIM-DM). The most commonly used routing protocol (not a multicast routing protocol), the Routing Information Protocol, is discussed in a later section.

Distance Vector Multicast Routing Protocol (DVMRP)

The Distance Vector Multicast Routing Protocol (DVMRP) was derived from the Routing Information Protocol (RIP) with the introduction of multicast delivery trees constructed from information about the 'distance' from the local router back toward the multicast source. DVMRP uses an RPM algorithm to construct its multicast delivery trees.

The first multicast packet received by a multicast router using DVMRP is flooded to all interfaces except the one on which the packet was received. Subsequent pruning messages are used to prune branches of the delivery tree that are either not on the shortest path back to the multicast source, or that have no active multicast group members. A 'graft' message is added that allows a previously pruned branch of the multicast delivery tree to be reactivated. This allows for lower latency when a leaf router adds a new member to a multicast membership group. Graft messages are forwarded one hop (one router) back at a time toward a multicast source until they reach a router that is on an active branch of the multicast delivery tree.

If there is more than one multicast router on a network, the one that has the shortest path back to the multicast source is elected to forward multicast packets from that source. All other routers will discard multicast packets from that source. If two multicast routers on a network have the same distance back to a multicast source, the router with the lowest IP address is elected.

DVMRP also supports tunnel interfaces, where two multicast routers are connected through a router that cannot process multicast packets. This allows multicast packets to cross networks with routers that are not multicast-aware.

Protocol-Independent Multicast – Dense Mode

There are two protocols in Protocol Independent Multicast (PIM), Protocol Independent Multicast-Dense Mode (PIM-DM) which is used when the multicast destinations are closely spaced, and Protocol Independent Multicast-Sparse Mode (PIM-SM) which is used when the multicast destinations are spaced further apart. PIM-DM is most commonly implemented in an intranetwork (LAN) where the distance between users is minimal.

Unicast Routing Protocols

Routing Information Protocol (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. The same format is used by both types.

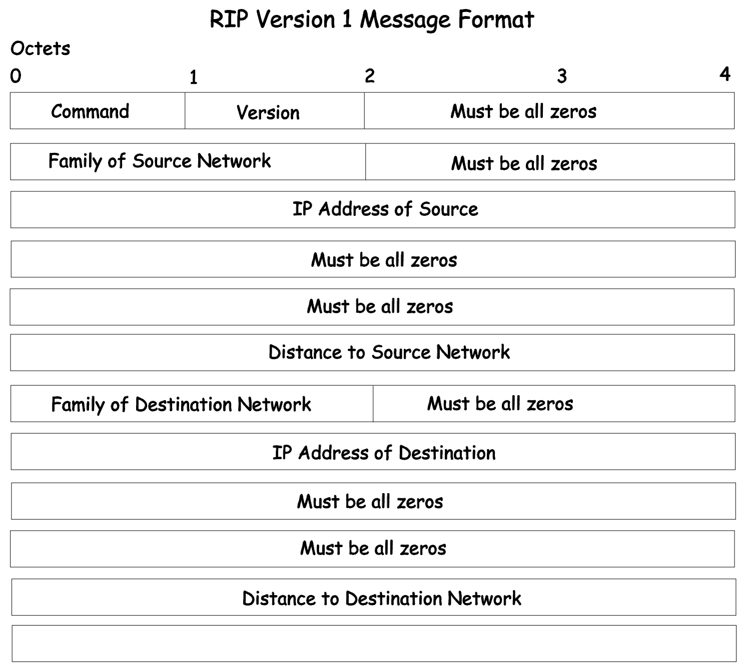


Figure 5- 15. RIP v.1 Message Format

The COMMAND field specifies an operation according the following table:

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

9	Update Request
10	Update Response
11	Update Acknowledgement

Table 5- 5. 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:

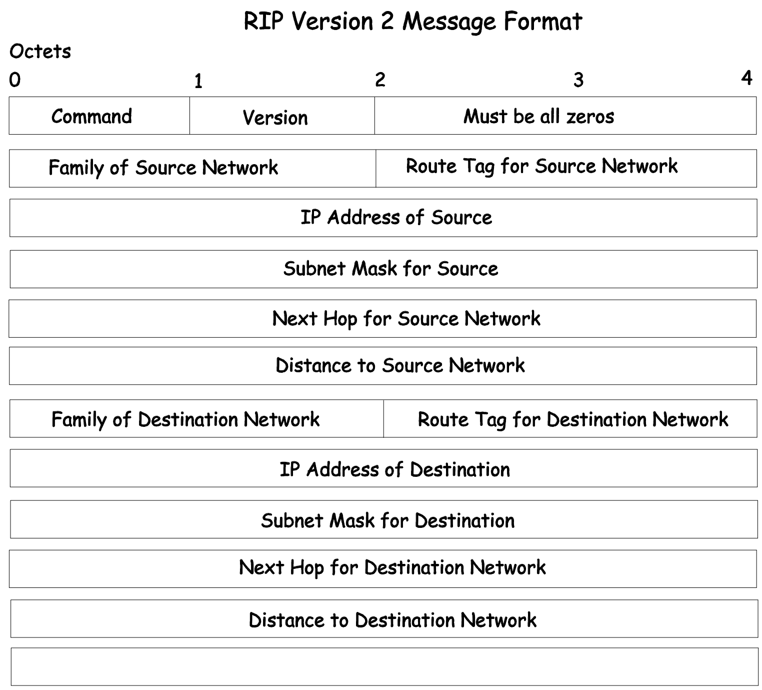


Figure 5- 16. RIP Message Format

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.

Open Shortest Path First (OSPF)

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

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

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

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

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

The Link-State Algorithm

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

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

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

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

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

The 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.

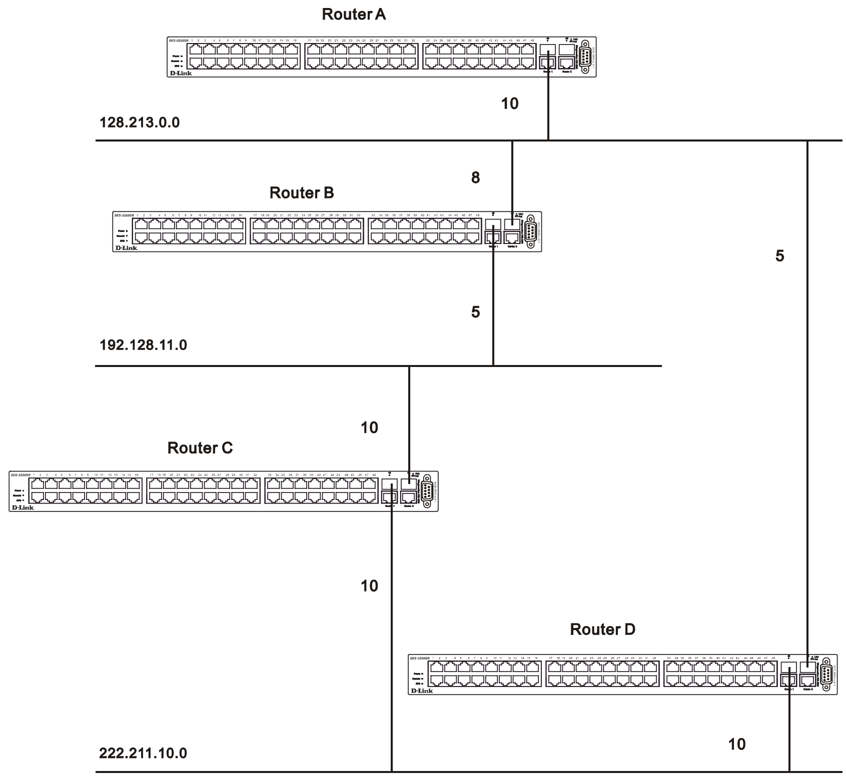


Figure 5- 17. Constructing a Shortest Path Tree

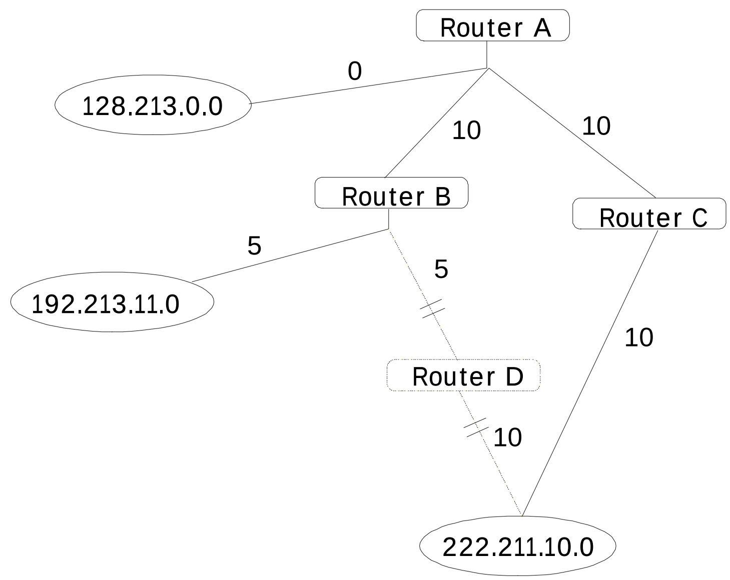


Figure 5- 18. Constructing a Shortest Path Tree

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

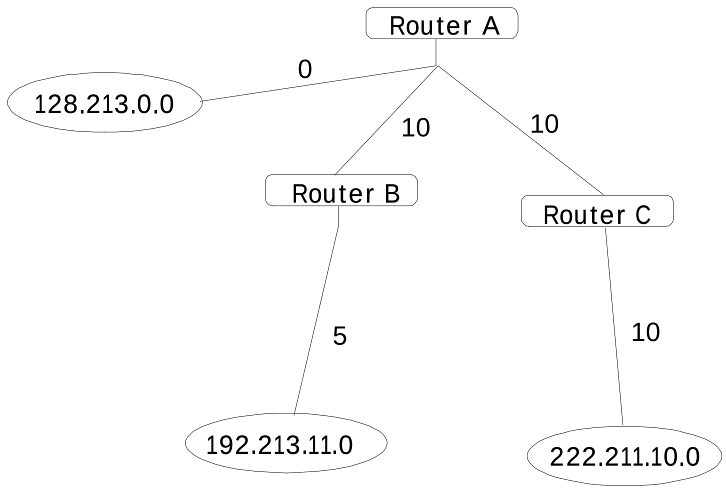


Figure 5- 19. Constructing a Shortest Path Tree - Completed

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

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

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

Areas and Border Routers

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

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

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

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

Link-State Packets

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

- Router Link-State Updates – these describe a router's links to destinations within an area.
- Summary Link-State Updates – issued by Border Routers and describe links to networks outside the area but within the Autonomous System (AS).
- Network Link-State Updates – issued by multi-access areas that have more than one attached router. One router is elected as the Designated

Router (DR) and this router issues the network link-state updates describing every router on the segment.

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

The format of these link-state updates are 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).

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.

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.

The Backbone and Area 0

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

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

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

Virtual Links

Virtual links accomplish two purposes:

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

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

Areas Not Physically Connected to Area 0

All areas of an OSPF network should have a physical connection to the backbone, but 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
- The Link-State Update packet
- Link-State Acknowledgment packet

The OSPF Packet Header

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

The format of the OSPP packet header is shown below:

OSPF Packet Header

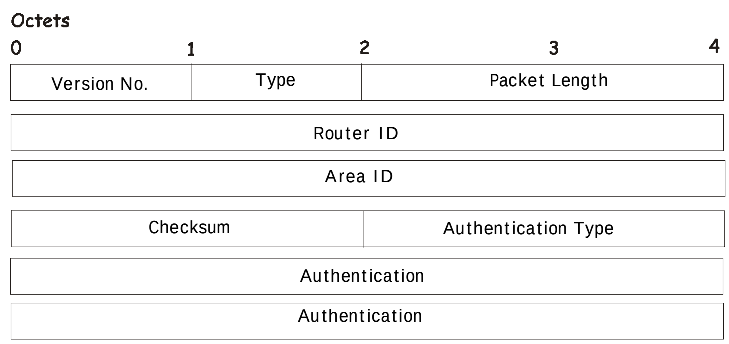


Figure 5- 20. OSPF Packet Header

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

	1 Hello 2 Database Description 3 Link-State Request 4 Link-State Update 5 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.

Table 5- 6. OSPF Packet Header

The Hello Packet

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

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

The format of the Hello packet is shown below:

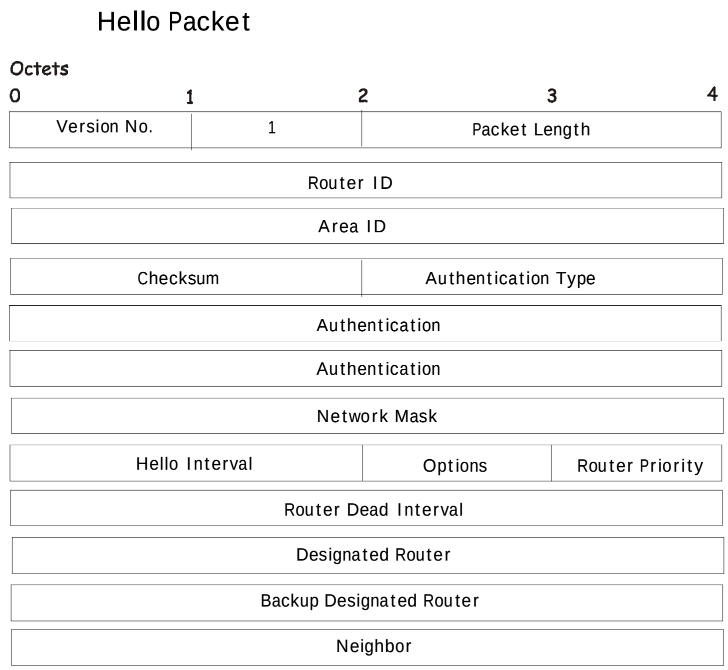


Figure 5- 21. Hello Packet

Field	Description
Network Mask	The network mask associated with this interface.
Options	The optional capabilities supported by the router.
Hello Interval	The number of seconds between this router's Hello packets.
Router Priority	This router's Router Priority. The Router Priority is used in the election of the DR and

	BDR. If this field is set to 0, the router is ineligible to become the DR or the BDR.
Router Dead Interval	The number of seconds that must pass before declaring a silent router as down.
Designated Router	The identity of the DR for this network, in the view of the advertising router. The DR is identified here by its IP interface address on the network.
Backup Designated Router	The identity of the Backup Designated Router (BDR) for this network. The BDR is identified here by its IP interface address on the network. This field is set to 0.0.0.0 if there is no BDR.
Neighbor	The Router Ids of each router from whom valid Hello packets have been seen within the Router Dead Interval on the network.

Table 5- 7. Hello Packet

The Database Description Packet

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

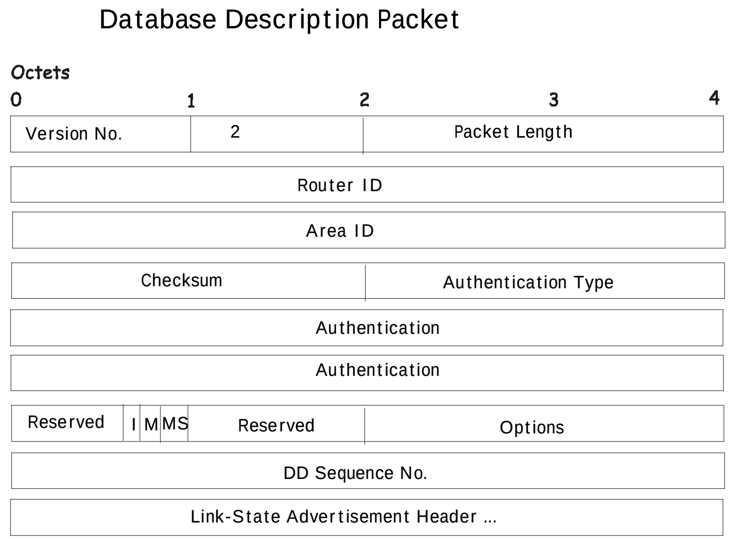


Figure 5- 22. Database Description Packet

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.

Table 5- 8. Database Description Packet

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.

The Link-State Request Packet

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

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

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

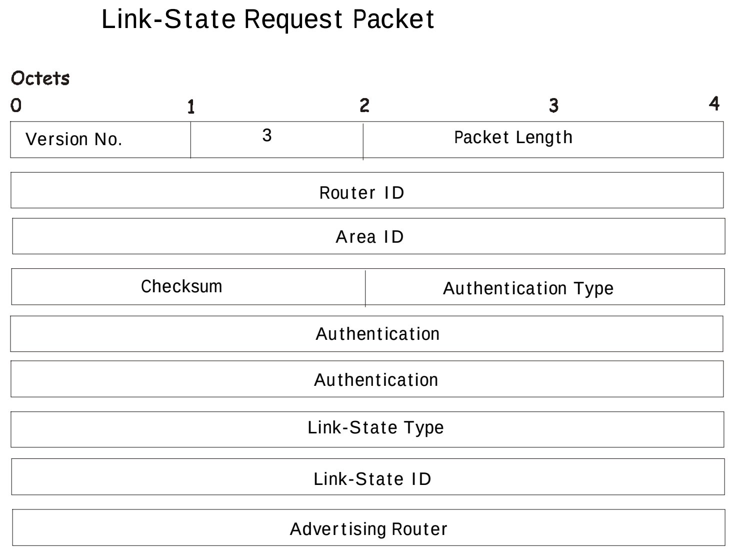


Figure 5- 23. Link-State Request Packet

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.

The Link-State Update Packet

Link-State Update packets are OSPF packet type 4. These packets implement the flooding of link-state advertisements.

Each Link-State Update packet carries a collection of link-state advertisements one hop further from its origin. Several link-state advertisements may be included in a single packet.

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

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

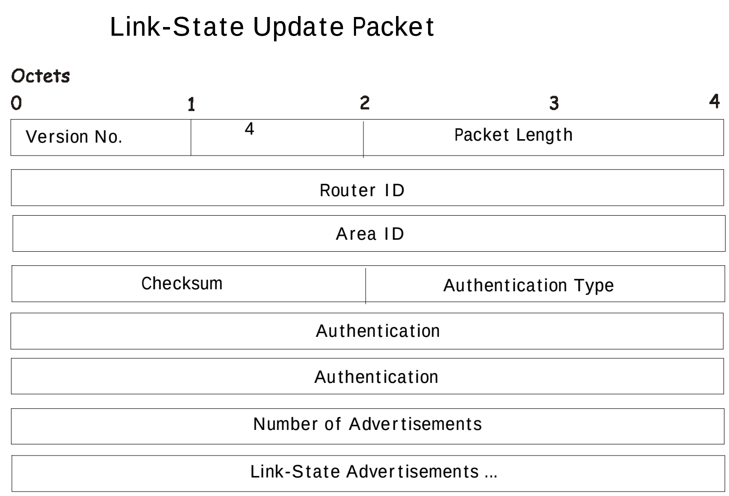


Figure 5- 24. Link-State Update Packet

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.

The Link-State Acknowledgment Packet

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

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

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

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

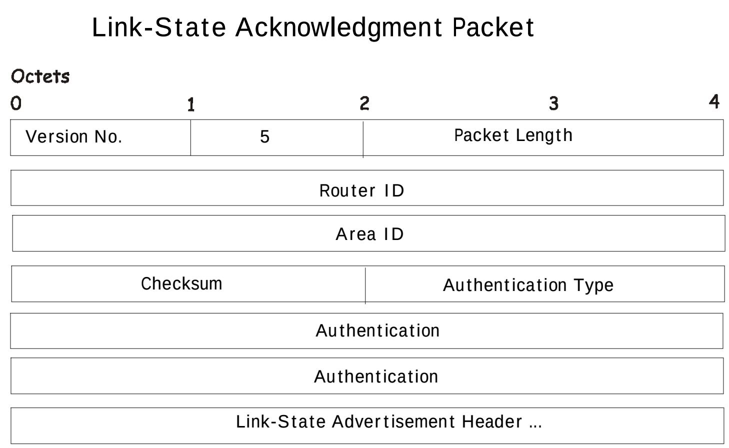


Figure 5- 25. Link-State Acknowledgement Packet

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

The Link State Advertisement Header

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

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

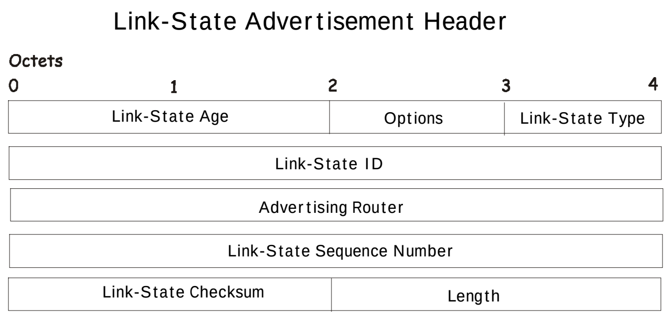


Figure 5- 26. Link-State Advertisement Header

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: Type Description 1 Router Links 2 Network Links 3 Summary Link (IP Network) 4 Summary Link (ASBR) 5 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 excepting the Link State Age field.
Length	The length in bytes of the link state advertisement. This includes the 20-byte link state advertisement header.

Table 5- 9. Link-State Advertisement Header

Router Links Advertisements

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

The format of the Router Links Advertisement is shown below:

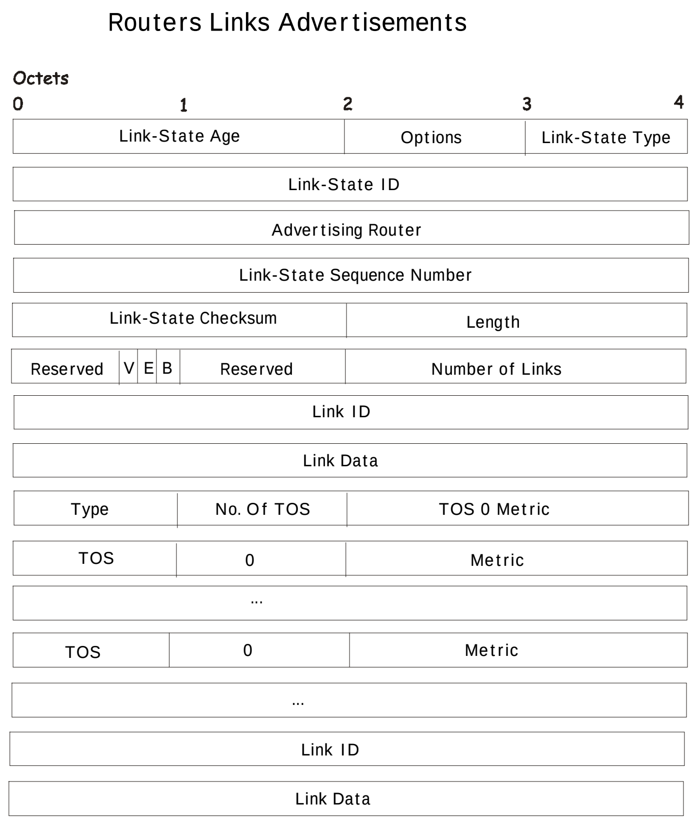


Figure 5- 27. Routers Links Advertisement

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

Field	Description

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.

Table 5- 10. Routers Links Advertisement

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 1 Point-to-point connection to another router. 2 Connection to a transit network. 3 Connection to a stub network. 4 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 1 Neighboring router's Router ID. 2 IP address of Designated Router. 3 IP network/subnet number. 4 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.

Table 5- 11. Routers Links Advertisements – Continued

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.

Table 5- 12. Routers Links Advertisement – Continued

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:

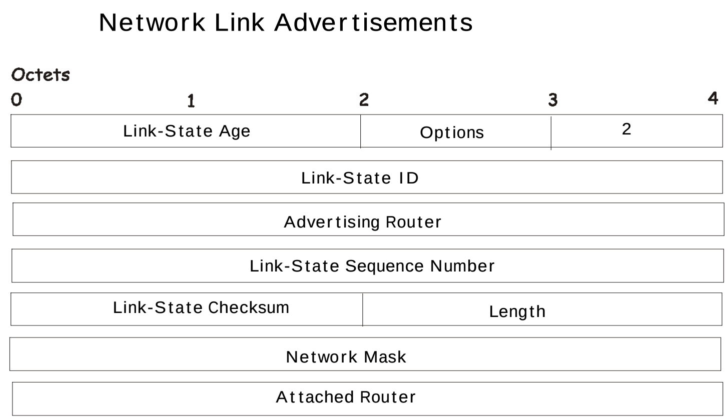


Figure 5- 28. Network Link Advertisement

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.

Table 5- 13. Network Link Advertisement

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.

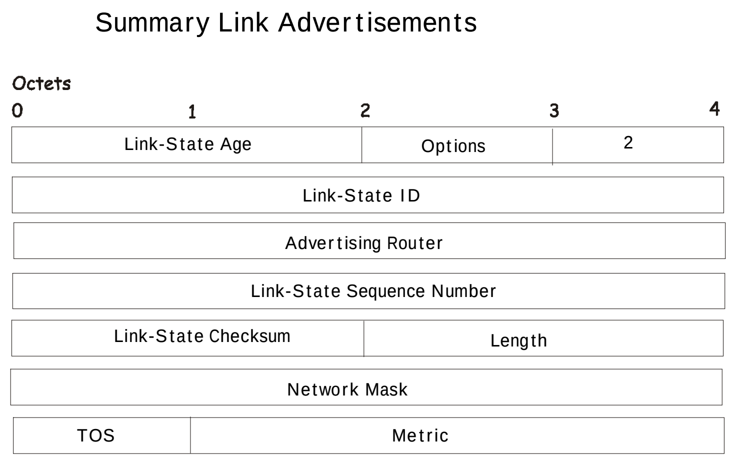


Figure 5- 29. Summary Link Advertisement

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.

Table 5- 14. Summary Link Advertisement

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

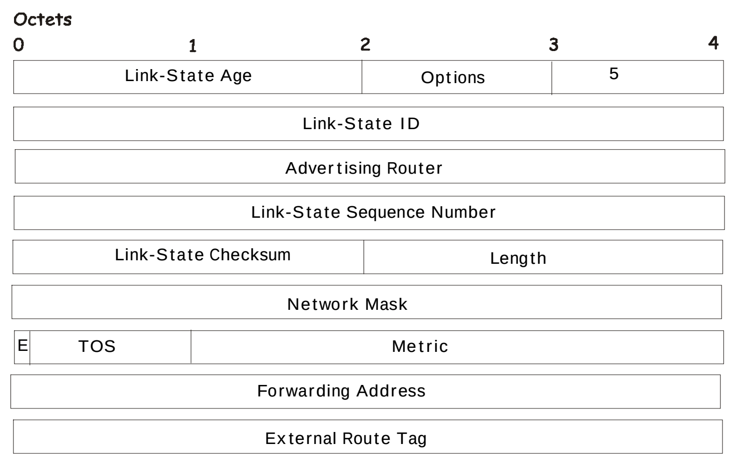


Figure 5- 30. AS External Link Advertisement

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.

Table 5- 15. AS External System Advertisement

6

WEB-BASED SWITCH MANAGEMENT

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).*

Before You Start

The DES-3350SR switch supports a wide array of functions and gives great flexibility and increased network performance by eliminating the routing bottleneck between the WAN or Internet and the Intranet. Its function in a network can be thought of as a new generation of router that performs routing functions in hardware, rather than software. It is a router that also has up to 48+2 independent Ethernet collision domains.

This flexibility and rich feature set requires a bit of thought to arrive at a deployment strategy that will maximize the potential of the DES-3350SR.

General Deployment Strategy

1. Determine how the network would be best segmented. This is probably done using VLANs in an existing layer 2 switched network.
2. Develop an IP addressing scheme. This involves allocating a block of IP addresses to each network segment. Each network subnet is then assigned a network address and a subnet mask. See Chapter 5's "IP Addressing and Subnetting" section for more information.
3. Determine which network resources must be shared by the subnets. Shared resources may be connected directly to the Layer 3 switch, if need be. Static routes to each of the shared resources should be determined.
4. Determine how each subnet will communicate with the WAN or Internet. Again, static routes should be determined and default gateways identified.

5. Develop a security scheme. Some subnets on the network need more security or should be isolated from the other subnets. IP or MAC filtering can be used. Also, one or more VLANs on the Layer 3 switch can be configured without an IP subnet – in which case, these VLANs will function as a layer 2 VLAN and would require an external router to connect to the rest of the network.
6. Develop a policy scheme. Some subnets will have a greater need for multicasting bandwidth, for example. A policy is a mechanism to alter the normal packet forwarding in a network device, and can be used to intelligently allocate bandwidth to time-critical applications such as the integration of voice, video, and data on the network.
7. Develop a redundancy scheme. Planning redundant links and routes to network critical resources can save valuable time in case of a link or device failure. The DES-3350SR Spanning Tree function can be used to block the redundant link until it is needed.

VLAN Layout

VLANs on the DES-3350SR have rather more functions than on a traditional layer 2 switch, and must therefore be laid-out and configured with a bit more care. VLANs with an IP interface assigned to them could be thought of as network links – not just as a collection of associated end users. Further, VLANs assigned an IP network address and subnet mask enables IP routing between them.

VLANs must be configured on the switch before they can be assigned IP subnets. Further, the static VLAN configuration is specified on a per port basis. On the DES-3350SR, a VLAN can consist of end-nodes – just like a traditional layer 2 switch, but a VLAN can also consist of one or more layer 2 switches – each of which is connected to multiple end-nodes or network resources.

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

Assigning IP Network Addresses and Subnet Masks to VLANs

The DES-3350SR allows the assignment of IP subnets to individual VLANs.

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

Defining Static Routes

Routes between the IP interfaces and a default gateway or other router with a WAN connection should be determined beforehand and entered into the static/default routing table on the DES-3350SR.

Getting Started

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.

Configuring the Switch

User Accounts Management

From the **Management** menu, click **User Accounts** and then

Figure 6- 2. User Account Management window

Click **Add** to add a user.

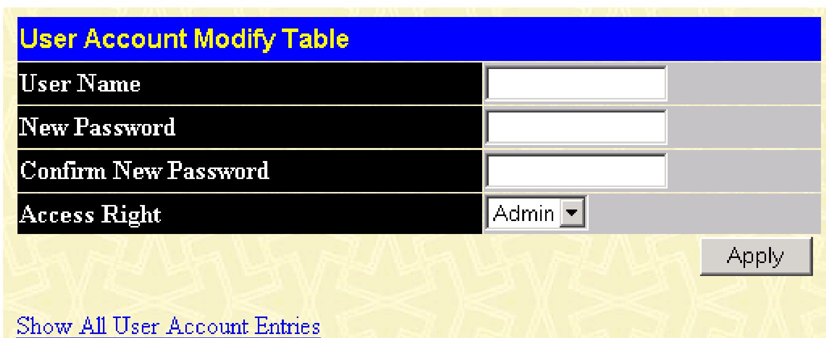


Figure 6- 3. User Account Modify Table window

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** window on the **Maintenance** 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 Management	***Privilege***	
	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:

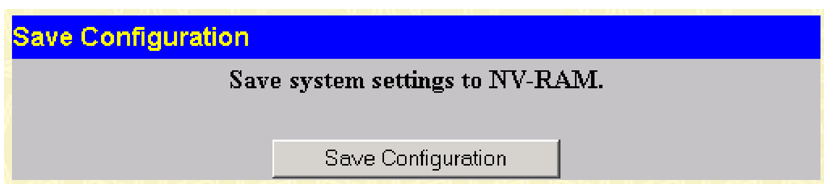


Figure 6- 4. Save Configuration window

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.

Using Web-Based Management

Setting up Web Management

Before running Web-based management, some basic configuration of the switch may need to be performed. The following at a minimum must be configured or known for the switch to be managed:

- IP Address
- Subnet Mask
- Administrator password

In addition, several other parameters may need to be configured or known to properly communicate with the switch or allow full management capability. These include:

- Default Gateway
- Trap Destination and Community Name

Configuration of these items may be made from the User Interface, which is accessible via either the serial console or Telnet. Refer to the User's Guide that came with your system for more information about the subsection describing the required configuration.

Setting an IP Address

The IP address for the switch must be set before it can be managed with the Web-based manager. The switch IP address may 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 alternatively be set using the Command Line Interface (CLI) over the console serial port as follows:

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

2. Alternatively, you can enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/z** at the command line prompt. 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.

Using this method, 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 Web-based management agent.

Saving Configuration Changes

Clicking the **Apply** button makes any configuration change active, but only for the current session. If the switch is restarted (rebooted) without entering the configuration changes into the non-volatile RAM (NV-RAM), the configuration changes will be lost.

To enter configuration changes into the switch's non-volatile RAM, select **Save Changes** from the **Maintenance** menu. Click on the **Save Configuration** button to enter the current configuration into NV-RAM. The configuration will then be loaded into the switch's memory when it is restarted.

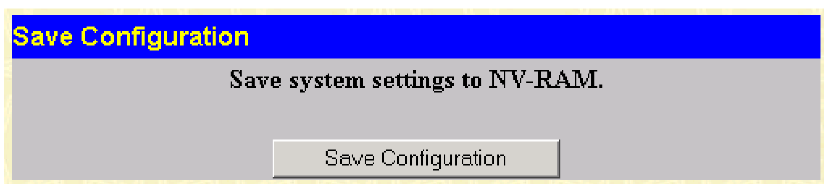


Figure 6- 6. Save Configuration window

Starting and Stopping the Web-based Manager

Do the following to use the Web-based manager:

1. Start a Java-enabled Web browser from any machine with network access to the switch. (Preferred browsers include Opera, Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above.)

2. Enter the IP address for the switch you want to manage in the URL field of the browser.

3. The screen below will appear, prompting you to enter the user name and password for management access.

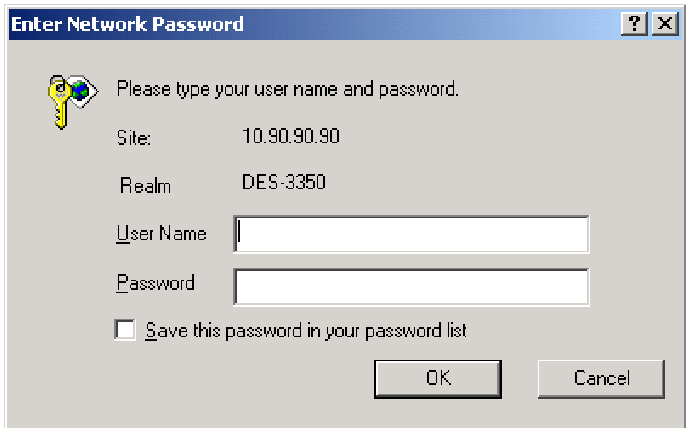


Figure 6- 7. Password dialog box

4. There is no default User Name or Password. Click the **OK** button to continue. The default user has *Admin* privileges.

5. The full application will now launch. A three-frame page will display with a switch graphic located in the upper right hand frame.

6. To stop the Web-based manager, simply close the Web browser application.

Web-based Manager's User Interface

The user interface provides access to various switch configuration and management screens, allows you to view performance statistics, and permits you to graphically monitor the system status.

Areas of the User Interface

The figure below shows the user interface. The user interface is divided into 3 distinct areas as described in the table.

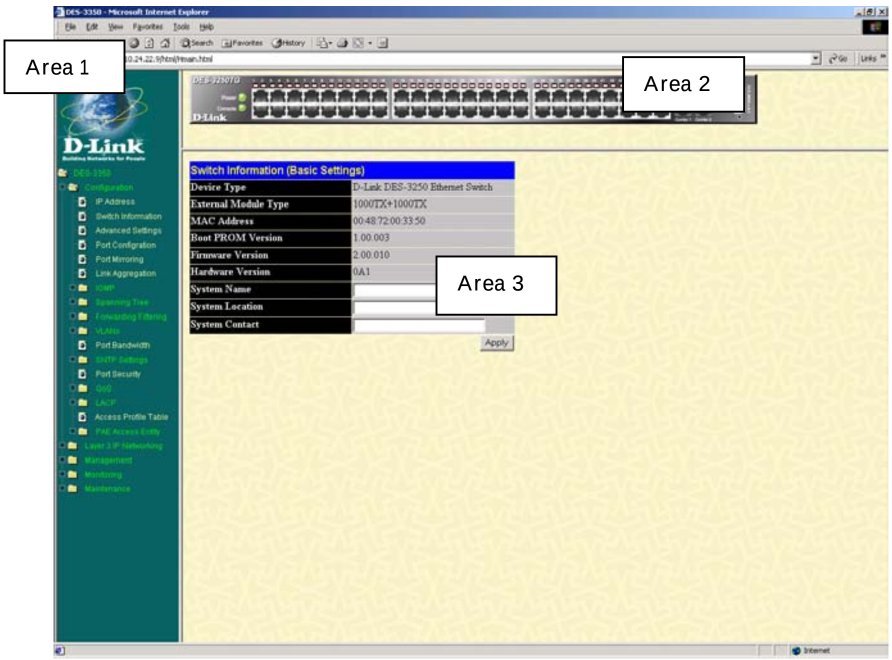


Figure 6- 8. Main Web-Manager window

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.

This section, arranged by topic, describes how to perform common monitoring and configuration tasks on the DES-3350SR switch using the Web-based Manager, you can perform any of the tasks described in the following sections.

Configuration

The **Configuration** menu consists of the following folders and screens: **IP Address**, **Switch Information**, **Advanced Settings**, **Port Configuration**, **Port Mirroring**, **IGMP**, **Spanning Tree**, **Forwarding Filtering**, **VLANs**, **Port Bandwidth**, **SNTP Settings**, **Port Security**, **QoS**, **LACP**, **Access Profile Table**, and **PAE Access Entity**. See below for further description.

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:

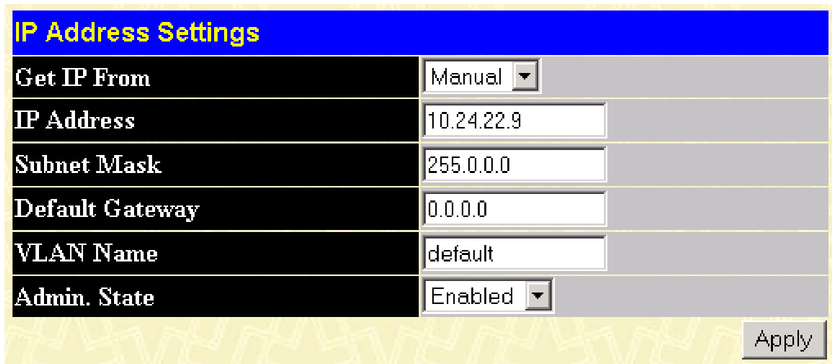


Figure 6- 9. IP Address Settings window

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:

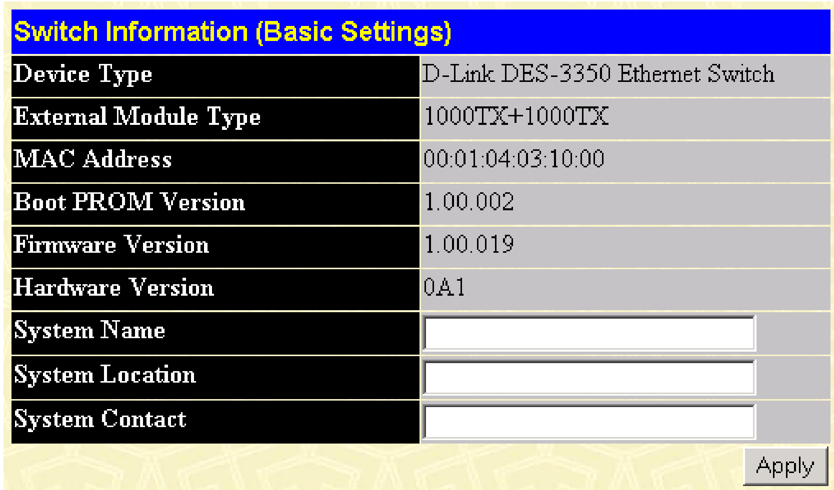
Parameter	Description
BOOTP	The switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it 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:
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 ID number 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.

Switch Information

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



Switch Information (Basic Settings)	
Device Type	D-Link DES-3350 Ethernet Switch
External Module Type	1000TX+1000TX
MAC Address	00:01:04:03:10:00
Boot PROM Version	1.00.002
Firmware Version	1.00.019
Hardware Version	0A1
System Name	
System Location	
System Contact	
	Apply

Figure 6- 10. 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** 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:

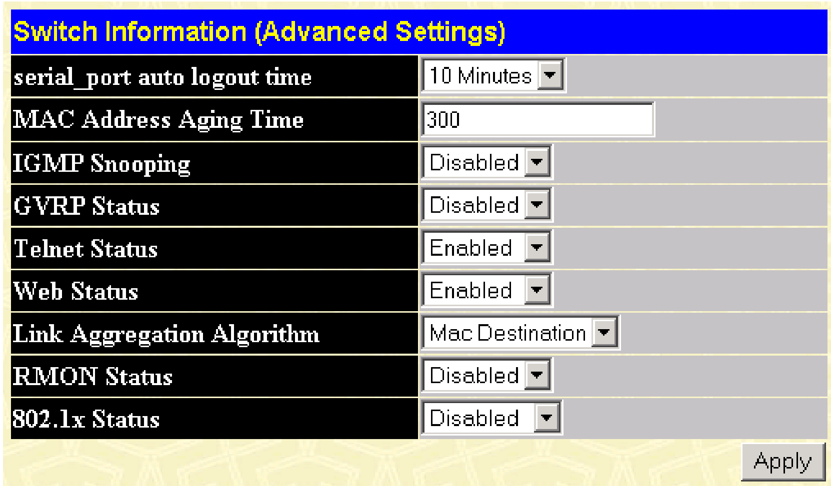


Figure 6- 11. Switch Information (Advanced Settings) window

The following fields can be set:

Parameter	Description
Serial_port auto logout time<*Never*>	Set the age out timer for the serial port to *2 minutes*, *5 minutes*, *10 minutes*, *15 minutes*, or *Never*.
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	IGMP Snooping allows the switch to

<*Disabled*>	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 <*Disabled*>	To disable 802.1x port access control, toggle to *Disabled*. Otherwise, select either *Port Base* or *Mac Base*.

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	Link Down
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	Link Down
14	Enabled	Auto	Link Down
15	Enabled	Auto	Link Down
16	Enabled	Auto	Link Down
17	Enabled	Auto	Link Down
18	Enabled	Auto	Link Down
19	Enabled	Auto	Link Down
20	Enabled	Auto	Link Down
21	Enabled	Auto	Link Down
22	Enabled	Auto	Link Down
23	Enabled	Auto	100M/Full
24	Enabled	Auto	Link Down
25	Enabled	Auto	Link Down
26	Enabled	Auto	Link Down
27	Enabled	Auto	Link Down
28	Enabled	Auto	Link Down
29	Enabled	Auto	Link Down
30	Enabled	Auto	Link Down

31	Enabled	Auto	100M/Full
32	Enabled	Auto	Link Down
33	Enabled	Auto	Link Down
34	Enabled	Auto	Link Down
35	Enabled	Auto	Link Down
36	Enabled	Auto	Link Down
37	Enabled	Auto	Link Down
38	Enabled	Auto	Link Down
39	Enabled	Auto	Link Down
40	Enabled	Auto	Link Down
41	Enabled	Auto	Link Down
42	Enabled	Auto	Link Down
43	Enabled	Auto	Link Down
44	Enabled	Auto	Link Down
45	Enabled	Auto	Link Down
46	Enabled	Auto	Link Down
47	Enabled	Auto	Link Down
48	Enabled	Auto	Link Down
49	Enabled	Auto	Link Down
50	Enabled	Auto	Link Down

Figure 6- 12. 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.

Note: *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

To configure a port for port mirroring:

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

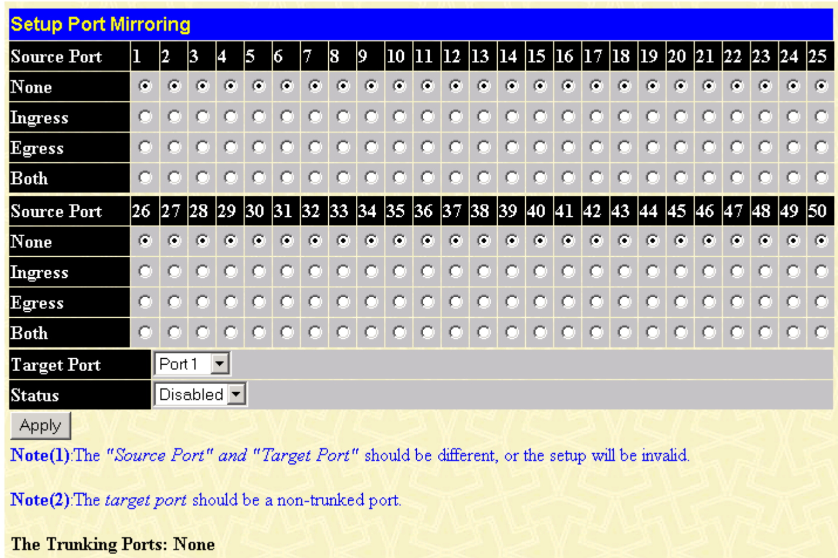


Figure 6- 13. Setup Port Mirroring window

The target port is where information will be duplicated and sent for capture and network analysis. This is the port where a network analyzer would be attached 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

To configure IGMP Snooping:

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

Current IGMP Snooping Group Entries				
VLAN ID	VLAN Name	State	Querier State	Modify
1	default	Disabled	Disabled	Modify

Figure 6- 14. Current IGMP Snooping Group Entries window

To edit an IGMP Snooping entry on the switch, click the pointer icon next to the entry on the Current IGMP Snooping Group Entries window:

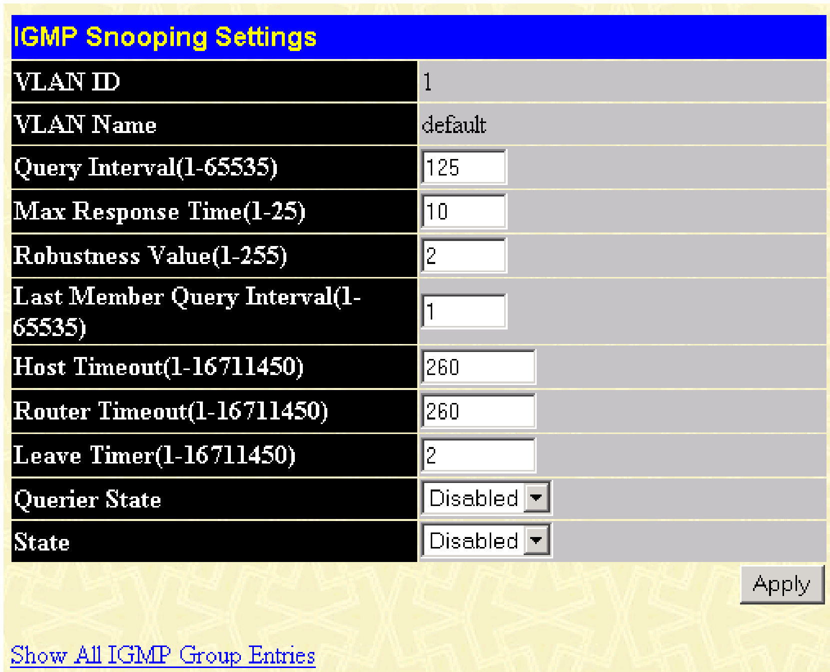


Figure 6- 15. IGMP Snooping Settings window

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(1-25)	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(1-255)	A tuning variable to allow for VLANs that are expected to lose a large number of packets. A value between *1* and *255* can be entered, with larger values being specified for VLANs that are expected to lose larger numbers of packets.
Last Member Query Interval(1-65535)	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 Port Settings

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

A router port has the following behavior:

- All IGMP Report packets will be forwarded to the router port.
- IGMP queries (from the router port) will be flooded to all ports.
- All UDP multicast packets will be forwarded to the router port. Because routers do not send IGMP reports or implement IGMP snooping, a multicast router connected to the router port of 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.

To setup a static router port:

Click **Static Router Ports Entry** under the **IGMP** folder on the **Configuration** menu:

Current Static Router Ports Entries

VLAN ID	VLAN Name	Modify
1	default	Modify

Figure 6- 16. Current Static Router Ports Entries window

To add a static router port configuration, click the pointer icon:

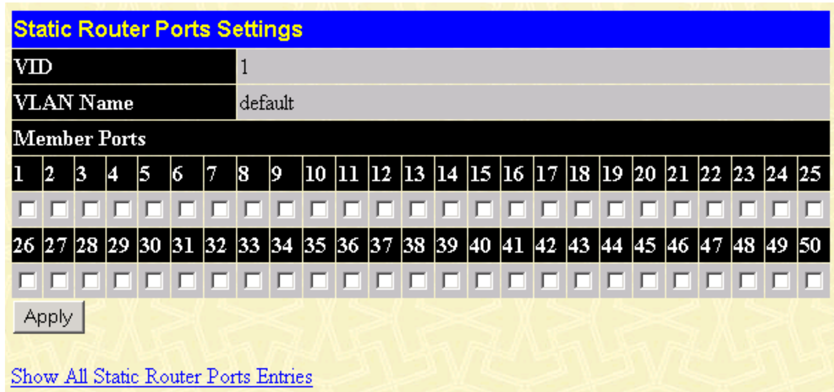


Figure 6- 17. Static Router Ports Settings window

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

STP Switch Settings

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

To globally configure STP on the switch, click the Spanning Tree folder, and then the STP Switch Settings link:

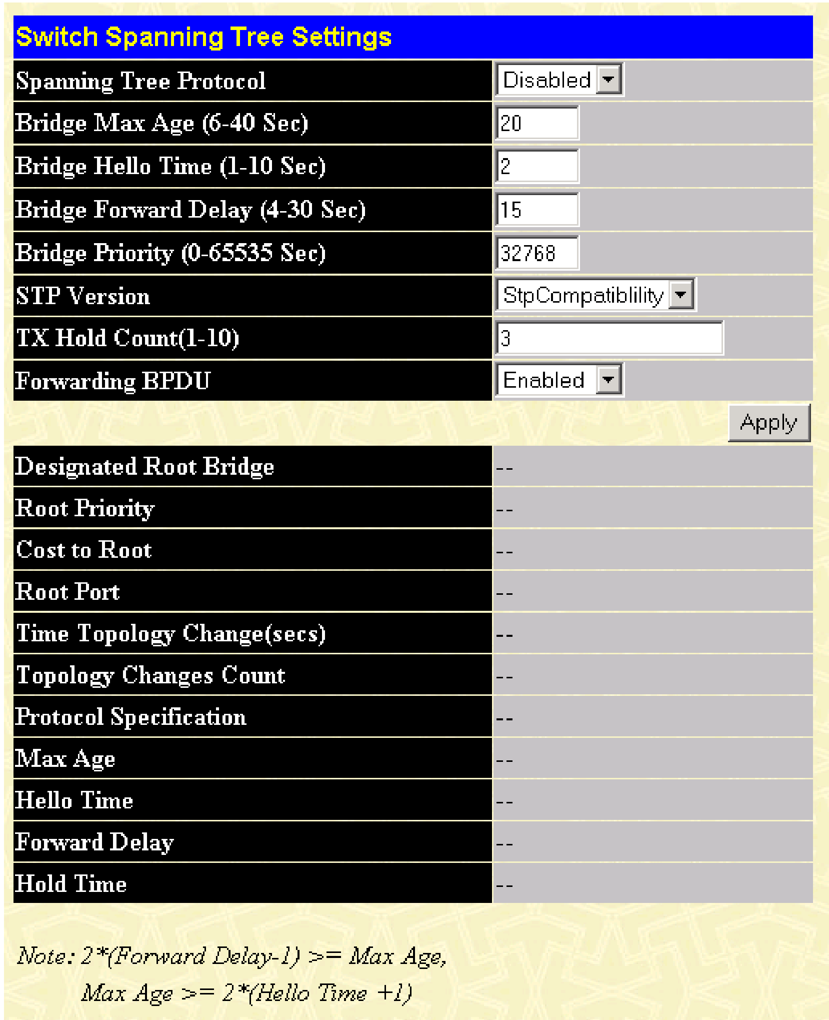


Figure 6- 18. Switch Spanning Tree Settings window

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	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 (default) or STP Compatibility. Both versions use STP parameters in the same way. RSTP is fully compatible with IEEE 802.1d STP and will function with legacy equipment.
TX Hold Count(1-10) <*3*>	This is the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default value is *3*.
Forwarding BPDU <*Enabled*>	This 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:

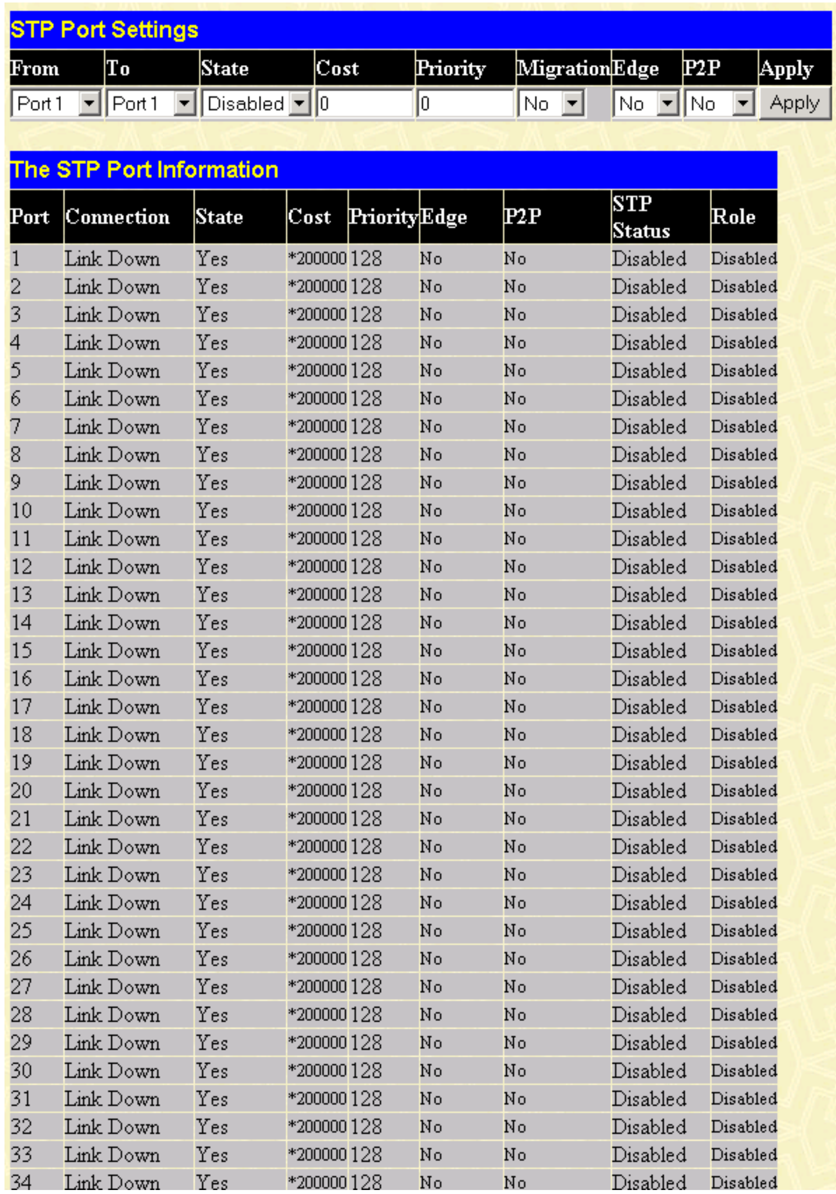
Max. Age ≤ 2 x (Forward Delay - 1 second)

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 on a per user-defined group of ports basis, 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	0	0	No	No	No	Apply

The STP Port Information

Port	Connection	State	Cost	Priority	Edge	P2P	STP Status	Role
1	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
2	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
3	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
4	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
5	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
6	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
7	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
8	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
9	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
10	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
11	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
12	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
13	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
14	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
15	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
16	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
17	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
18	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
19	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
20	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
21	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
22	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
23	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
24	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
25	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
26	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
27	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
28	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
29	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
30	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
31	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
32	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
33	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
34	Link Down	Yes	*200000	128	No	No	Disabled	Disabled

35	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
36	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
37	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
38	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
39	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
40	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
41	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
42	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
43	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
44	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
45	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
46	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
47	100M/Full	Yes	*200000	128	No	No	Forwarding	NonStp
48	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
49	Link Down	Yes	*200000	128	No	No	Disabled	Disabled
50	Link Down	Yes	*200000	128	No	No	Disabled	Disabled

Figure 6- 19. 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**	Select the range of ports that will make up the STP Group.
State<*Disabled*>	Toggle to enable STP on the selected ports.
Cost(1~200000000)	A Port Cost can be set from *1* to *200000*. The lower the number, the greater the probability the port will be chosen to forward packets.
Priority(0~240)	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. False 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

Forwarding Filtering

Unicast Forwarding

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

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 Forwarding:

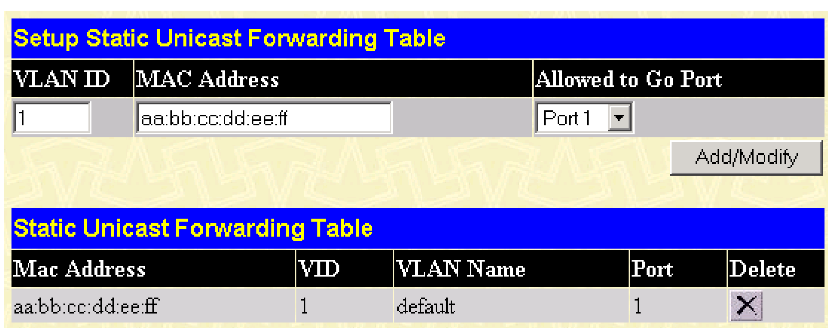


Figure 6- 20. Setup Static Unicast Forwarding Table window

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 Configuration menu and then click Multicast Forwarding:

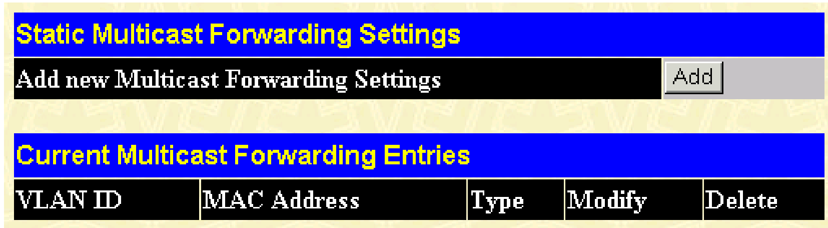


Figure 6- 21. Static Multicast Forwarding Settings window

To add a new multicast MAC address to the switch's forwarding table, click the Add button:

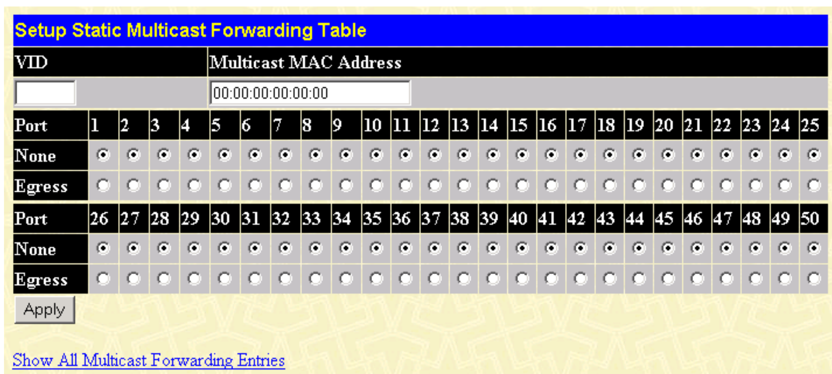


Figure 6- 22. Setup Static Multicast Forwarding Table window

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.
Type	Only Static multicast forwarding entries can be entered in this version

	of the switch.
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

***To create a new 802.1Q VLAN**:*

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:

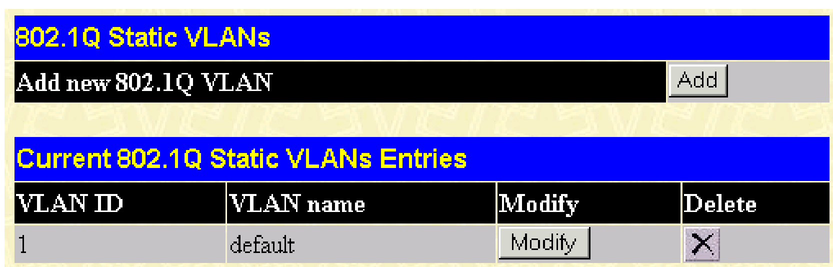


Figure 6- 23. 802.1Q Static VLANs window

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

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

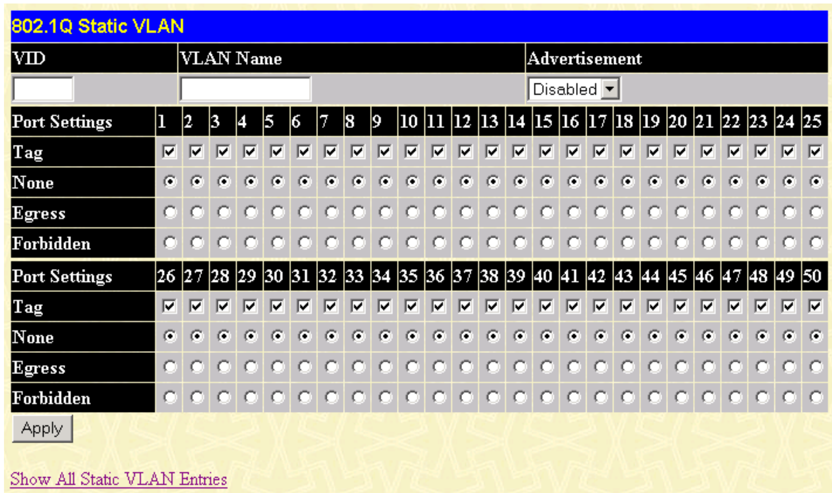


Figure 6- 24. (Add) 802.1Q Static VLAN window

To edit an existing 802.1Q VLAN, click the corresponding pointer icon in the Modify column on the 802.1Q Static Vlans window. The following window will open:

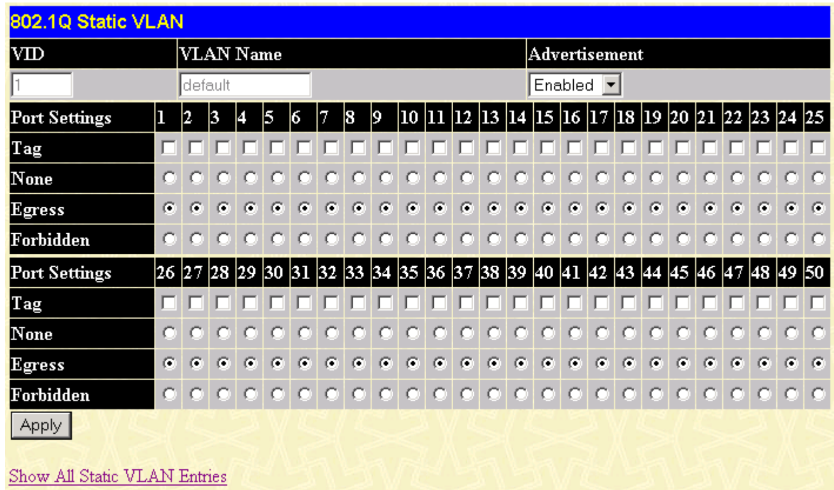


Figure 6- 25. (Modify) 802.1Q Static VLAN window

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	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.

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 can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port.

802.1Q Port Settings

From	To	GVRP	Ingress	Apply
Port 1	Port 1	Disabled	Disabled	Apply

802.1Q Port Table

Port	PVID	GVRP	Ingress Checking
1	1	Enabled	Disabled
2	1	Enabled	Disabled
3	1	Enabled	Disabled
4	1	Enabled	Disabled
5	1	Enabled	Disabled
6	1	Enabled	Disabled
7	1	Enabled	Disabled
8	1	Enabled	Disabled
9	1	Enabled	Disabled
10	1	Enabled	Disabled
11	1	Enabled	Disabled
12	1	Enabled	Disabled
13	1	Enabled	Disabled
14	1	Enabled	Disabled
15	1	Enabled	Disabled
16	1	Enabled	Disabled
17	1	Enabled	Disabled
18	1	Enabled	Disabled
19	1	Enabled	Disabled
20	1	Enabled	Disabled
21	1	Enabled	Disabled
22	1	Enabled	Disabled
23	1	Enabled	Disabled
24	1	Enabled	Disabled
25	1	Enabled	Disabled
26	1	Enabled	Disabled
27	1	Enabled	Disabled
28	1	Enabled	Disabled
29	1	Enabled	Disabled
30	1	Enabled	Disabled

31	1	Enabled	Disabled
32	1	Enabled	Disabled
33	1	Enabled	Disabled
34	1	Enabled	Disabled
35	1	Enabled	Disabled
36	1	Enabled	Disabled
37	1	Enabled	Disabled
38	1	Enabled	Disabled
39	1	Enabled	Disabled
40	1	Enabled	Disabled
41	1	Enabled	Disabled
42	1	Enabled	Disabled
43	1	Enabled	Disabled
44	1	Enabled	Disabled
45	1	Enabled	Disabled
46	1	Enabled	Disabled
47	1	Enabled	Disabled
48	1	Enabled	Disabled
49	1	Enabled	Disabled
50	1	Enabled	Disabled

Figure 6- 26. 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.

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.

To access the Port Bandwidth Settings window, click Port Bandwidth in the Configuration folder:

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

31	no_limit	no_limit
32	no_limit	no_limit
33	no_limit	no_limit
34	no_limit	no_limit
35	no_limit	no_limit
36	no_limit	no_limit
37	no_limit	no_limit
38	no_limit	no_limit
39	no_limit	no_limit
40	no_limit	no_limit
41	no_limit	no_limit
42	no_limit	no_limit
43	no_limit	no_limit
44	no_limit	no_limit
45	no_limit	no_limit
46	no_limit	no_limit
47	no_limit	no_limit
48	no_limit	no_limit
49	no_limit	no_limit
50	no_limit	no_limit

Figure 6- 27. 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 (NPT). 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.

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

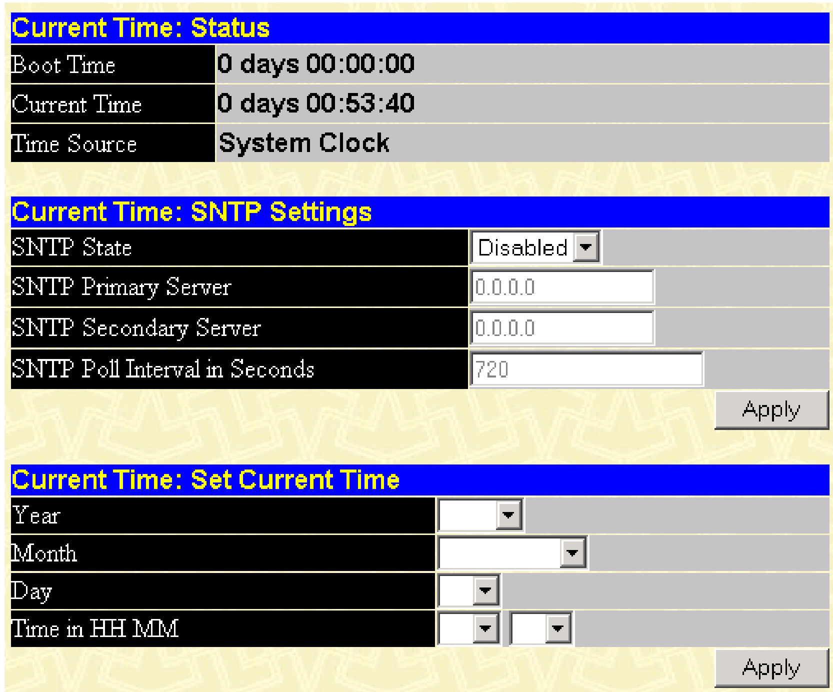


Figure 6- 28. Current Time window

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**.

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:

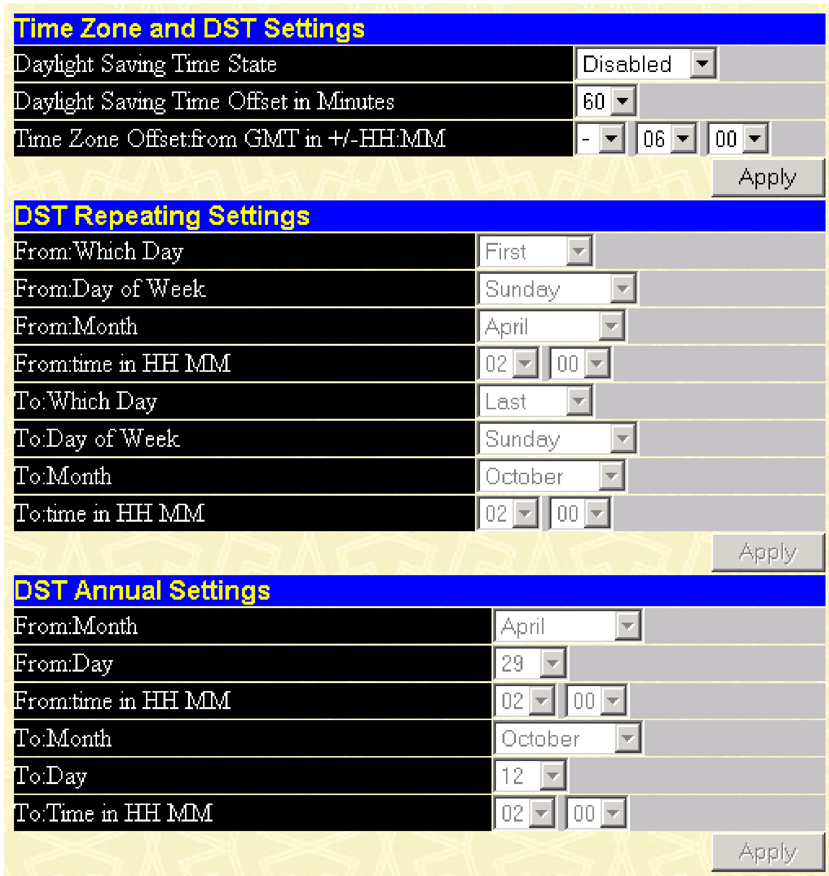


Figure 6- 29. Time Zone and DST Settings window

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 (or ports) from connecting to the switch's locked ports and gaining access to the network.

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
32	Disabled	1	DeleteOnReset
33	Disabled	1	DeleteOnReset
34	Disabled	1	DeleteOnReset
35	Disabled	1	DeleteOnReset
36	Disabled	1	DeleteOnReset
37	Disabled	1	DeleteOnReset
38	Disabled	1	DeleteOnReset
39	Disabled	1	DeleteOnReset
40	Disabled	1	DeleteOnReset

41	Disabled	1	DeleteOnReset
42	Disabled	1	DeleteOnReset
43	Disabled	1	DeleteOnReset
44	Disabled	1	DeleteOnReset
45	Disabled	1	DeleteOnReset
46	Disabled	1	DeleteOnReset
47	Disabled	1	DeleteOnReset
48	Disabled	1	DeleteOnReset
49	Disabled	1	DeleteOnReset
50	Disabled	1	DeleteOnReset

Figure 6- 30. Port Security Settings window

The following fields can be set:

Parameter	Description
From and **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 Address.(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	Select *Delete On Timeout* to clear dynamic entries for the ports on timeout of the Forwarding Data Base

<*Delete On Reset*>	(FDB). Specify *Delete On Reset* to delete all FDB entries, including static entries upon system reset or rebooting.

QOS

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.

Configuring QOS Output Scheduling

Click QoS on the Configuration menu, and then click scheduling:

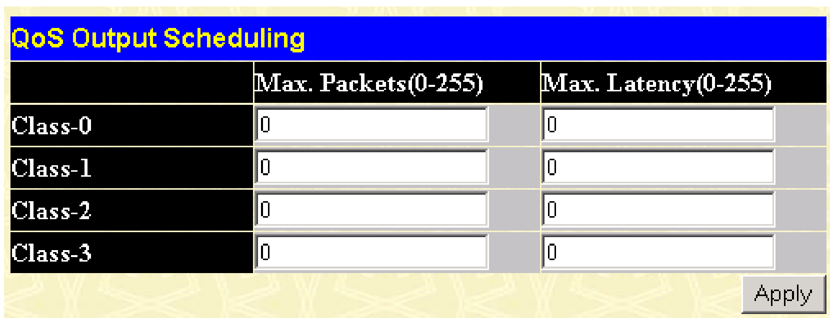


Figure 6- 31. QoS Output Scheduling window

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.

Configuring 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	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	0
25	0
26	0
27	0
28	0
29	0
30	0

31	0
32	0
33	0
34	0
35	0
36	0
37	0
38	0
39	0
40	0
41	0
42	0
43	0
44	0
45	0
46	0
47	0
48	0
49	0
50	0

Figure 6- 32. 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.

Configuring 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:

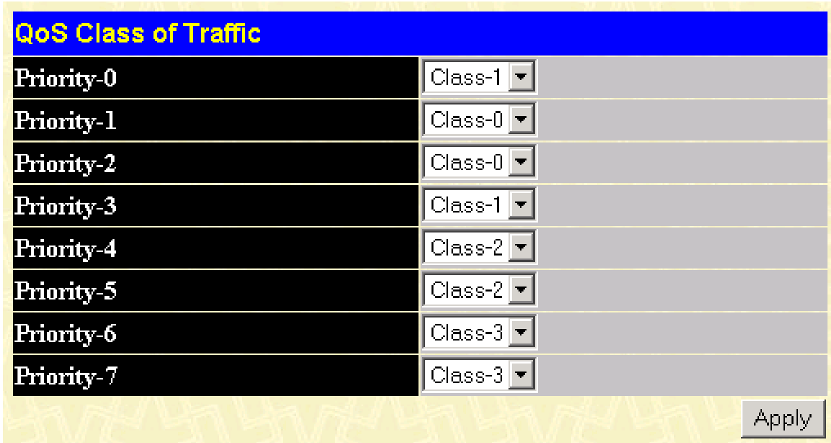


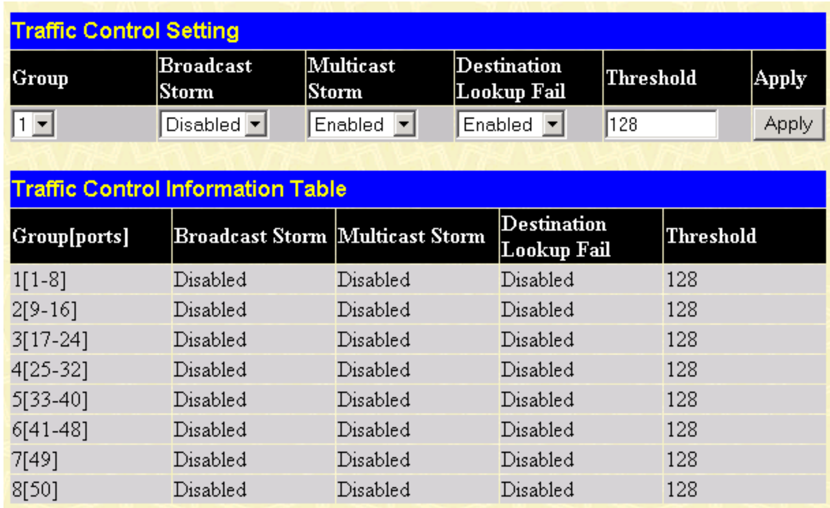
Figure 6- 33. QoS Class of Traffic window

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.

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 6- 34. Traffic Control Setting window

The following fields can be set:

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.

Traffic Segmentation

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

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

Traffic Segmentation Setting

Port	Forward Portlist	Apply
		Apply

Traffic Segmentation Table

Port	Forward Portlist
1	1-50
2	1-50
3	1-50
4	1-50
5	1-50
6	1-50
7	1-50
8	1-50
9	1-50
10	1-50
11	1-50
12	1-50
13	1-50
14	1-50
15	1-50
16	1-50
17	1-50
18	1-50
19	1-50
20	1-50
21	1-50
22	1-50
23	1-50
24	1-50
25	1-50
26	1-50
27	1-50
28	1-50
29	1-50
30	1-50

31	1-50
32	1-50
33	1-50
34	1-50
35	1-50
36	1-50
37	1-50
38	1-50
39	1-50
40	1-50
41	1-50
42	1-50
43	1-50
44	1-50
45	1-50
46	1-50
47	1-50
48	1-50
49	1-50
50	1-50

Figure 6- 35. 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 example, 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

The Link Aggregation Control Protocol provides for the formation of a single Layer 2 link from two or more standard Ethernet member links via automatic member link activation using the Link Aggregation Control Protocol (LACP). LACP provides a robust means of assuring that both ends of the link are up and agree to be members of the aggregation before the link member is activated.

LACP must be enabled at both ends of the link to be operational. Should LACP not be available at both ends of the link, 802.3ad provides a manual aggregation that only requires both ends of the link be in a link up state. Because manual aggregation provides for the activation of a member link without performing the LACP message exchanges, it should not be considered as reliable and robust as an LACP negotiated link.

LACP automatically determines which member links can be aggregated and then aggregates them. It provides for the controlled addition and removal of physical links for the link aggregation such that no frames are lost or duplicated.

Click Lacp Port in the LACP folder on the Configuration menu:

Lacp Port Settings

From	To	Mode	Apply
Port 1	Port 1	Passive	Apply

Lacp Port Table

Port	Activity
1	Active
2	Active
3	Active
4	Active
5	Active
6	Active
7	Active
8	Active
9	Active
10	Active
11	Active
12	Active
13	Active
14	Active
15	Active
16	Active
17	Active
18	Active
19	Active
20	Active
21	Active
22	Active
23	Active
24	Active
25	Active
26	Active
27	Active
28	Active
29	Active
30	Active

31	Active
32	Active
33	Active
34	Active
35	Active
36	Active
37	Active
38	Active
39	Active
40	Active
41	Active
42	Active
43	Active
44	Active
45	Active
46	Active
47	Active
48	Active
49	Active
50	Active

Figure 6- 36. Lacp Port Settings window

To use LACP, select the desired range of ports in the first two fields, change the State to *Enabled*, and click **Apply** to let your changes take effect.

Link Aggregation

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

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

The switch allows the creation of up to 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 configuration of the Master Port in the group becomes the configuration for all of the ports in the aggregation group. All configuration options – including the VLAN configuration – that can be applied to the Master Port are applied to the entire link aggregation group.

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

The Spanning Tree Protocol will treat a link aggregation group as a single link. 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.

Click Link Aggregation in the LACP folder on the Configuration menu:

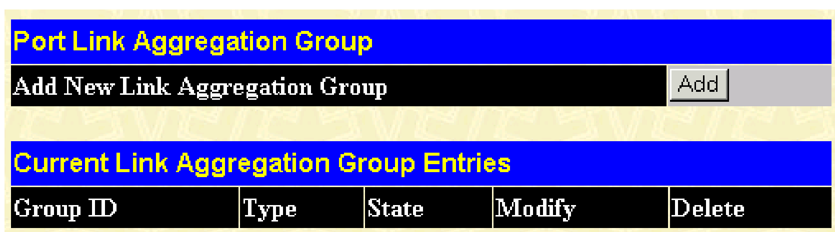


Figure 6- 37. Port Link Aggregation Group window

To configure a link aggregation group, click Add on the Port Link Aggregation Group window above:

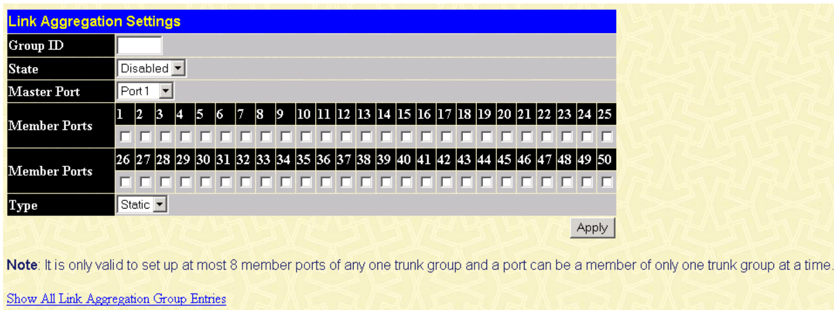


Figure 6- 38. Link Aggregation Settings window

The following fields can be set:

Parameter	Description
Group ID	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*	The Master port of link aggregation

1>	group.
Member Port	Allows the specification of the ports that will make up the link aggregation group.
Type	Toggle between *Static* and *LACP*.

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.

Click Access Profile Table on the Configuration menu to open the Access Profile Table window:

Figure 6- 39. Access Profile Table window

To create an Access Profile Mask:

Click the **Add** button in the window above. A new window is displayed. Use this to create an access profile and specify what criteria are used to examine frames. Once the profile has been created you can set up the rule applied to the profile as described later in this section.

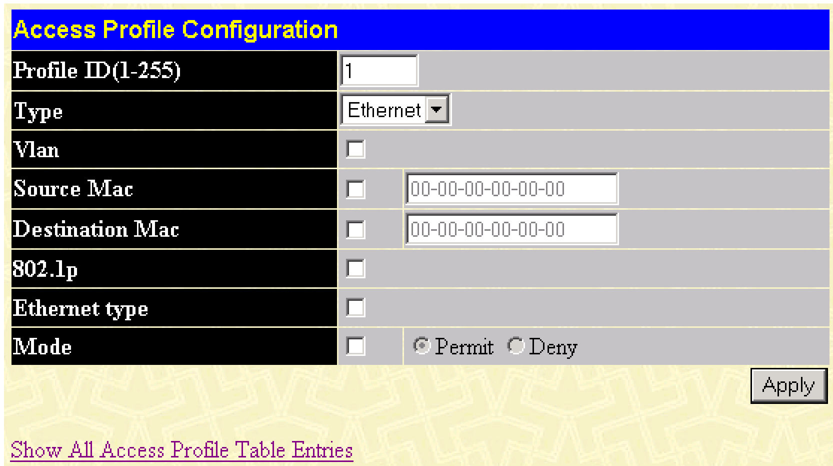


Figure 6- 40. Access Profile (Ethernet) Configuration window

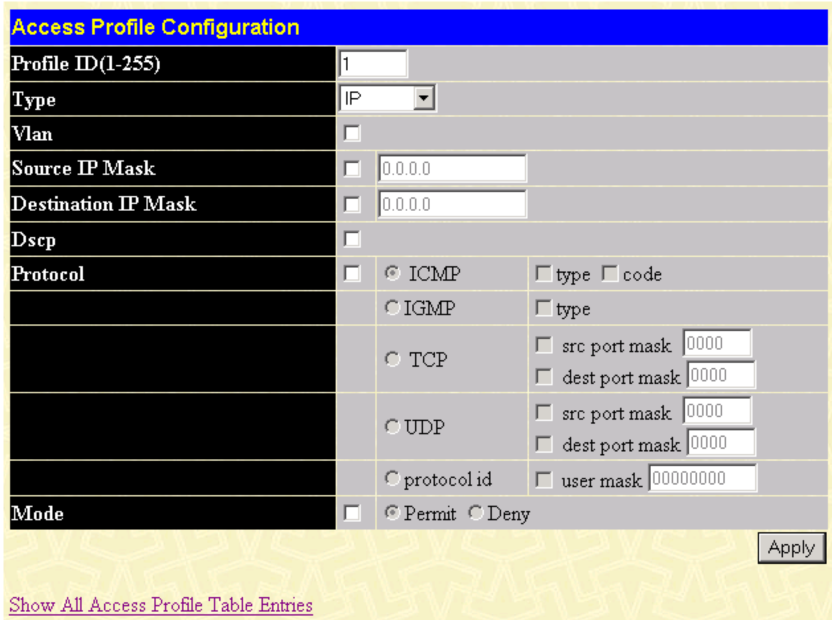


Figure 6- 41. Access Profile (IP) Configuration window

Configure the following Access Profile settings:

Parameter	Description
Profile ID(1-255)	Type in a unique identifier number for this profile set. This value can be set from 1 to 255.
Access Profile	Select profile based on Ethernet (MAC Address) or IP address. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the switch to examine the layer 2 part of each packet header. Select IP to instruct the switch to examine the IP address in each frame's header.

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 MAC/IP Mask	Source MAC Mask - Enter a MAC address mask for the source MAC address. Source IP Mask - Enter an IP address mask for the source IP address.
Destination MAC/IP Mask	Destination MAC Mask - Enter a MAC address mask for the destination MAC address. Destination IP Mask - Enter an IP address mask for the destination IP 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.
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.
Ethernet type (for Ethernet Access Profiles only)	Selecting this option instructs the switch to examine the Ethernet type value in each frame's header.
Protocol (for IP address Access Profiles only)	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 cod 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).

dest port mask - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff).

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). Select *protocol id* to instruct the switch to examine each frame's Protocol ID field. *user mask* – Specify that the rule applies to the IP protocol ID and the mask options behind the IP header.
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.

To establish the rule for a previously created Access Profile:

Select the Access Profile entry from the **Access Profile Table** window and then click the **Modify** button for that individual entry.

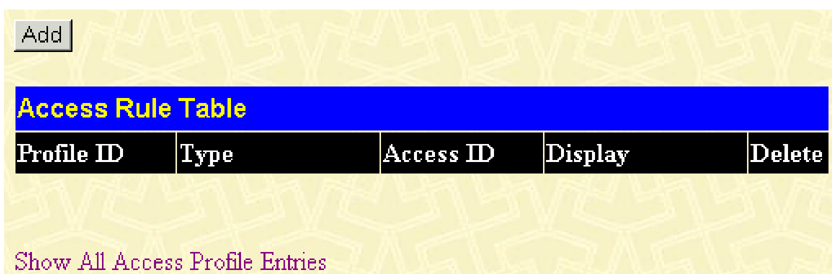


Figure 6- 42. Access Rule Table window

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

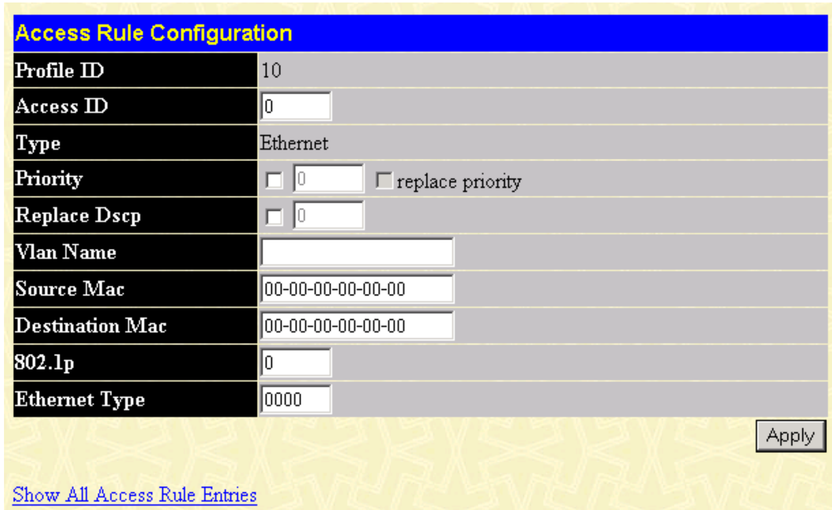


Figure 6- 43. Access Rule Configuration window

Configure the following Access Rule Configuration settings (additional parameters are described in earlier sections):

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 to 255.
Priority	Select this option to instruct the switch to use the 802.1p priority value entered in the adjacent field for packets that meet the criteria. A number between 0 – lowest

	priority, and 7 – highest priority, can be entered.
replace priority	Select this option to instruct the switch to replace the 802.1p value (in a packet that meets the selected criteria). In this way, packets meeting the criteria can have their priority handling modified for use within the switch, and then have a different priority value assigned when they leave the switch.
Replace Dscp	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.

PAE Access Entity

The DES-3350SR implements the server-side of the IEEE 802.1x Port-based Network Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the switch that a user or network device must meet before allowing that port to forward or receive frames.

IEEE 802.1X operation must be enabled on the switch before it will function. This is done using the 802.1x Status control on the **Switch Information (Advanced Settings)** window. 802.1X settings can be configured before it is enabled switch-wide.

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
24	both	auto	30	60	30	30	2	3600	no
25	both	auto	30	60	30	30	2	3600	no
26	both	auto	30	60	30	30	2	3600	no
27	both	auto	30	60	30	30	2	3600	no
28	both	auto	30	60	30	30	2	3600	no

29	both	auto	30	60	30	30	2	3600	no
30	both	auto	30	60	30	30	2	3600	no
31	both	auto	30	60	30	30	2	3600	no
32	both	auto	30	60	30	30	2	3600	no
33	both	auto	30	60	30	30	2	3600	no
34	both	auto	30	60	30	30	2	3600	no
35	both	auto	30	60	30	30	2	3600	no
36	both	auto	30	60	30	30	2	3600	no
37	both	auto	30	60	30	30	2	3600	no
38	both	auto	30	60	30	30	2	3600	no
39	both	auto	30	60	30	30	2	3600	no
40	both	auto	30	60	30	30	2	3600	no
41	both	auto	30	60	30	30	2	3600	no
42	both	auto	30	60	30	30	2	3600	no
43	both	auto	30	60	30	30	2	3600	no
44	both	auto	30	60	30	30	2	3600	no
45	both	auto	30	60	30	30	2	3600	no
46	both	auto	30	60	30	30	2	3600	no
47	both	auto	30	60	30	30	2	3600	no
48	both	auto	30	60	30	30	2	3600	no
49	both	auto	30	60	30	30	2	3600	no
50	both	auto	30	60	30	30	2	3600	no

Figure 6- 44. First 802.1X Authenticator Settings window

Click the selection button on the far left that corresponds to the port you want to configure

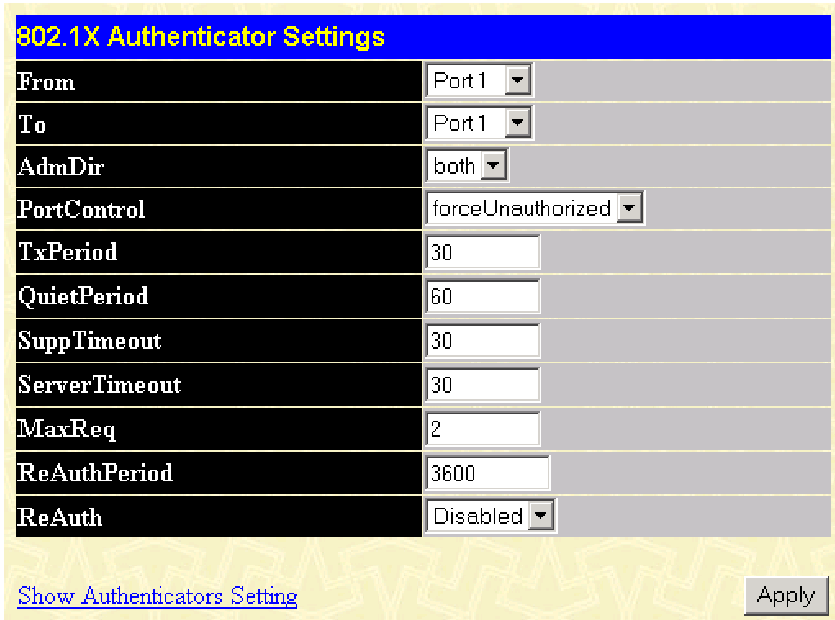


Figure 6- 45. Second 802.1X Authenticator Settings window

Configure the following 802.1x port settings:

Parameter	Description
From and **To**	Ports 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.

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 reauthentication.

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:

802.1X Capability Settings

From	To	Capability	Apply
Port 1	Port 1	None	Apply

802.1X Capability Table

Port	Capability
1	None
2	None
3	None
4	None
5	None
6	None
7	None
8	None
9	None
10	None
11	None
12	None
13	None
14	None
15	None
16	None
17	None
18	None
19	None
20	None
21	None
22	None
23	None
24	None
25	None
26	None
27	None
28	None
29	None
30	None

31	None
32	None
33	None
34	None
35	None
36	None
37	None
38	None
39	None
40	None
41	None
42	None
43	None
44	None
45	None
46	None
47	None
48	None
49	None
50	None

Figure 6- 46. 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 Port(s)

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:

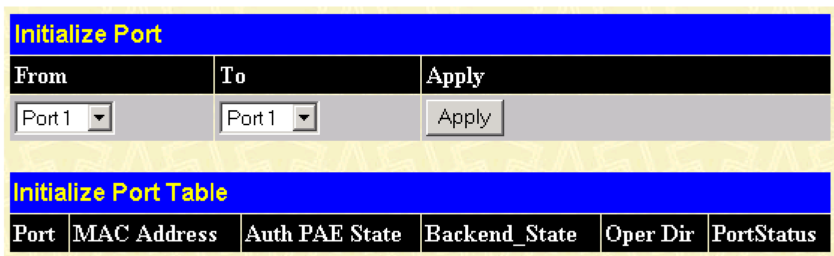


Figure 6- 47. Initialize Port window

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

Reauthenticate Port(s)

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:

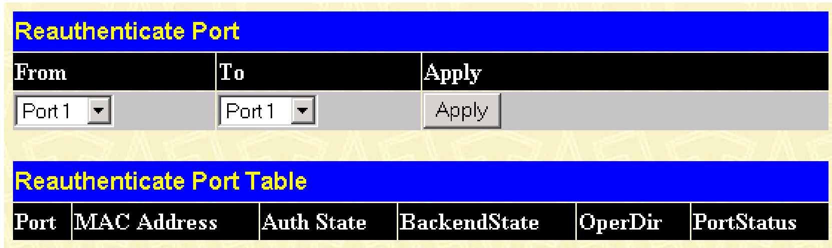


Figure 6- 48. Reauthenticate Port window

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*.

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:

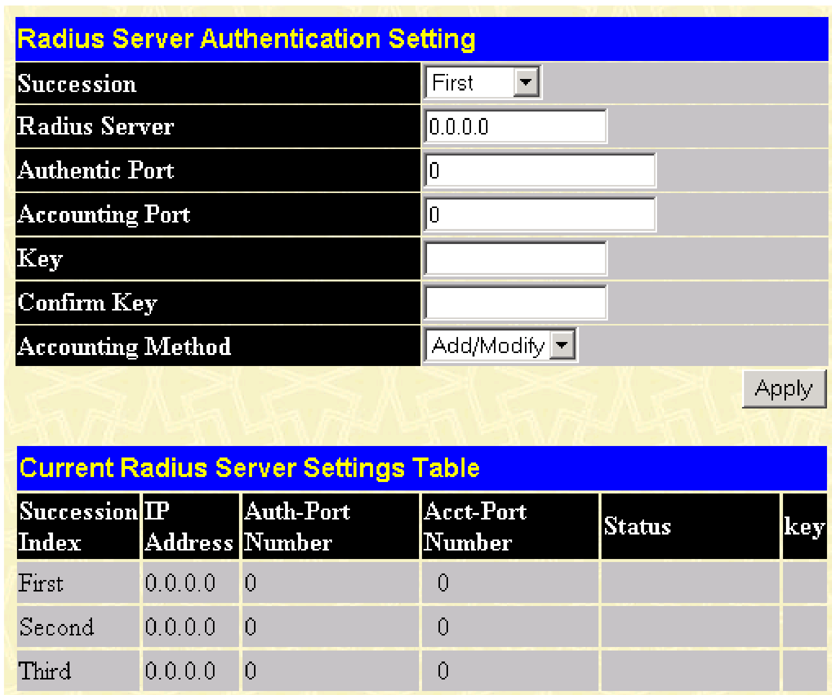


Figure 6- 49. Radius Server Authentication Setting window

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.

Management

The DES-3350SR allows you to manage the switch via the **Management** menu. The menu consists of the following folders and screens: **Security IP**, **User Accounts**, and **SNMPV3**. See below for further description.

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:

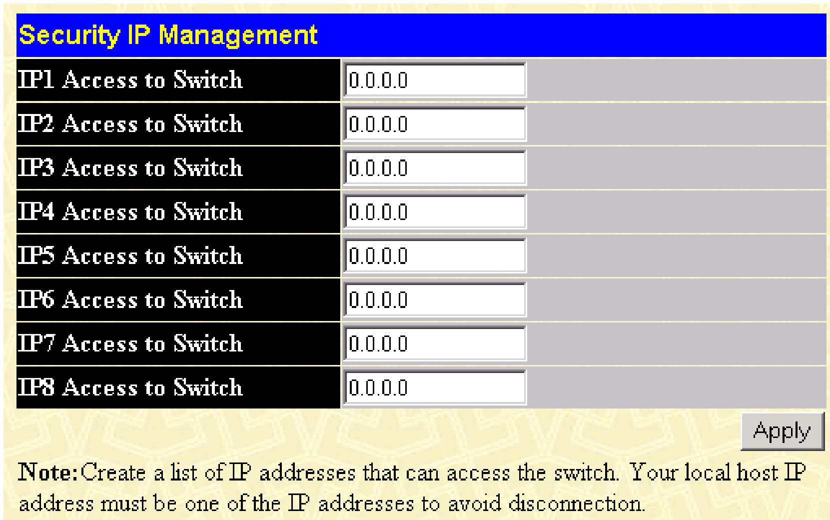


Figure 6- 50. Security IP Management window

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

Figure 6- 51. User Account Management window

Click **Add** to add a user.

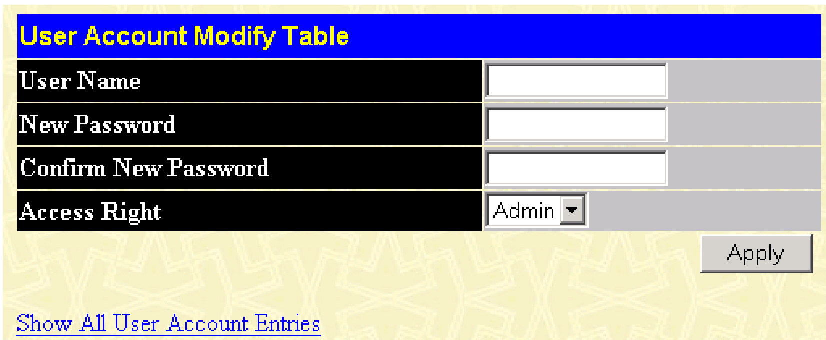


Figure 6- 52. User Account Modify Table window

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.

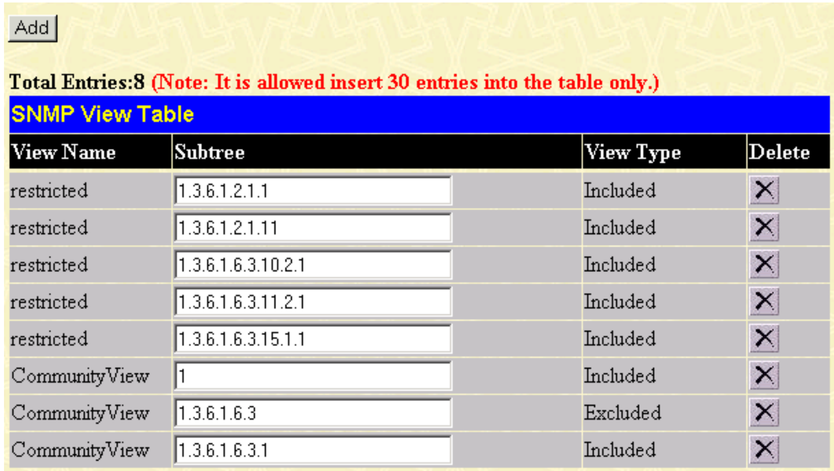
SNMPV3

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 menu.

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.


Add

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

SNMP View Table

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

Figure 6- 53. 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.

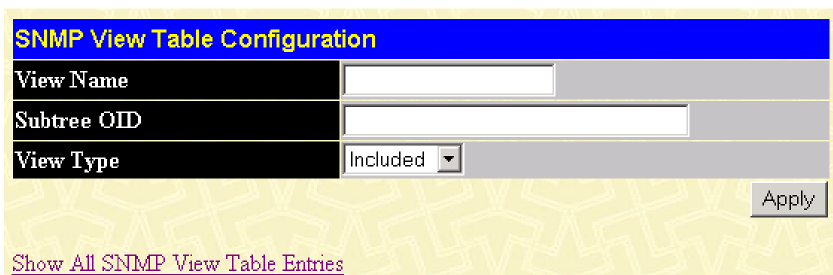


Figure 6- 54. SNMP View Table Configuration window

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.

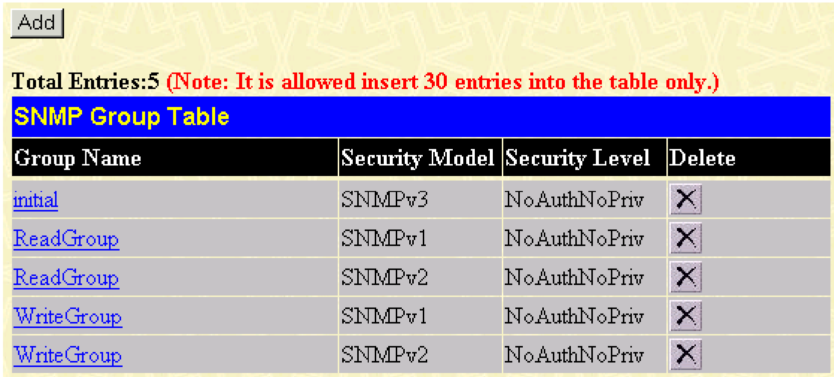


Figure 6- 55. SNMP Group Table window

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.

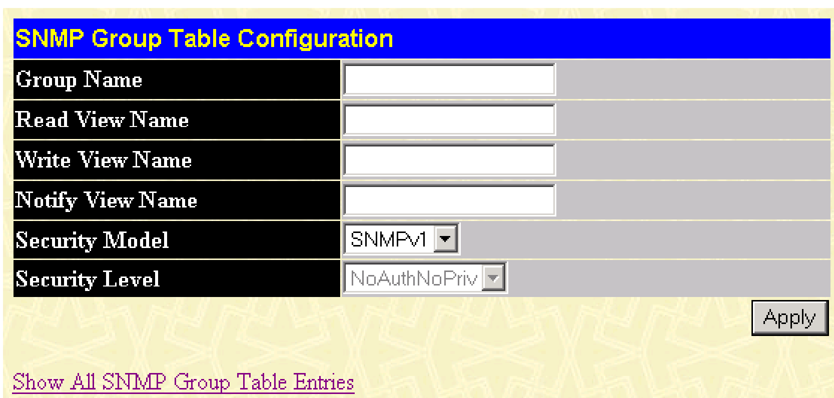


Figure 6- 56. SNMP Group Table Configuration window

Parameter	Description

Group Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Read View Name	This name is used to specify the SNMP group created can request SNMP messages.
Write View Name	Specify a SNMP group name for users that are allowed SNMP write privileges to the switch's SNMP agent.
Notify View Name	Specify a SNMP group name for users that can receive SNMP trap messages generated by the switch's SNMP agent.
Security Model	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. *USM* – 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.

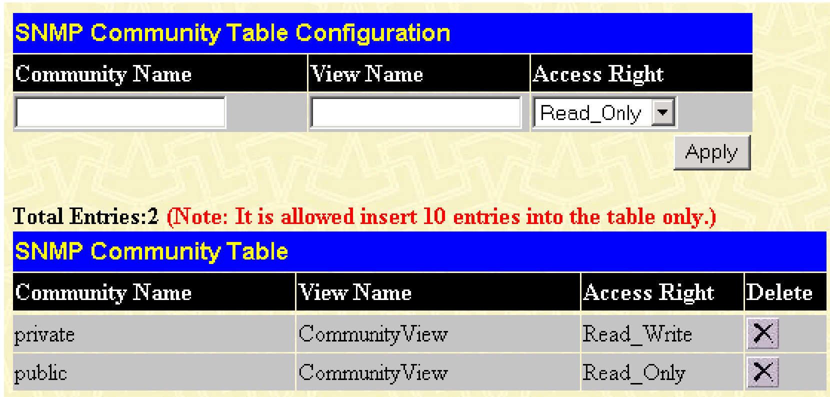


Figure 6- 57. SNMP Community Table Configuration window

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 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.

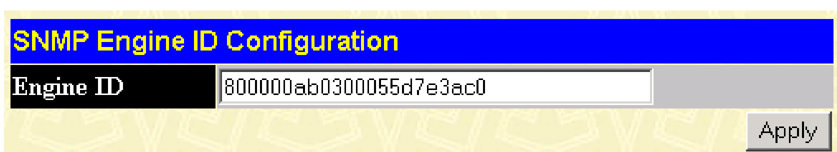


Figure 6- 58. SNMP Engine ID Configuration window

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

SNMP Host Table

Use the SNMP Host Table to set up trap recipients.

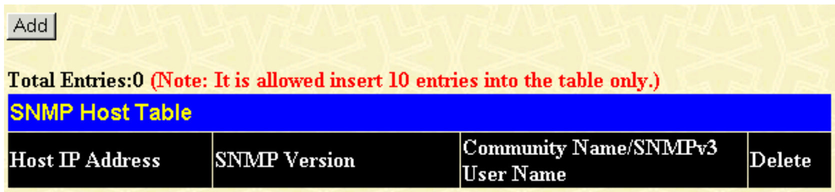


Figure 6- 59. SNMP Host Table window

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.

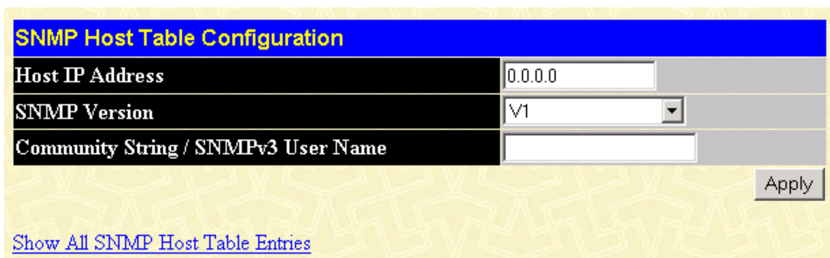


Figure 6- 60. SNMP Host Table Configuration window

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. *V2* – 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 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.

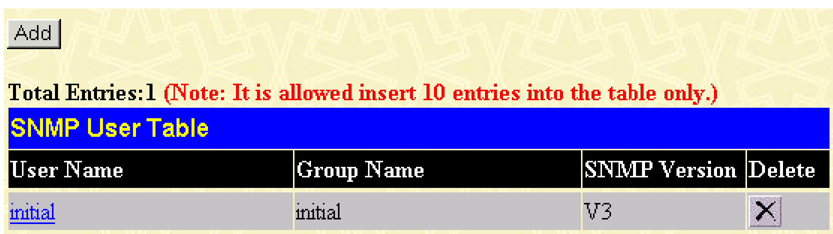


Figure 6- 61. SNMP User Table window

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

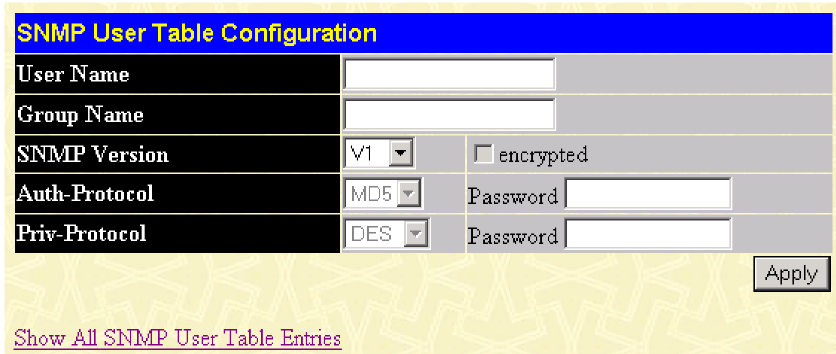


Figure 6- 62. SNMP User Table Configuration window

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.

Layer 3 IP Networking

To access the Layer 3 IP Networking links, select **Layer 3 IP Networking** from the main folder.

Setting up IP Interfaces

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, 31, 32, 33, 34
Engineer	2	9, 10, 11, 12
Marketing	3	43, 44, 45, 46
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4
Backbone	6	25, 26

Table 6- 1. VLAN Example – Assigned Ports

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

Using a 10.xxx.xxx.xxx IP address notation, the above example would give six network addresses and 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 6- 2. VLAN Example – Assigned IP Interfaces

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

IP Interface Settings

To setup IP Interfaces on the switch:

Go to the **Layer 3 IP Networking** link, and then click on the **IP Interface Settings** link to open the following window:

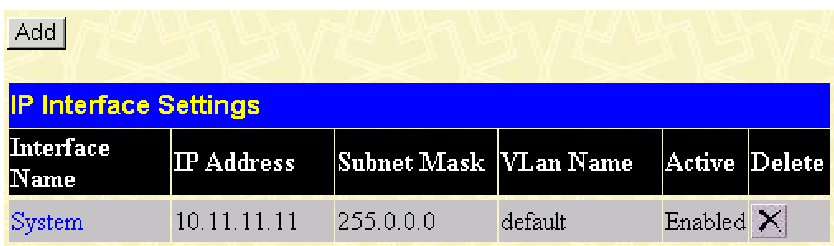


Figure 6- 63. IP Interface Settings window

To setup a new IP interface, click the Add button:

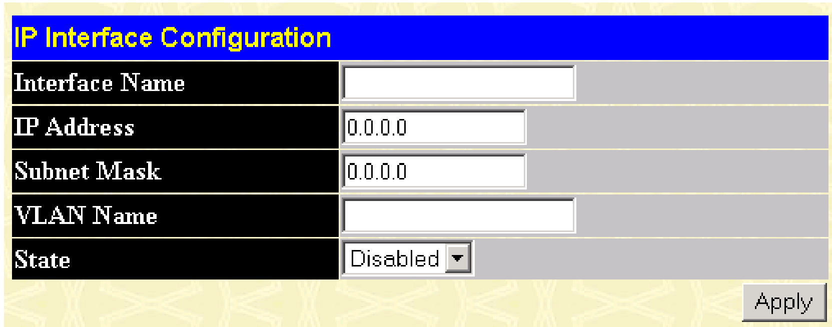


Figure 6- 64. IP Interface Configuration window

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

The following fields can be set:

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

	interface.
VLAN Name	This field allows the entry of the VLAN Name for the VLAN the IP interface belongs to.
State <*Disabled*>	This field is toggled between *Enabled* and *Disabled* using the space bar. This entry determines whether the interface will be active or not.

Layer 3 Global Settings

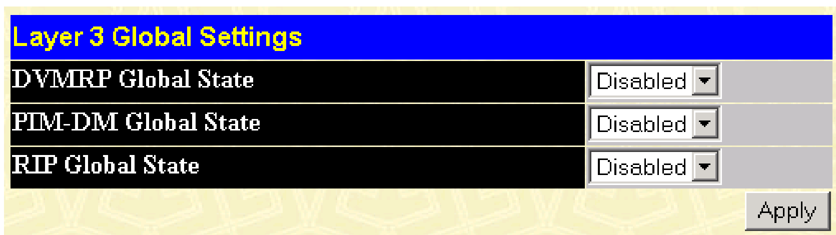


Figure 6- 65. Layer 3 Global Settings window

This window allows you to globally configure DVMRP, PIM-DM, and RIP settings. Click **Apply** to let your settings take effect.

MD5 Key Table Settings

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

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

To configure an MD5 Key, click the MD5 Key Table Settings link to open the following dialog box:

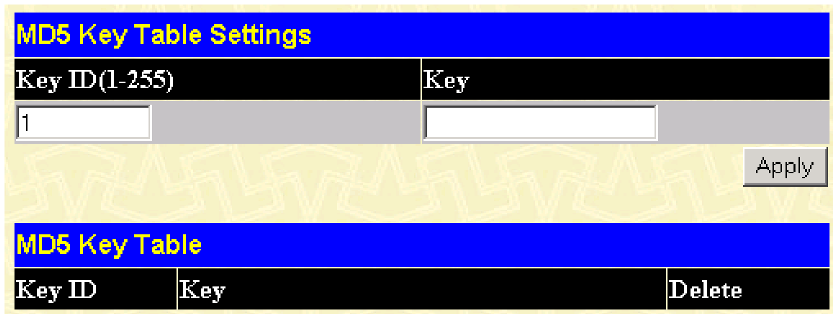


Figure 6- 66. MD5 Key Table Settings window

To delete an entry in the MD5 Key Table, select the click-box for the entry to be removed in the Delete column in the window above.

The following fields can be set:

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

Route Redistribution Settings

Route redistribution allows routers on the network – that are running different routing protocols – to exchange routing information. This is accomplished by comparing the routes stored in the various router's routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual routers current routing protocol. The DES-3350SR 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 DES-3350SR's switch is also redistributed.

To configure Route Redistribution on the switch, click on the Route Redistribution Settings link under the Layer 3 IP Network folder.

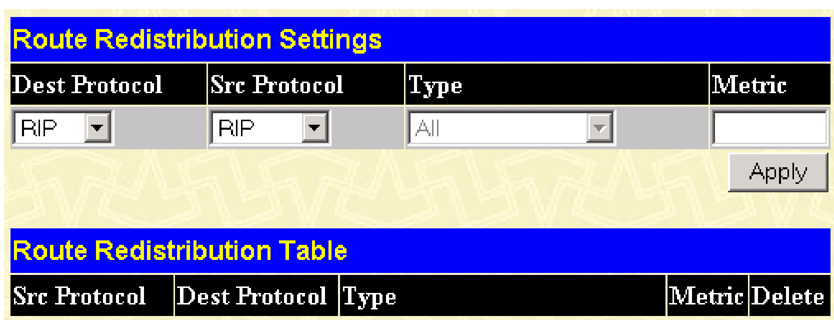


Figure 6- 67. Route Redistribution Settings window

The following fields can be set or are displayed:

Parameter	Description
Dest Protocol	Allows the selection of the protocol of the destination device. Available

	choices are *RIP* and *OSPF*.
Src Protocol	Allows the selection of the protocol of the source device. Available choices are *RIP*, *OSPF*, *Static*, or *Local*.
Type	Allows the selection of up to seven methods for calculating the metric value—depending on the selections in the first two fields. *Type-1* calculates the metric by adding the destination's interface cost to the metric entered in the Metric field. *Type-2* uses the metric entered in the Metric field without change. *Internal* uses routes learned from OSPF. *External* uses protocols other than OSPF. Other options include: *Internal & Type-1*, *Internal & Type-2*, and *All*.
Metric	Allows the entry of an interface cost.

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 enter an IP address into the switch's IP Forwarding Table, click the Static/Default Route Settings link on the Layer 3 IP Networking folder:

Figure 6- 68. Static/Default Route Settings window

To delete an existing static/default route, click the click-box for the entry in the Delete column.

To add a new static/default route, click the Add button:

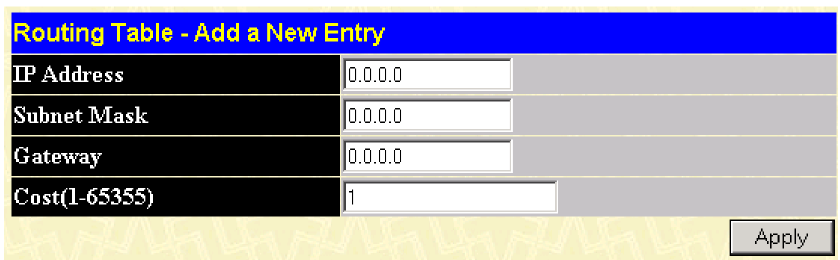


Figure 6- 69. Routing Table – Add a New Entry window

The following fields can be set:

Parameter	Description
IP Address <*0.0.0.0*>	Allows the entry of an IP address that will be a static entry into the switch's Routing Table.
Subnet Mask <*0.0.0.0*>	Allows the entry of a subnet mask corresponding to the IP address above.
Gateway <*0.0.0.0*>	Allows the entry of an IP address of a gateway for the IP address above.

	gateway for the IP address above.
Cost(1-65355) <*1* >	Allows the entry of a routing protocol metric representing the number of routers between the switch and the IP address above.

RIP

Click on the **RIP Interfaces Settings** link on the **RIP** folder to view and configure RIP settings.

RIP Interface Settings					
Interface Name	**IP Address**	**Tx Mode**	**RX Mode**	**Auth.**	**State**
System	10.24.22.9	Disabled	Disabled	Disabled	Disabled

Figure 6- 70. RIP Interface Settings window

To edit an RIP Interface, click on the desired Interface Name on the window above.

RIP Interface Settings-Edit	
Interface Name	System
IP Address	10.24.22.9
Tx Mode	Disabled
RX Mode	Disabled
Authentication	Disabled
Password	
State	Disabled
	APPLY

Figure 6- 71. RIP Interface Settings-Edit window

The following fields can be set:

Parameter	Description
Interface Name	The name of the IP interface on which RIP is to be setup. This interface must be previously configured on the Switch.
IP Address	The IP address of the interface name.
TX Mode <*Disabled*>	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 <*Disabled*>	Toggle among *Disabled*, *V1 Only*, *V2 Only*, and *V1 or V2*. This entry specifies which version of the RIP protocol will be used to interpret received RIP packets. *Disabled* prevents the reception of RIP packets.
Authentication	Toggle between *Disabled* and *Enabled* to specify that routers on the network should use 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 RIP on

this interface of the switch.

OSPF

OSPF General Settings

The **OSPF General Settings** window allows OSPF to be enabled or disabled on the switch – without changing the switch's OSPF configuration. In addition, the switch can be designated as an Autonomous System (**AS**) **Border Router**.

From the Layer 3 IP Networking folder, click on the OSPF folder and then click on the OSPF General Settings link:

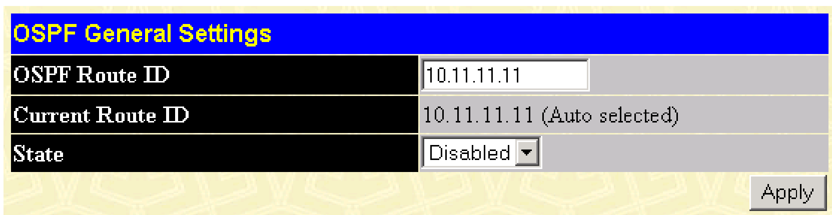


Figure 6- 72. OSPF General Settings window

The following parameters can be set or are displayed:

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 10.255.255.255, but any unique 32-

	bit number will do. If 0.0.0.0 is entered, the highest IP address assigned to the switch will become the OSPF Route ID.
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 Settings

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.

From the Layer 3 IP Networking folder, click on the OSPF folder and then click on the OSPF Area Setting link:

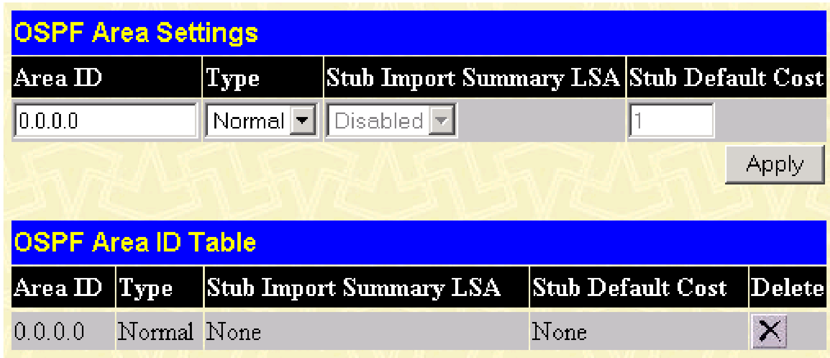


Figure 6- 73. OSPF Area Settings window

This window displays a summary of all of the OSPF areas defined on the switch in the OSPF Area ID Table in the lower half of the window.

To add an OSPF area to the switch, enter the required information above and then click on the **Apply** button.

To delete an entry, click the "X" icon in the Delete column next to the entry to be deleted.

The following fields can be set or are displayed:

Parameter	Description
Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Type	This field can be toggled between Normal and Stub using the space bar. When it is toggled to Stub, additional fields appear – Stub

	Import Summary LSA, and Default Cost.
Stub Import Summary LSA	Displays whether or not the selected Area will allow Summary Link-State Advertisements (Summary LSAs) to be imported into the area from other areas.
Stub Default Cost	Displays the default cost for the route to the stub of between *0* and *65,535*.

OSPF Interface Settings

This menu is used to configure the OSPF interface settings.

To configure an OSPF Interface, click on the OSPF Interface Settings link:

OSPF Interface Settings

Name	IP Address	Area ID	Priority	Hello Time	Dead Time	Auth. Type	State
System	10.24.22.8	0.0.0.0	1	10	40	None	Disabled

Figure 6- 74. OSPF Interface Settings window

All of the IP Interfaces currently configured on the switch will be displayed. Select the IP interface you want to configure OSPF for by clicking it. This will open the following window:

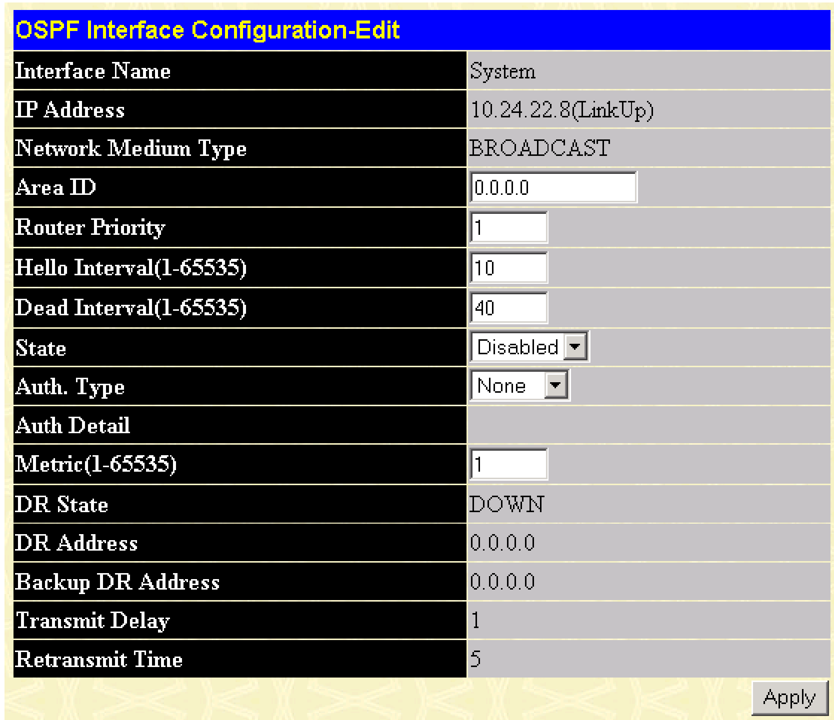


Figure 6- 75. OSPF Interface Configuration-Edit window

The following fields can then be set:

Parameter	Description
Interface Name	Displays the of an IP interface previously configured on the switch.
Area ID	Allows the entry of an OSPF Area ID configured above.
Router Priority	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 transmissions 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 ID 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 Settings** window. When *MD5* is selected, the Auth. Key ID field allows the specification of the Key ID as defined in the MD5 configuration above. This must be the same MD5 Key as used by the neighboring router.
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*.

OSPF Virtual Link Settings

Virtual Interfaces are used by OSPF to link areas that do not have a physical connection to the backbone (also called Area 0) or to link areas of the backbone itself that are discontinuous. This allows routing information to flow from an area that is physically disconnected from area 0 into area 0 by configuring an interface across one of the areas previously defined above.

To setup an OSPF Virtual Interface on the switch, click the OSPF Virtual Link Settings link under the OSPF folder:

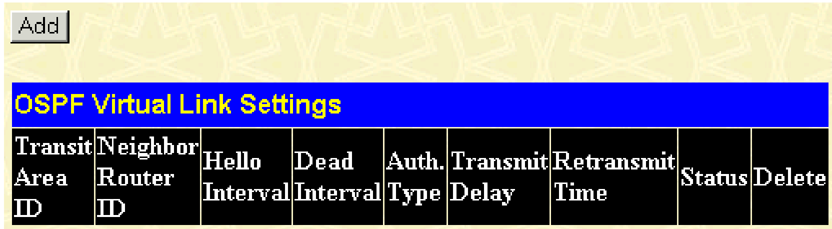


Figure 6- 76. OSPF Virtual Link Settings window

To add an OSPF Virtual Interface on the switch, click the Add button:

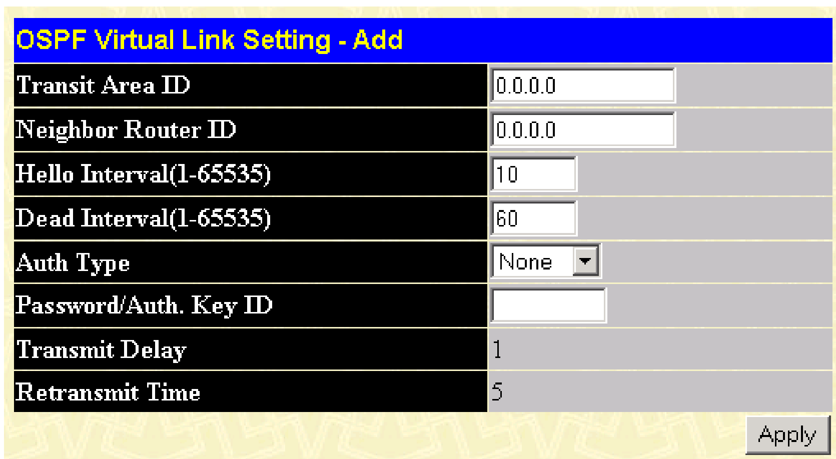


Figure 6- 77. OSPF Virtual Link Setting – Add window

The following fields can be set or are displayed:

Parameter	Description
Transit Area ID	Allows the entry of an OSPF Area ID – previously defined on the switch – that allows a remote area to

	communicate with the backbone (area 0). A Transit Area cannot be a Stub Area or a Backbone Area.
Neighbor Router ID	The OSPF router ID for the remote router. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.
Hello Interval(1-65535)	Allows the specification of the interval between the transmissions 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.
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 ID 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 Settings** window. When *MD5* is selected, the Auth. Key ID field allows the specification of the Key ID as defined in the MD5 configuration above. This must be the same MD5 Key as used by the neighboring router.
Password/Auth. Key ID	This is the same value entered in the **MD5 Key Table Settings** window.
Transmit Delay	The estimated number of seconds it takes to transmit a link state update packet over this interface.
Retransmit Time	The number of seconds between link state advertisement retransmissions, for adjacencies belonging to this interface.

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.

To configure OSPF Area Aggregation on the switch, click the OSPF Area Aggregation Settings link under the OSPF folder:

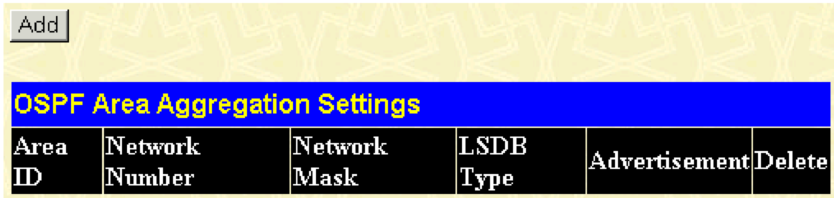


Figure 6- 78. OSPF Area Aggregation Settings window

To add an OSPF Area Aggregation entry on the switch, click the New button:

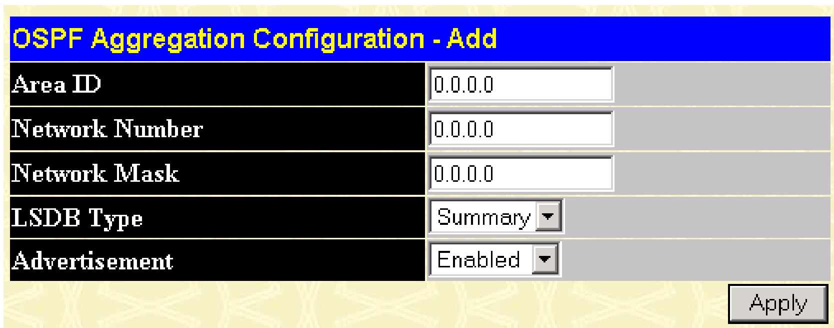


Figure 6- 79. OSPF Aggregation Configuration – Add window

The following fields can be set or are displayed:

Parameter	Description
Area ID	Allows the entry the OSPF Area ID for which the routing information will be aggregated. This Area ID must be previously defined on the switch.

Network Number	Sometimes called the Network Address. The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area above.
Network Mask	Allows the entry of the network mask.
LSDB Type	*Summary* is the only option available in the current software release.
Advertisement	This field can be toggled between *Enabled* and *Disabled*. It determines whether the selected OSPF Area will advertise its summary LSDB (Network-Number and Network-Mask) or not.

OSPF Host Route Settings

This menu is used to configure OSPF host route settings on the switch.

To configure OSPF Host Route Settings on the switch, click OSPF Host Route Settings link in the OSPF folder:

Figure 6- 80. OSPF Host Route Setting window

To add an OSPF Host Route on the switch, click the New button:

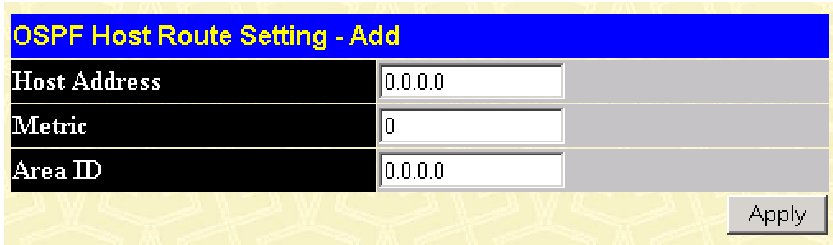


Figure 6- 81. OSPF Host Route Settings – Add window

The following fields can be set or are displayed:

Parameter	Description
Host Address	The IP address of the host.
Metric	A value between *1* and *65,535* 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

DHCP/BOOTP Relay can be configured on both the switch level, or on a per-IP interface level.

To enable and configure DHCP or BOOTP on the switch, click DHCP/Bootp Relay Information on the DHCP/BootP Relay link:

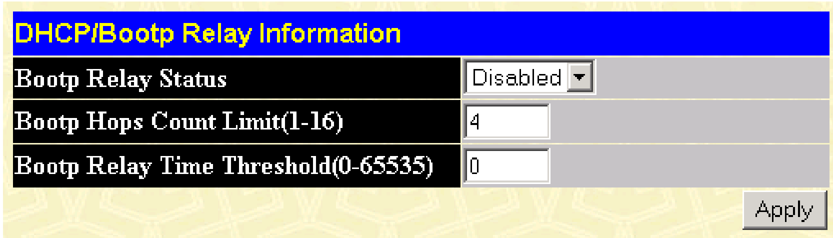


Figure 6- 82. DHCP/Bootp Relay Information window

The following fields can be set:

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

***To configure the DHCP/BOOTP Relay interface, click on the BOOTP/DHCP Relay Interface Configuration link*:**

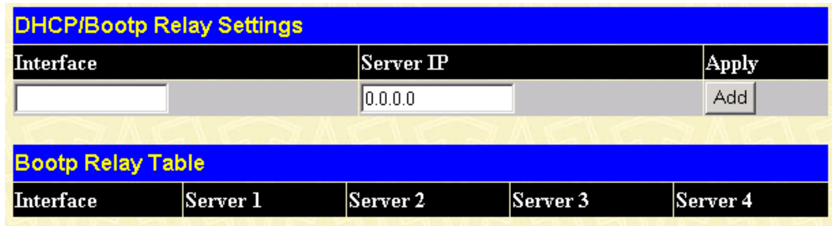


Figure 6- 83. DHCP/Bootp Relay Settings window

The following fields can be set:

Parameter	Description
Interface	The interface name of the IP interface on which the BOOTP or DHCP servers reside on.
Server IP <*0.0.0.0*>	Allows the entry of IP addresses for up to four BOOTP or DHCP servers.

DNS Relay

To configure DNS Relay, click on the DNS Relay Information link in the DNS Relay folder:

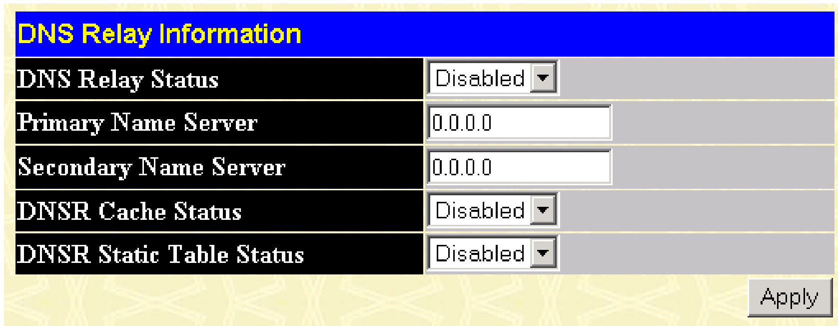


Figure 6- 84. DNS Relay Information window

The following fields can be set:

Parameter	Description
DNS Relay State <*Disabled*>	This field can be toggled between *Disabled* and *Enabled* using the pull-down menu, and is used to enable or disable the DNS Relay service on the switch.
Primary Name Server <*0.0.0.0*>	Allows the entry of the IP address of a primary domain name server (DNS).
Secondary Name Server <*0.0.0.0*>	Allows the entry of the IP address of a secondary domain name server (DNS).
DNSR Cache Status <*Disabled*>	This can be toggled between *Disabled* and *Enabled.* This determines if a DNS cache will be enabled on the switch.
DNSR Static Table Status <*Disabled*>	This field can be toggled using the pull-down menu between *Disabled*

Status <*Disabled*>	and *Enabled.* This determines if the static DNS table will be used or not.

To make a static DNS table entry, click on the DNS Relay Static Setting link in the DNS Relay folder:

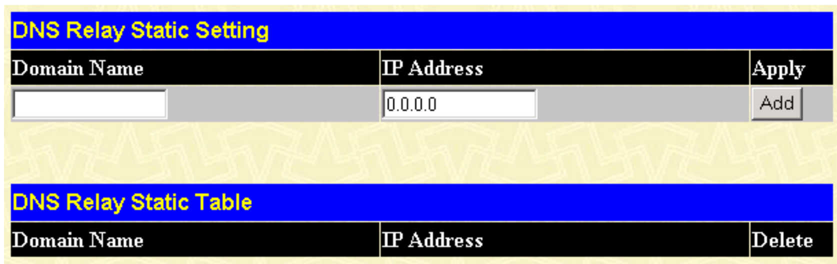


Figure 6- 85. DNS Relay Static Setting window

To add a new entry to the table, enter the domain name and IP address and then click the **Add** button.

The following fields can be set:

Parameter	Description
Domain Name	The domain name of the static DNS table entry.
IP Address <*0.0.0.0*>	The IP address of the domain name above.

IP Multicast Routing Protocol

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

IGMP Interface Settings

The Internet Group Multicasting Protocol (IGMP) can be configured on the switch on a per-IP interface basis. Each IP interface configured on the switch is displayed in the **IGMP Interface Settings** window.

From the Layer 3 IP Networking folder, select IP Multicast Routing Protocols and then click IGMP Interface Settings to open the following window:

IGMP Interface Settings

Interface Name	IP Address	Version	State
System	10.11.11.11	2	Disabled

Figure 6- 86. IGMP Interface Table window

To edit an IGMP Interface Settings entry on the switch, click on the entry in the table above:

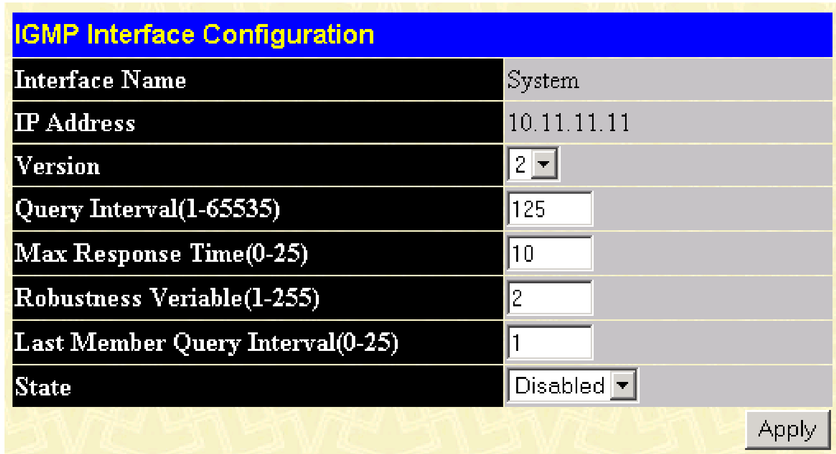


Figure 6- 87. IGMP Interface Configuration window

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 using the Version field's pull-down menu. The length of time between queries can be varied by entering a value between *1* and *65,535* seconds in the Query Interval field. The maximum length of time between the receipt of a query and the sending of an IGMP response report can be varied by entering a value in the Max Response Time field.

The Robustness Variable field allows IGMP to be 'tuned' for sub-networks that are expected to lose a lot of packets. A high value (max. 255) for the robustness variable will help compensate for 'lossy' sub-networks. A low value (min. 2) should be used for sub-networks with less packet loss during times of heavy network traffic.

The following fields can be set:

Parameter	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 <*2*>	Enter the IGMP version (*1* or *2*) that will be used to interpret IGMP queries on the interface.
Query Interval(1-65535) <*125*>	Allows the entry of a value between *1* and *65535* seconds, with a default of *125* seconds. This specifies the length of time between sending IGMP queries.
Max Response Time(0-25) <*10*>	Sets the maximum amount of time allowed before sending an IGMP response report. A value between *0* and *25* seconds can be entered, with a default of *10* seconds.
Robustness Variable(1-255) <*2*>	A tuning variable to allow for subnetworks that are expected to lose a large number of packets. A value between *1* 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(0-25)	Specifies the maximum amount of time between query messages. The default is *1* second.

State	Toggle to disable or enable IGMP for the interface.

DVMRP Interface Settings

To configure DVMRP for an IP interface**, c**lick the DVMRP Interface Settings link in the IP Multicast Routing Protocol folder:

DVMRP Interface Settings		
Interface Name	IP Address	State
System	10.11.11.11	Enabled

Figure 6- 88. DVMRP Interface Settings window

Now select an entry by clicking on it:

DVMRP Interface Configuration	
Interface Name	System
IP Address	10.24.22.9
Neighbor Timeout Interval(1-65535 sec)	35
Probe Interval(1-65535 sec)	10
Metric(1-31)	1
State	Disabled
	Apply

Figure 6- 89. DVMRP Interface Configuration window

This window allows the Distance-Vector Multicast Routing Protocol to be configured for each IP interface defined on the switch.

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. It relies upon RIP hop counts to calculate 'shortest paths' back to the source of a multicast message, but defines a 'route cost' to calculate which branches of a multicast delivery tree should be 'pruned' – once the delivery tree is established.

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

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

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

The following fields can be set:

Parameter	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 sec) <*35*>	This field allows an entry between *1* and *65,535* seconds and defines the time period for DVMRP will hold Neighbor Router reports before issuing poison route messages. The default is *35* seconds.
Probe Interval(1-65535 sec) <*10*>	This field allows an entry between *0* and *65,535* seconds and defines the interval between 'probes'. The default is *10*.
Metric(1-31) <*1*>	This field allows an entry between *1* and *31* and defines the route cost for the IP interface. The DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hop count in RIP. The default cost is *1*.
State <*Disabled*>	This field can be toggled between *Enabled* and *Disabled* and enables or disables DVMRP for the IP interface. The default is *Disabled*.

PIM

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

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

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

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

To configure PIMDM for an IP interface, click the PIMDM Interface Configuration link under the IP Multicast Routing Protocols folder:

Figure 6- 90. PIM-DM Interface Settings window

The Protocol Independent Multicast – Dense Mode (PIM-DM) protocol can be individually configured for each IP interface on the switch. This window displays all of the IP interfaces currently configured on the switch.

To configure PIM-DM for a given IP Interface, click on the entry in the above table:

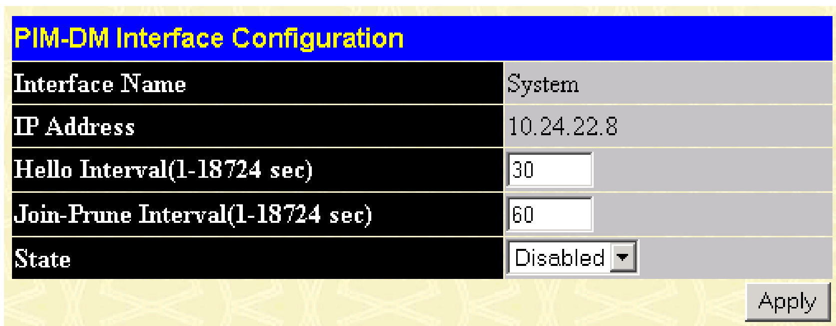


Figure 6- 91. PIM-DM Interface Configuration window

The following fields can be set:

Parameter	Description
Interface Name	Allows the entry of the name of the IP interface for which PIM-DM is to be configured. This must be a previously defined IP interface.

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

Monitoring

The DES-3350SR provides extensive network monitoring capabilities that can be viewed under the **Monitoring** menu. The menu consists of the following folders and windows: **Port Utilization**, **Packets**, **Errors**, **Size**, **MAC Address**, **IGMP Snooping Group**, **IGMP Snooping Forwarding**, **VLAN Status**, **Router Port**, **Power Status**, **Port Access Control**, and **Layer 3 feature**. See below for further description.

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:

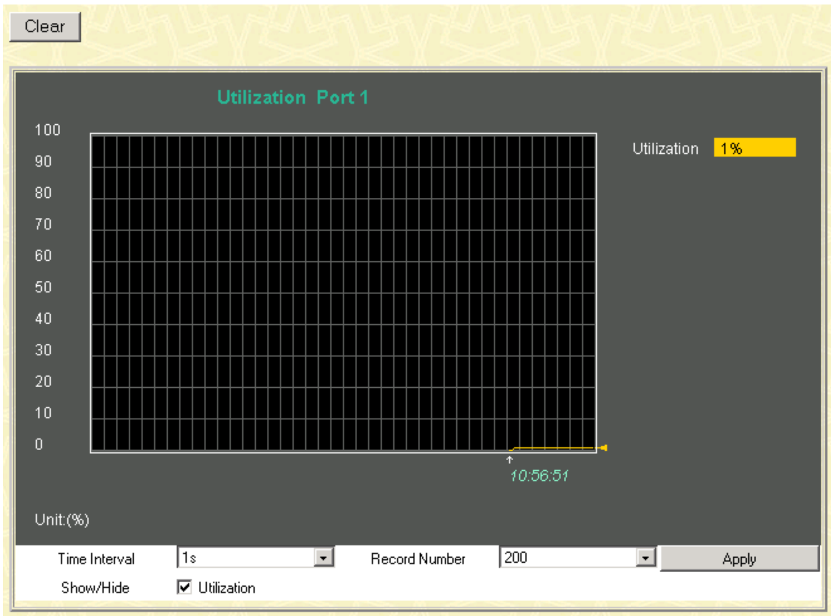


Figure 6- 92. Utilization window

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

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)

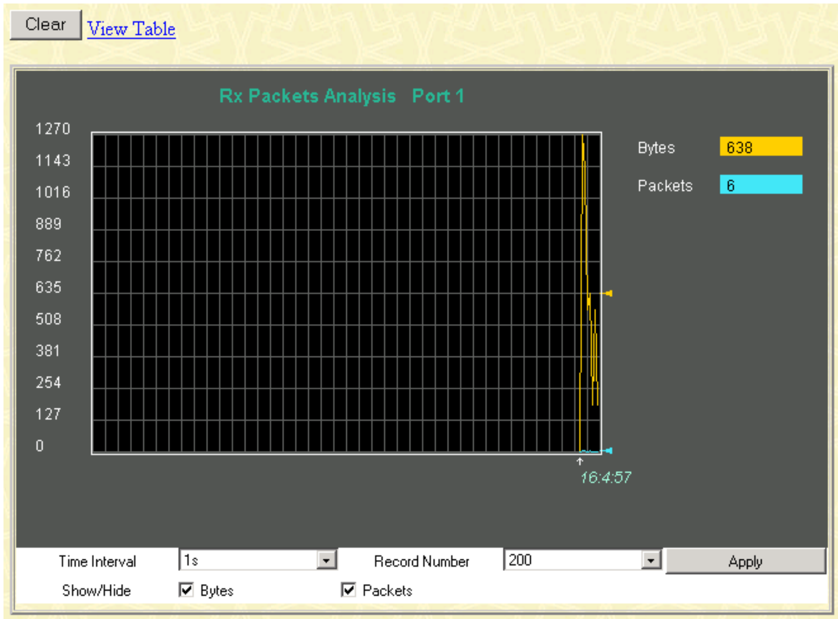
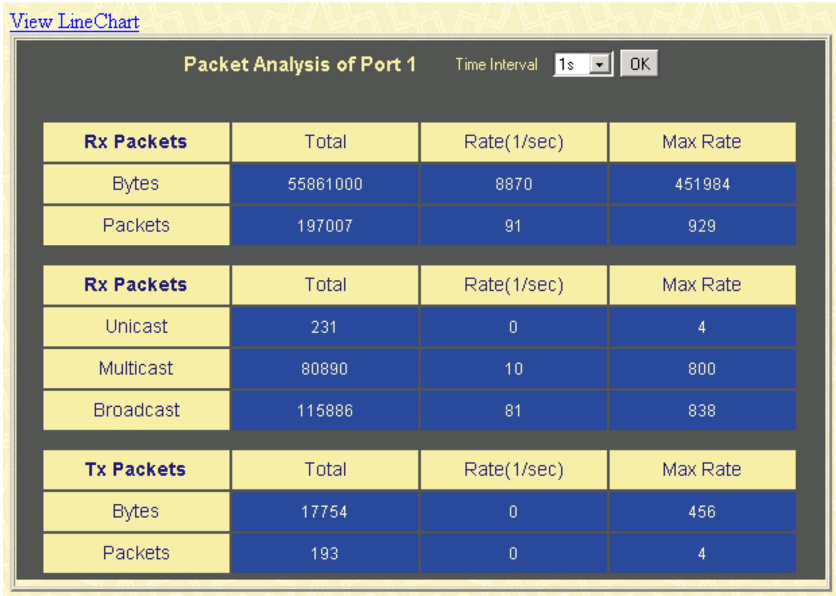


Figure 6- 93. Rx Packets Analysis window (line graph for Bytes and Packets)



View LineChart

Packet Analysis of Port 1   Time Interval 1s OK

Rx Packets	Total	Rate(1/sec)	Max Rate
Bytes	55861000	8870	451984
Packets	197007	91	929

Rx Packets	Total	Rate(1/sec)	Max Rate
Unicast	231	0	4
Multicast	80890	10	800
Broadcast	115886	81	838

Tx Packets	Total	Rate(1/sec)	Max Rate
Bytes	17754	0	456
Packets	193	0	4

Figure 6- 94. 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)

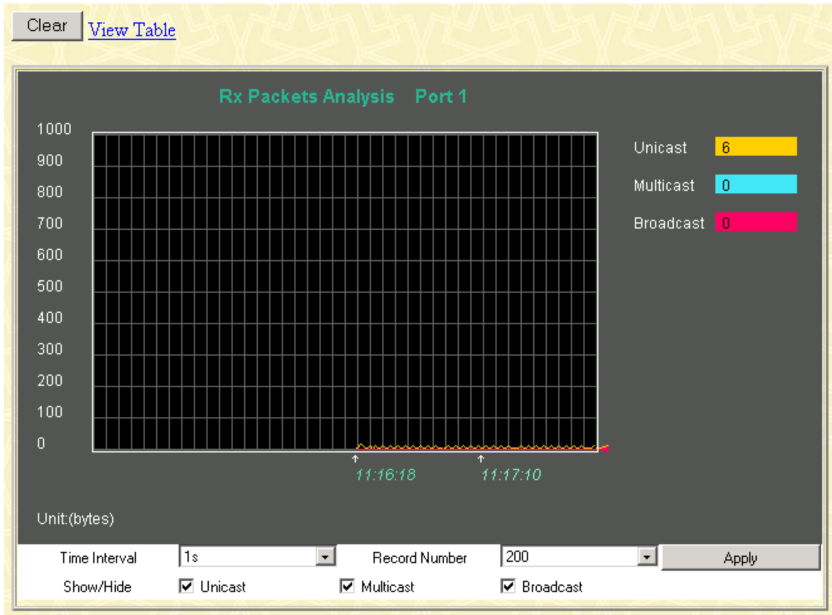
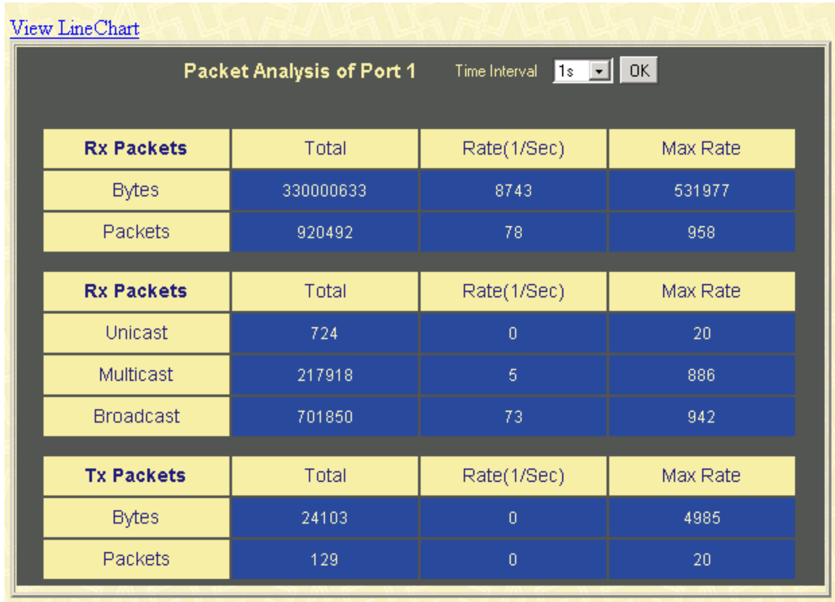


Figure 6- 95. Rx Packets Analysis window (line graph for Unicast, Multicast, and Broadcast Packets)



View LineChart

Packet Analysis of Port 1 — Time Interval 1s OK

Rx Packets	Total	Rate(1/Sec)	Max Rate
Bytes	330000633	8743	531977
Packets	920492	78	958

Rx Packets	Total	Rate(1/Sec)	Max Rate
Unicast	724	0	20
Multicast	217918	5	886
Broadcast	701850	73	942

Tx Packets	Total	Rate(1/Sec)	Max Rate
Bytes	24103	0	4985
Packets	129	0	20

Figure 6- 96. 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)

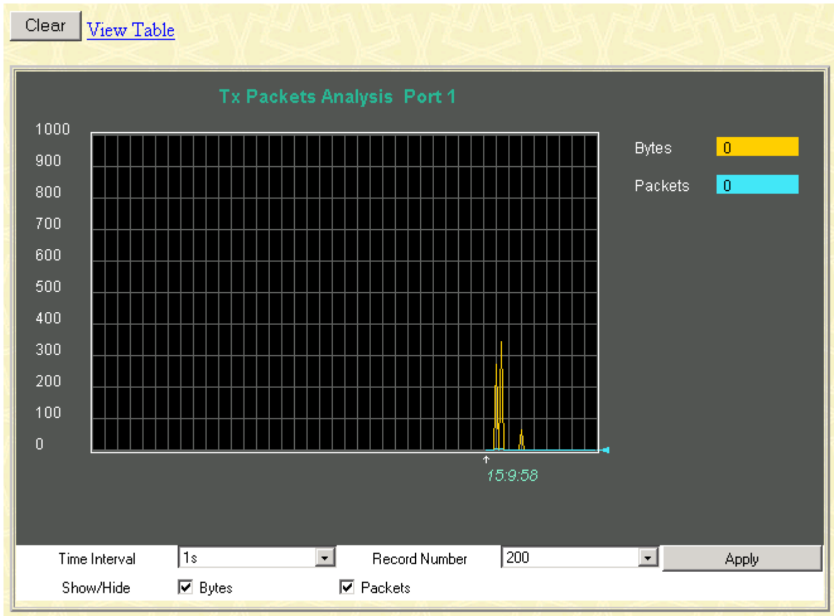


Figure 6- 97. Tx Packets Analysis window (line graph for Bytes and Packets)

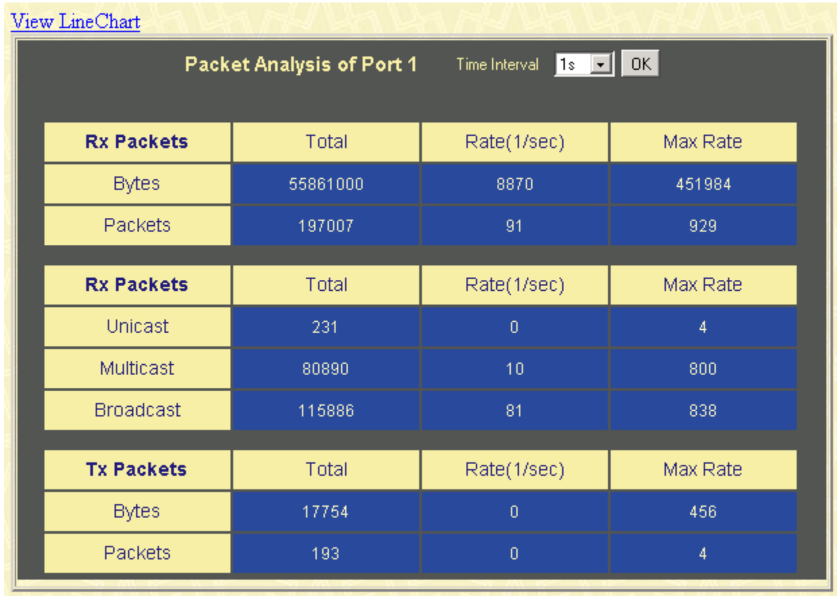


Figure 6- 98. Tx Packets Analysis window (table for Bytes and Packets)

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 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 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)

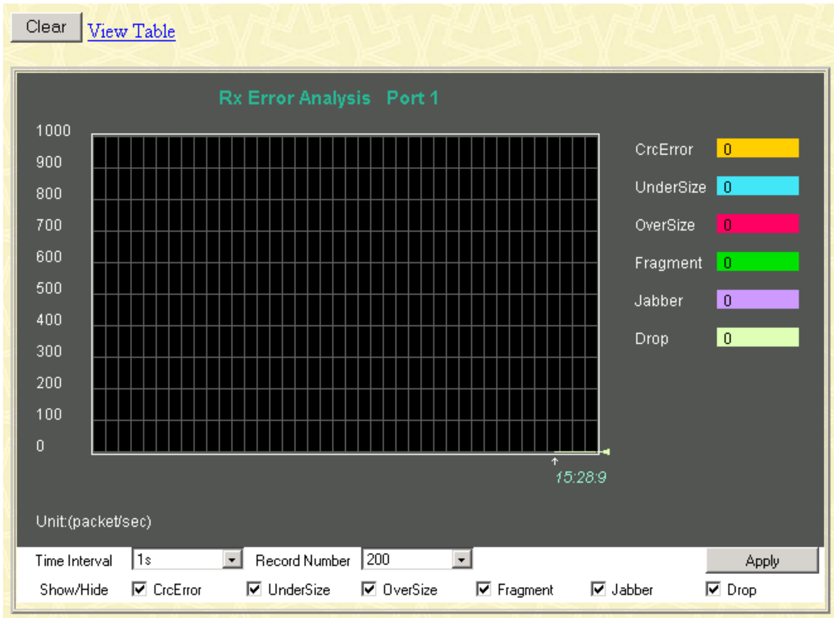
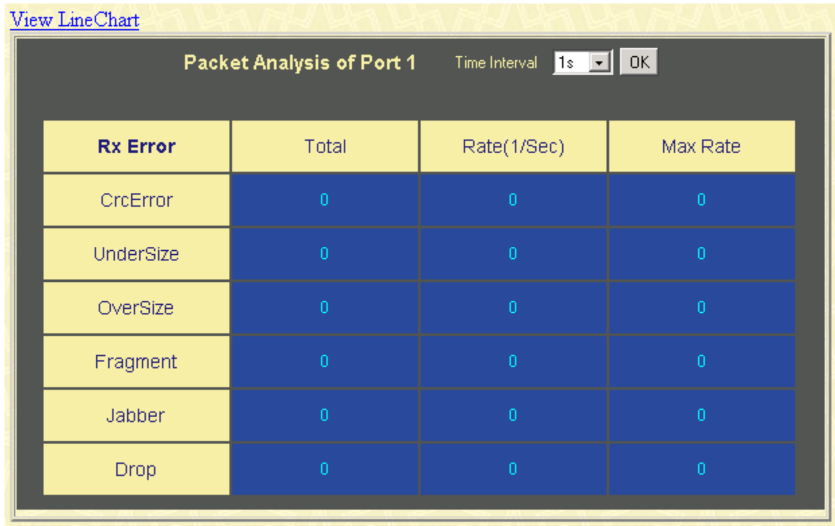


Figure 6- 99. Rx Error Analysis window (line graph)


View LineChart

Packet Analysis of Port 1 Time Interval 1s OK

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

Figure 6- 100. 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

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

than a table.

Transmitted (TX)

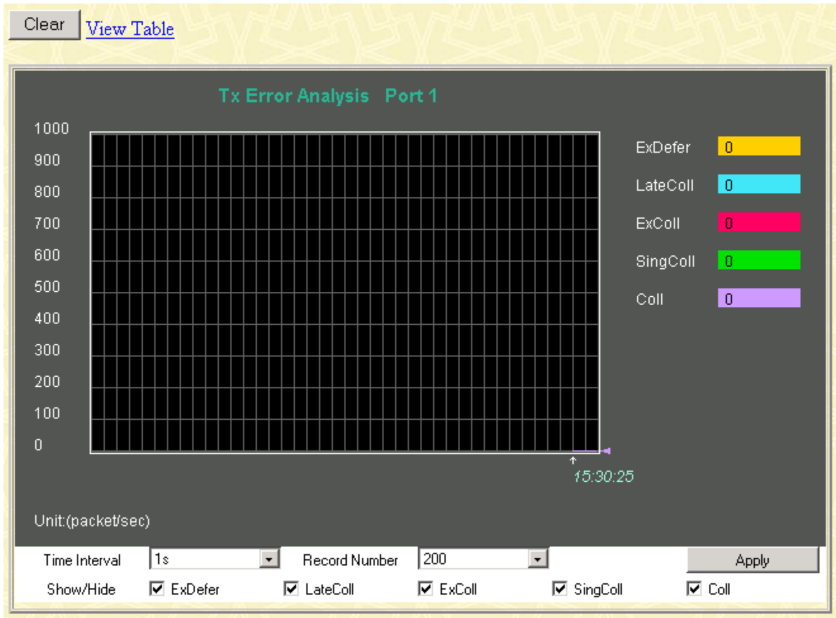


Figure 6- 101. Tx Error Analysis window (line graph)

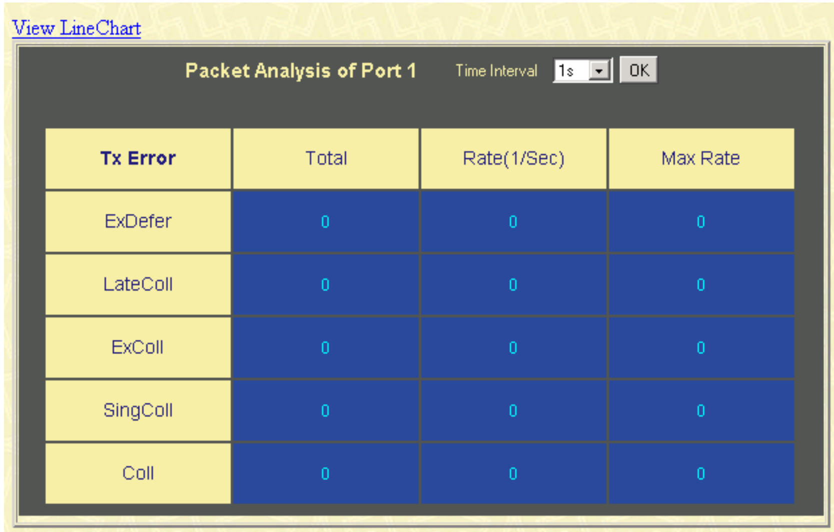


Figure 6- 102. Tx Error Analysis window (table)

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.*
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 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

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.

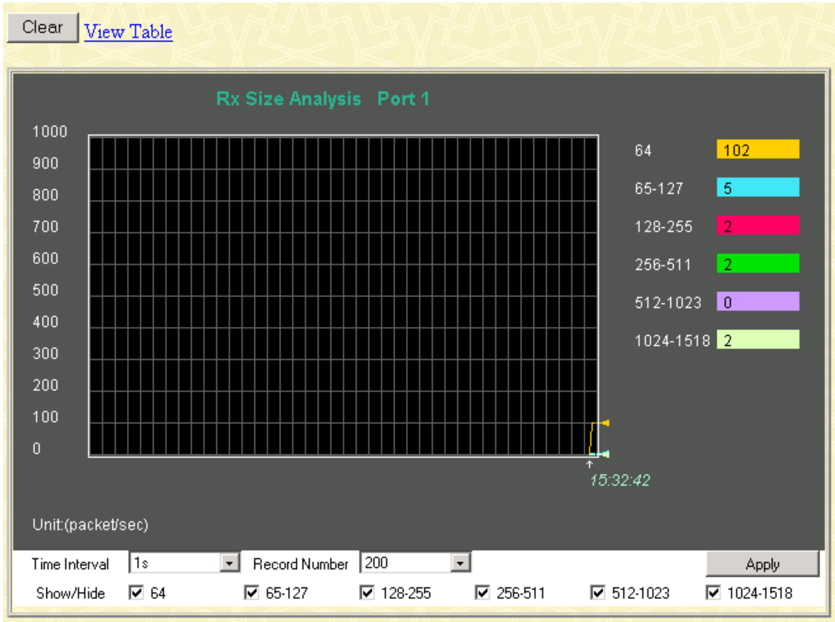
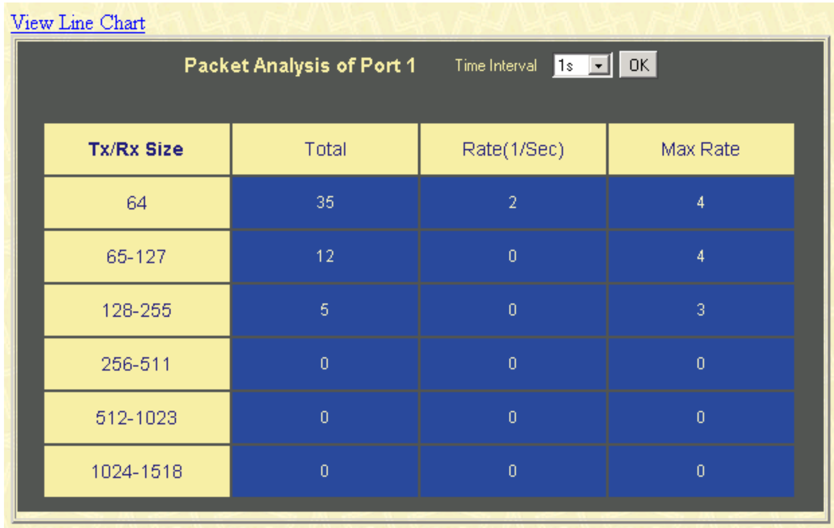


Figure 6- 103. Rx Size Analysis window (line graph)



Tx/Rx Size	Total	Rate(1/Sec)	Max Rate
64	35	2	4
65-127	12	0	4
128-255	5	0	3
256-511	0	0	0
512-1023	0	0	0
1024-1518	0	0	0

Figure 6- 104. 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).

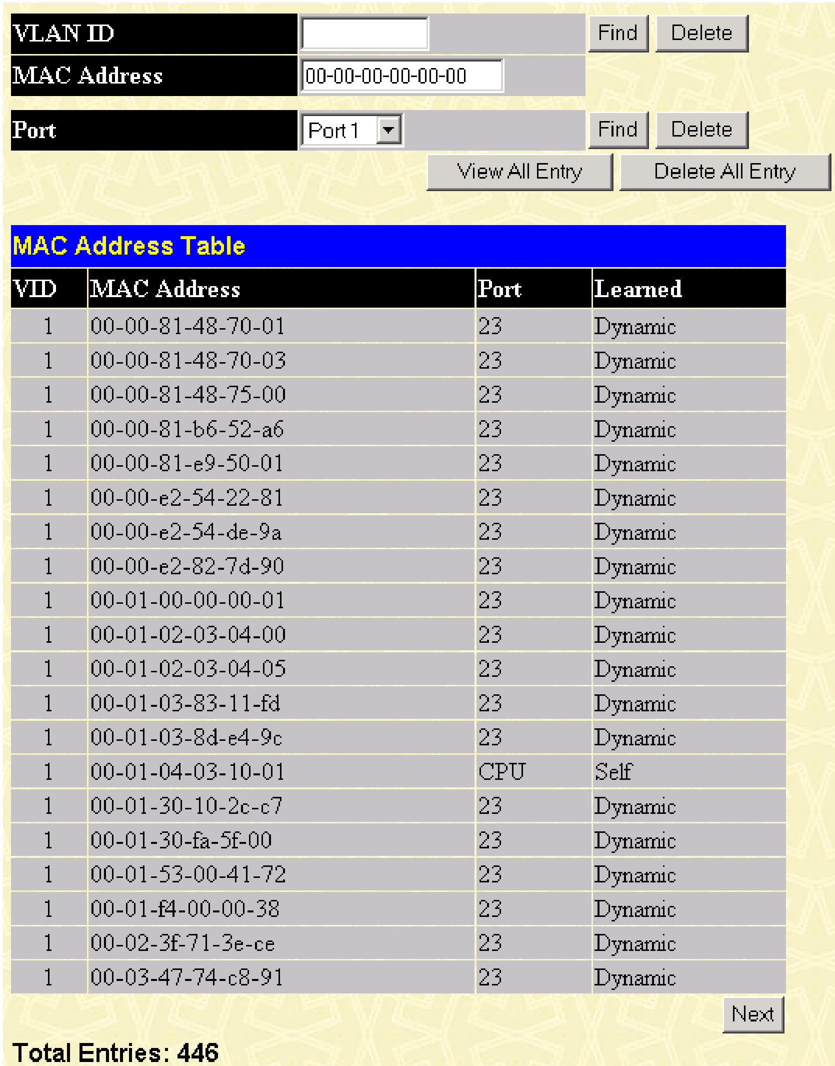
65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Show/Hide	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.
Clear	Clicking this button clears all statistics counters on this window.

	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:



VID	MAC Address	Port	Learned
1	00-00-81-48-70-01	23	Dynamic
1	00-00-81-48-70-03	23	Dynamic
1	00-00-81-48-75-00	23	Dynamic
1	00-00-81-b6-52-a6	23	Dynamic
1	00-00-81-e9-50-01	23	Dynamic
1	00-00-e2-54-22-81	23	Dynamic
1	00-00-e2-54-de-9a	23	Dynamic
1	00-00-e2-82-7d-90	23	Dynamic
1	00-01-00-00-00-01	23	Dynamic
1	00-01-02-03-04-00	23	Dynamic
1	00-01-02-03-04-05	23	Dynamic
1	00-01-03-83-11-fd	23	Dynamic
1	00-01-03-8d-e4-9c	23	Dynamic
1	00-01-04-03-10-01	CPU	Self
1	00-01-30-10-2c-c7	23	Dynamic
1	00-01-30-fa-5f-00	23	Dynamic
1	00-01-53-00-41-72	23	Dynamic
1	00-01-f4-00-00-38	23	Dynamic
1	00-02-3f-71-3e-ce	23	Dynamic
1	00-03-47-74-c8-91	23	Dynamic

Figure 6- 105. MAC Address Table window

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:

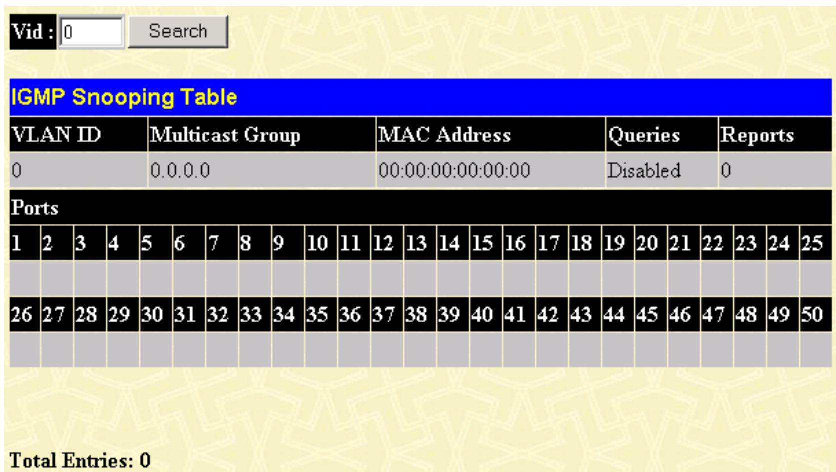


Figure 6- 106. IGMP Snooping Table window

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:

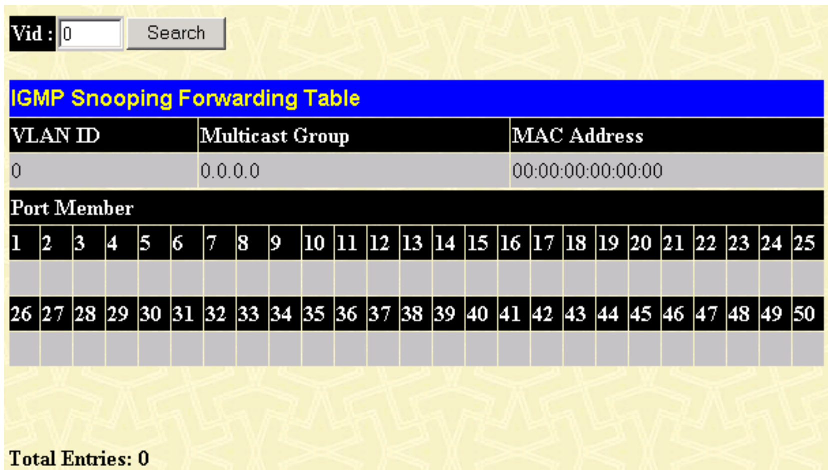


Figure 6- 107. IGMP Snooping Forwarding Table window

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

VLAN Status

Total VLAN Entries: 1

VLAN Status			
VLAN ID	VLAN Name	Status	Advertisemnet
1	default	static	Enabled

Tag Ports

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50

Egress Ports

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E

Figure 6- 108. 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:

Total VLAN Entries: 1

Router Port

VLAN ID	VLAN Name
1	default

Static Router Port

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50

Dynamic Router Port

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50

Figure 6- 109. Router Port window

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

Power Status

This read-only window displays power information.

To view the Power Status window, click on the Power Status link on the Monitoring menu:

Power Status

Power Number	Occupied State	Active State
Main Power Supply	Exist	Active
Redundant Power Supply	RPS exist	RPS inactive

Figure 6- 110. Power Status window

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

Port Access Control

This window displays port access control information.

To view Port Access Control information, click on the Port Access Control link on the Monitoring menu:

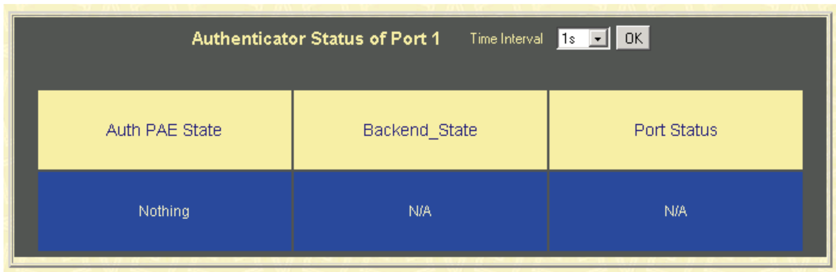


Figure 6- 111. Authenticator State window

Layer 3 feature

The windows in this section allow you to browse the switch's IP Address Table, Routing Table, ARP Table, IP Multicast Forwarding Table, IGMP Group Table, as well as OSPF, DVMRP, and PIM windows.

IP Address Table

To view the contents of the IP Address Table, click IP Address in the Layer 3 feature folder:

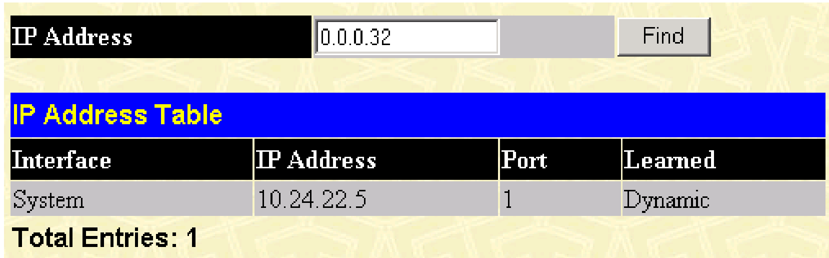


Figure 6- 112. IP Address Table window

The following fields are displayed:

Parameter	Description
Interface	Displays the IP interface name of the IP address destination.
IP Address	IP address of a learned or statically entered destination.
Port	Displays the port number of the IP address destination.
Learned	Displays whether the IP address is either statically or dynamically entered.

Routing Table

To view the contents of the Routing Table, click Routing Table in the Layer 3 feature folder:

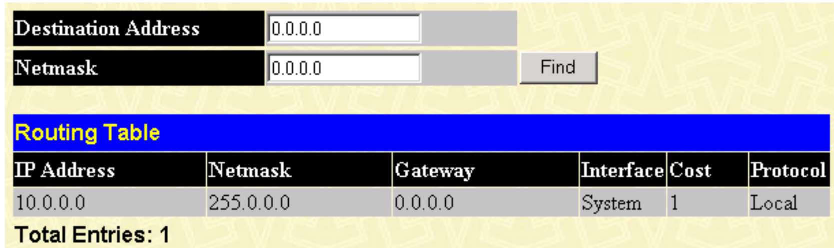


Figure 6- 113. Routing Table window

The following fields are displayed:

Parameter	Description
IP Address	The IP address of the remote device or subnet.
Netmask	The subnet mask corresponding to the IP address above.
Gateway	The IP address of the next hop router.
Interface	The name of the IP interface on which this router resides.
Cost	A numeric metric representing the relative performance difference or cost using this route versus another route to reach the remote device or subnet.
Protocol	The routing protocol in use by this route.

ARP Table

To view the contents of the ARP Table, click ARP Table in the Layer 3 feature folder:

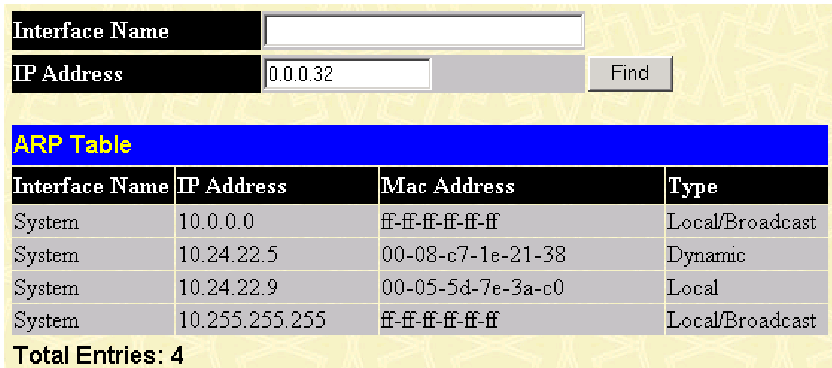


Figure 6- 114. ARP Table window

The following fields are displayed:

Parameter	Description
Interface Name	The name of the IP interface on which this router resides.
IP Address	The IP address of the remote device or subnet.
MAC Address	The hardware address of the device that is mapped.
Type	The type of Address Resolution Protocol (ARP) entry.

IP Multicast Forwarding Table

To view the contents of the IP Multicast Forwarding Table, click IP Multicasting Forwarding Table in the Layer 3 feature folder:

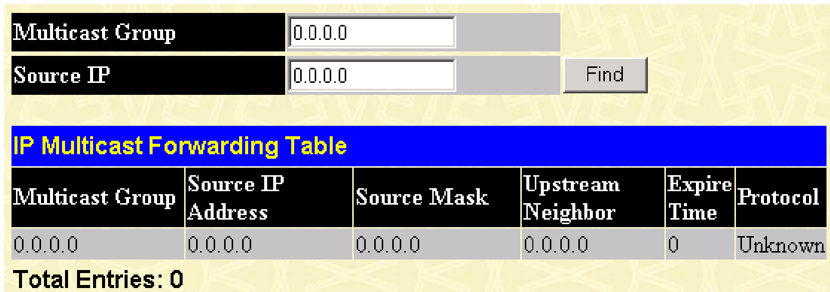


Figure 6- 115. IP Multicast Forwarding Table window

Parameter	Description
Multicast Group	The IP address of the multicast group.
Source IP Address	The IP address of the multicast source.
Source Mask	The subnet mask corresponding to the IP address above.
Upstream Neighbor	The IP address of the next router on the path from the switch to the multicast source.
Expire Time	Expiration time in seconds for this entry.
Protocol	The routing protocol in use.

IGMP Group Table

To view the contents of the IGMP Group Table, click IGMP Group Table in the Layer 3 feature folder:

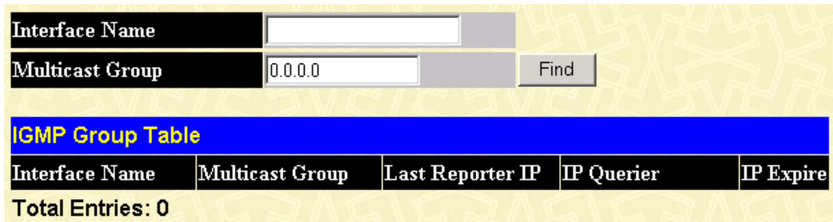


Figure 6- 116. IGMP Group Table window

Parameter	Description
Interface Name	The name of the IP interface the IGMP Group resides on.
Multicast Group	The IP address of the multicast group.
Last Reporter IP	The IP address of the last IGMP report sender.
IP Querier	The IP address of the IGMP querier.
IP Expire	Expiration time in seconds for this group.

OSPF Monitor

The switch maintains two OSPF Link State Databases (LSDB) – Internal and External. The Internal LSDB describes the Link State Advertisements (LSA) for OSPF Antonymous Systems (AS). The External LSDB describes the LSAs for those ASs not belonging to OSPF.

The internal OSPF Link State Database (LSDB) table can be viewed using the Web-based manager.

To view the switch's OSPF LSDB Table, click OSPF LSDB Table in the OSPF Monitor folder:

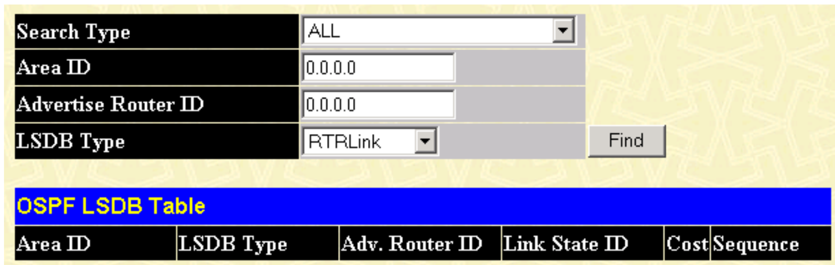


Figure 6- 117. OSPF LSDB Table window

The following fields can be set or are displayed:

Parameter	Description
Area ID	Displays the OSPF Area ID.
LSDB Type	Displays which one of five types of link advertisements by which the current link was discovered by the switch – Router link (*RTRLink*), Network link (*NETLink*), Summary link (*Summary*), Autonomous System link (*ASSummary*), Autonomous External System link (*ASExtLink*), or *ALL*.
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 5 The destination network's IP address.
Cost	Displays the routing metric associated with the link.
Sequence	Displays a sequence number corresponding to number of times the current link has been advertised as changed.

To view the switch's OSPF Neighbor Table, click OSPF Neighbor Table in the OSPF Monitor folder:

OSPF Neighbor Table

IP Address of Neighbor	Router ID of Neighbor	Neighbor Prority	Neighbor State

Total Entries: 0

Figure 6- 118. OSPF Neighbor Table window

The following fields are displayed.

Parameter	Description
IP Address of Neighbor	The IP address of the neighboring router.

Router ID of Neighbor	The router ID of a neighboring router.
Neighbor Priority	The priority value of the neighboring router.
Neighbor State	Indicates the relationship between the switch and the neighbor router.

To view the switch's OSPF Virtual Neighbor Table, click OSPF Virtual Neighbor Table in the OSPF Monitor folder:

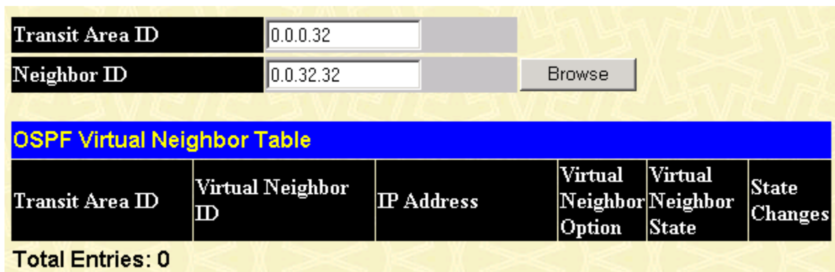


Figure 6- 119. OSPF Virtual Neighbor Table window

The following fields can be set or are displayed.

Parameter	Description
Transit Area ID	The area ID of the transit area that the virtual link resides on.
Virtual Neighbor ID	The router ID of the neighboring router via the virtual link.
IP Address	The IP address of the neighboring router.
Virtual	This field indicates whether the neighbor

Neighbor Option	router can accept OSPF optional operation within its OSPF domain. For example, TOS routing.
Virtual Neighbor State	Indicates the relationship between the switch and the neighbor router.
State Changes	The number of times the neighbor router has changed state.

DVMRP Monitor

To view the switch's DVMRP Routing Table, click DVMRP Routing Table in the DVMRP Monitor folder:

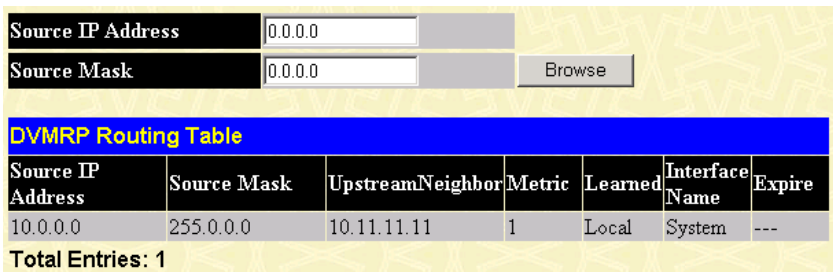


Figure 6- 120. DVMRP Routing Table window

The Source IP Address and Source Mask fields allow the entry of an IP address and corresponding subnet mask to search the table for. Click **Browse** and the DVMRP Routing table will be searched for the IP address and subnet mask above.

The following fields are displayed.

Parameter	Description
Source IP Address	The IP address of the DVMRP router.

Source Mask	The subnet mask corresponding to the IP address above.
UpstreamNeighbor	The IP address of the next hop router.
Metric	The cost that is between the switch and the source IP address above.
Learned	Indicates whether this entry is dynamic (learned) or not.
Interface Name	The name of the IP interface the upstream neighbor resides on.
Expire	The route's expiration time in seconds.

To view the switch's DVMRP Neighbor Address Table, click DVMRP Neighbor Address Table in the DVMRP Monitor folder:

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

Figure 6- 121. DVMRP Neighbor Address Table window

The following fields are displayed.

Parameter	Description
Interface Name	The name of the IP interface the router resides on.
Neighbor Address	IP address of the DVMRP neighbor.

Address	
Generation ID	The generation ID of the DVMRP neighbor.
Expire Time	Time in seconds until the DVMRP neighbor information expires.

To view the switch's DVMRP Routing Next Hop Table, click DVMRP Routing Next Hop Table in the DVMRP Monitor folder:

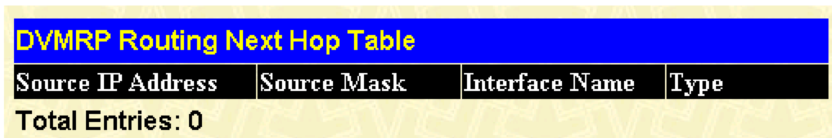


Figure 6- 122. DVMRP Routing Next Hop Table window

The following fields are displayed.

Parameter	Description
Source IP Address	The network address which, when combined with the corresponding next hop Source Mask value, identifies the source for which this entry specifies a next hop on an outgoing interface.
Source Mask	The network mask which, when combined with the corresponding next hop Source value, identifies the source for which this entry specifies a next hop on an outgoing interface.
Interface Name	The name of the IP interface this entry resides on.

Type	The type is leaf if no downstream dependent neighbors exist on the outgoing virtual interface. Otherwise, the type is branch.

PIM Monitor

To view the switch's PIM Neighbor Address Table, click PIM Neighbor Address Table in the PIM Monitor folder:

Figure 6- 123. PIM Neighbor Address Table window

The following fields can be set or are displayed.

Parameter	Description
Interface Name	The name of the IP interface where this PIM neighbor router entry resides.
Neighbor Address	The IP address of the PIM neighbor router.
Expire Time	Time in seconds until the PIM Neighbor Address Table information expires.

Maintenance

The **Maintenance** menu consists of the following folders and windows: **TFTP Services**, **Switch History**, **Ping Test**, **Save Changes**, **Reboot Services**, and **Logout**. See below for further description.

TFTP Services

Trivial File Transfer Protocol (TFTP) services allow the switch firmware to be upgraded by transferring a new firmware file from a TFTP server to the switch. A configuration file can also be loaded into the switch from a TFTP server, switch settings can be saved to the TFTP server, and a history log can be uploaded from the switch to the TFTP server.

Download Firmware 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:

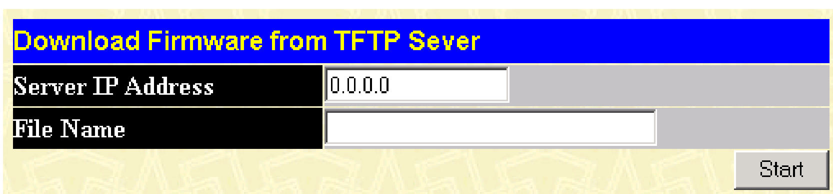


Figure 6- 124. Download Firmware from Server window

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** folder 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's, click on the Maintenance folder and then the TFTP Services folder and finally click on the Download Settings from TFTP Server link:

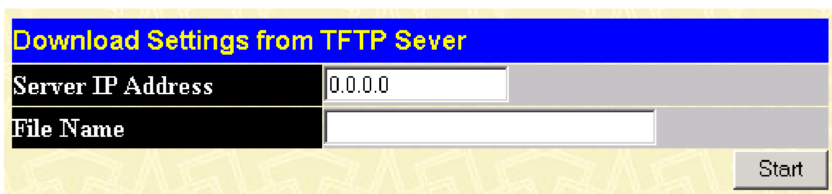


Figure 6- 125. Download Settings from TFTP Server window

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

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:

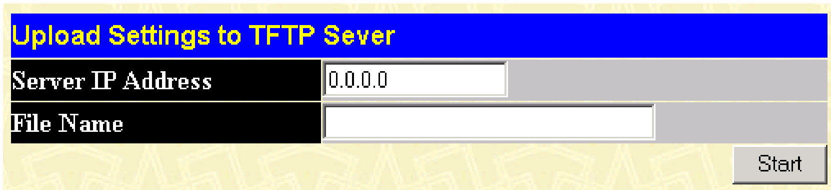


Figure 6- 126. Upload Settings to TFTP Server window

Enter the IP address of the TFTP server and the path and filename of the settings file on the TFTP server.

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:

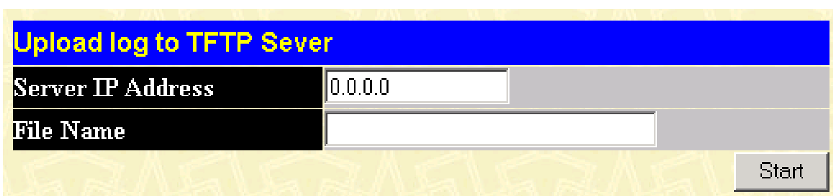


Figure 6- 127. Upload log to TFTP Server window

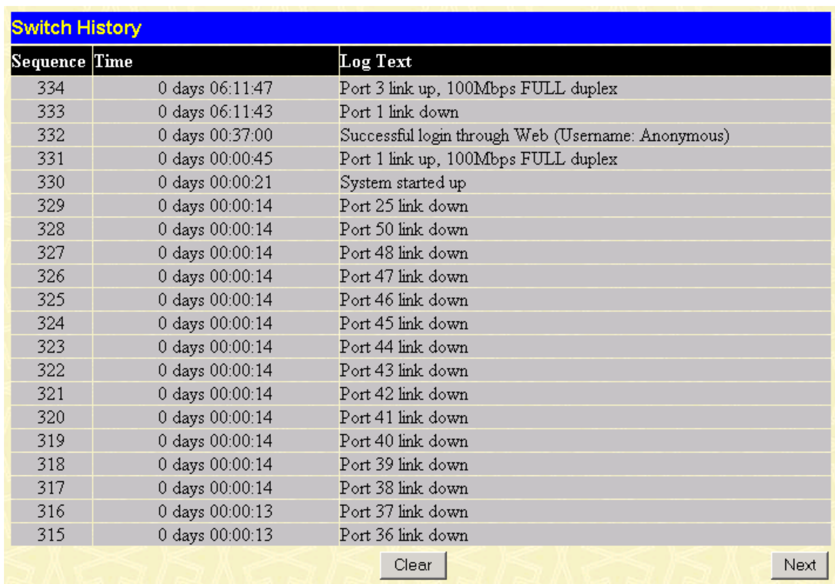
Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server.

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
334	0 days 06:11:47	Port 3 link up, 100Mbps FULL duplex
333	0 days 06:11:43	Port 1 link down
332	0 days 00:37:00	Successful login through Web (Username: Anonymous)
331	0 days 00:00:45	Port 1 link up, 100Mbps FULL duplex
330	0 days 00:00:21	System started up
329	0 days 00:00:14	Port 25 link down
328	0 days 00:00:14	Port 50 link down
327	0 days 00:00:14	Port 48 link down
326	0 days 00:00:14	Port 47 link down
325	0 days 00:00:14	Port 46 link down
324	0 days 00:00:14	Port 45 link down
323	0 days 00:00:14	Port 44 link down
322	0 days 00:00:14	Port 43 link down
321	0 days 00:00:14	Port 42 link down
320	0 days 00:00:14	Port 41 link down
319	0 days 00:00:14	Port 40 link down
318	0 days 00:00:14	Port 39 link down
317	0 days 00:00:14	Port 38 link down
316	0 days 00:00:13	Port 37 link down
315	0 days 00:00:13	Port 36 link down

Figure 6- 128. 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.

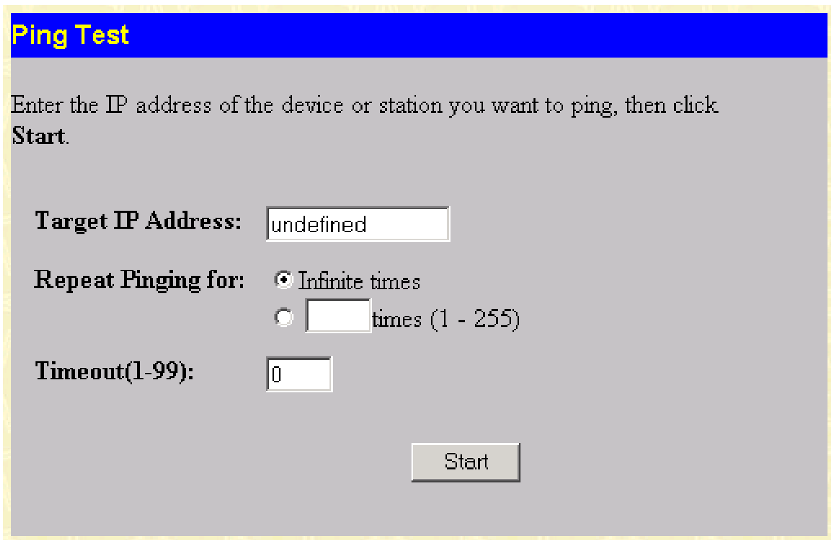


Figure 6- 129. Ping Test window

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.

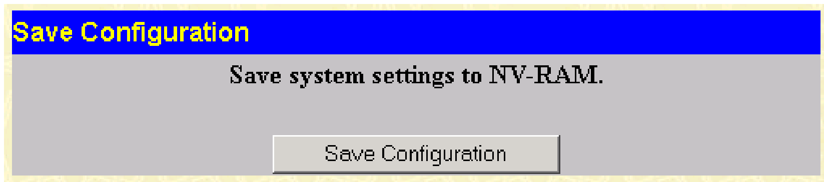


Figure 6- 130. Save Configuration window

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

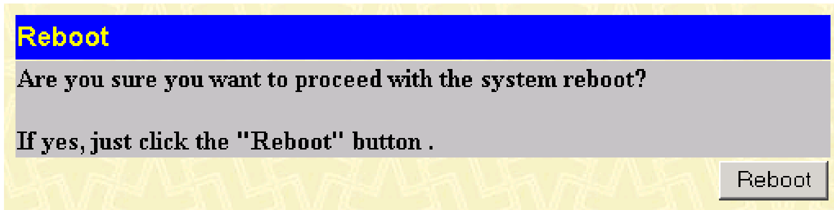


Figure 6- 131. Reboot window

Reset

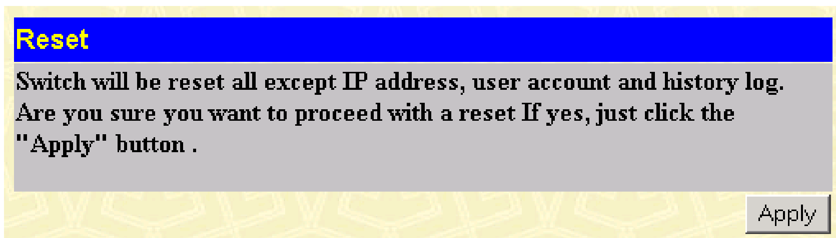


Figure 6- 132. Reset window

Reset System

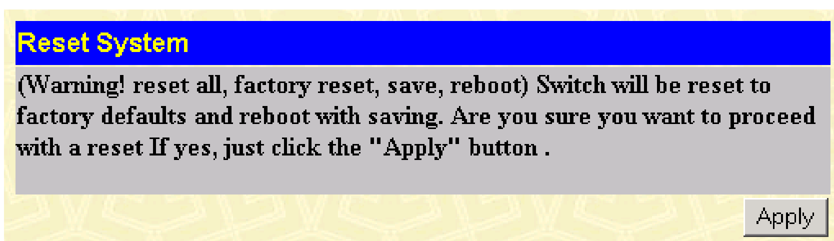


Figure 6- 133. Reset System window

Reset Config

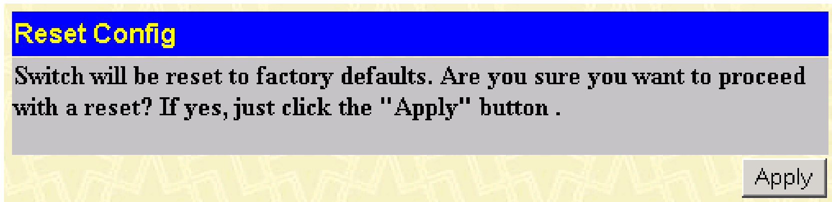


Figure 6- 134. Reset Config window

Logout

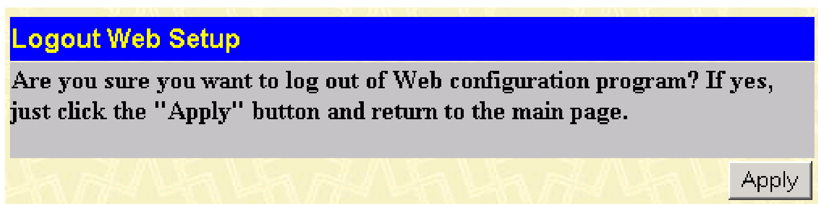


Figure 6- 135. Logout Web Setup window

Click **Apply** if you want to logout of the Web configuration program and return to the main page.

7

WARRANTY AND REGISTRATION

All countries and regions except 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 Bedienungsanleitung 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 größer 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 date of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.

Warranty service may be obtained by contacting a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing/shipping/insurance prepaid. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.

Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

Software:

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system/platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system/platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.

USA Only

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited warranty for its product only to the person or entity that originally purchased the product from:

- D-Link or its authorized reseller or distributor and
- Products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, and U.S. Military Installations, addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link products described below will be free from material defects in workmanship and materials from the date of original retail purchase of the product, for the period set forth below applicable to the product type ("Warranty Period"), except as otherwise stated herein.

5-Year Limited Warranty for the Product(s) is defined as follows:

- Hardware (excluding power supplies and fans) Five (5) Years
- Power Supplies and Fans Three (3) Year
- Spare parts and spare kits Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund at D-Link's sole discretion. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or have an identical make, model or part. D-Link may in its sole discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement Hardware will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund at D-Link's sole discretion. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Software will be warranted for the remainder of the original Warranty Period from the date or original retail purchase. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for hardware and software of D-Link's products, will not be applied to and does not cover any 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: Any claim under this limited warranty must be submitted in writing before the end of the Warranty Period to an Authorized D-Link Service Office.

- The customer must submit as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.
- The original product owner must obtain a Return Material Authorization ("RMA") number from the Authorized D-Link Service Office and, if requested,

provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the Product and will not ship back any accessories.
- The customer is responsible for all shipping charges to D-Link. No Charge on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products should be fully insured by the customer and shipped to D-Link Systems, Inc., 53 Discovery Drive, Irvine, CA 92618. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: This limited warranty provided by D-Link does not cover: Products, if in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. Repair by anyone other than D-Link or an Authorized D-Link Service Office will void this Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT,

INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

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 ANSI/IEEE 802.3 Nway auto-negotiation	
Protocols:	CSMA/CD	
Data Transfer Rates:	Half-duplex	Full-duplex
Ethernet	10 Mbps	20Mbps
Fast Ethernet	100Mbps	200Mbps
Gigabit Ethernet	n/a	2000Mbps
Topology:	Star	

	General
Network Cables: 10BASE-T: 100BASE-TX: Mini GBIC:	 2-pair UTP Cat. 3,4,5 (100 m) EIA/TIA- 568 100-ohm STP (100 m) 2-pair UTP Cat. 5 (100 m) EIA/TIA-568 100-ohm STP (100 m) 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 Enviroı mental
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:	-25 to 55 degrees Celsius
Humidity:	Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing
Dimensions:	441 mm x 207 mm x 44 mm (1U), 19 inch rack-mount width

	Physical and Environmental
	mount width
Weight:	4.4 kg
EMI:	FCC Class A, CE Class A
Safety:	CSA International

	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.

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.

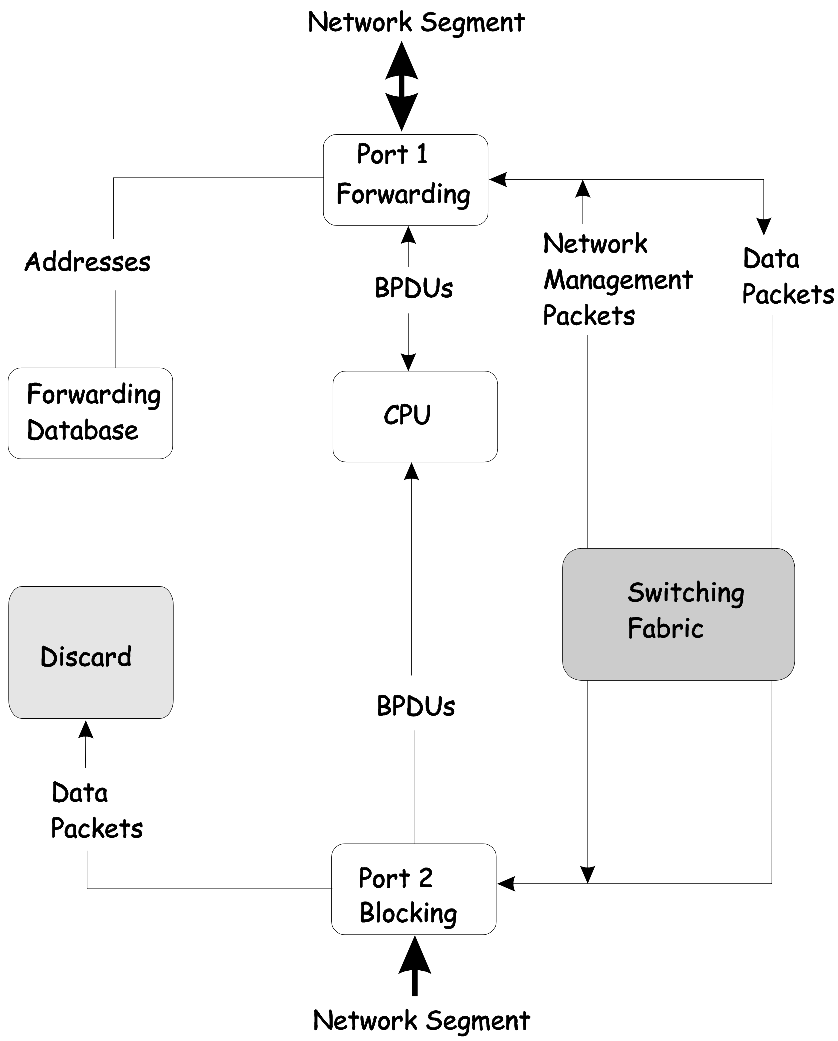
- The expiration of the forwarding delay timer moves the port to the forwarding state, where both learning and forwarding are enabled. At this point, packets are forwarded by the port.

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.



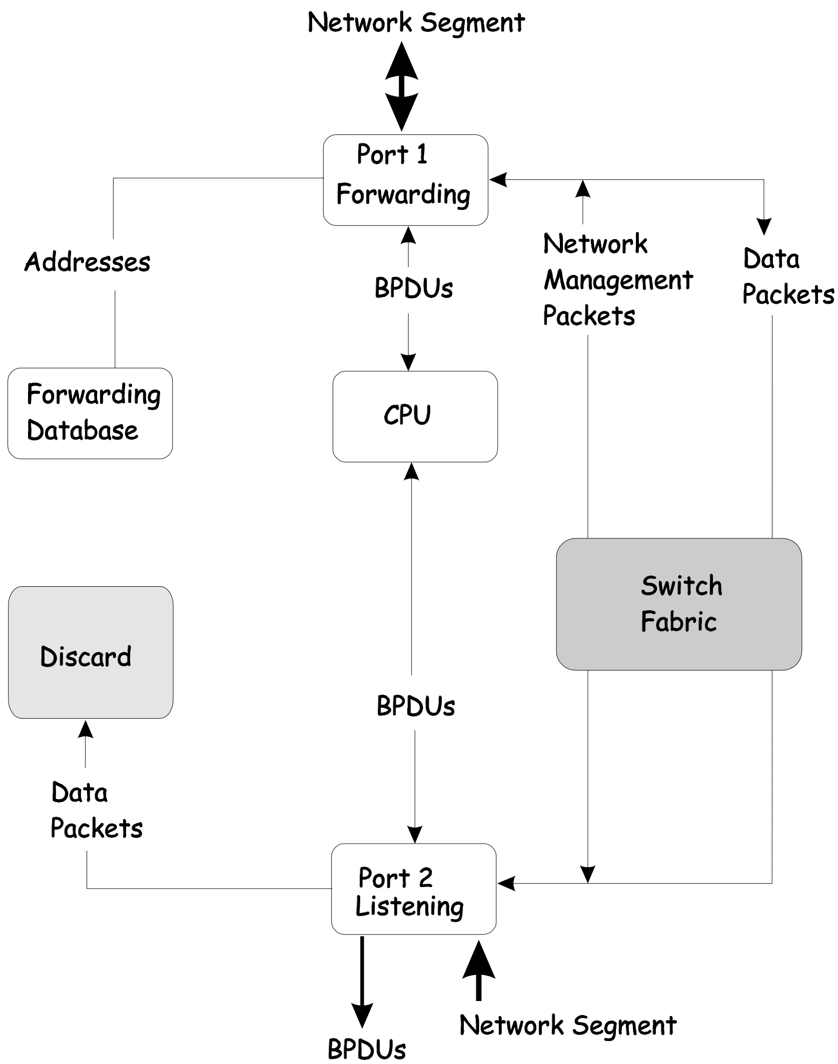
Listening State

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.

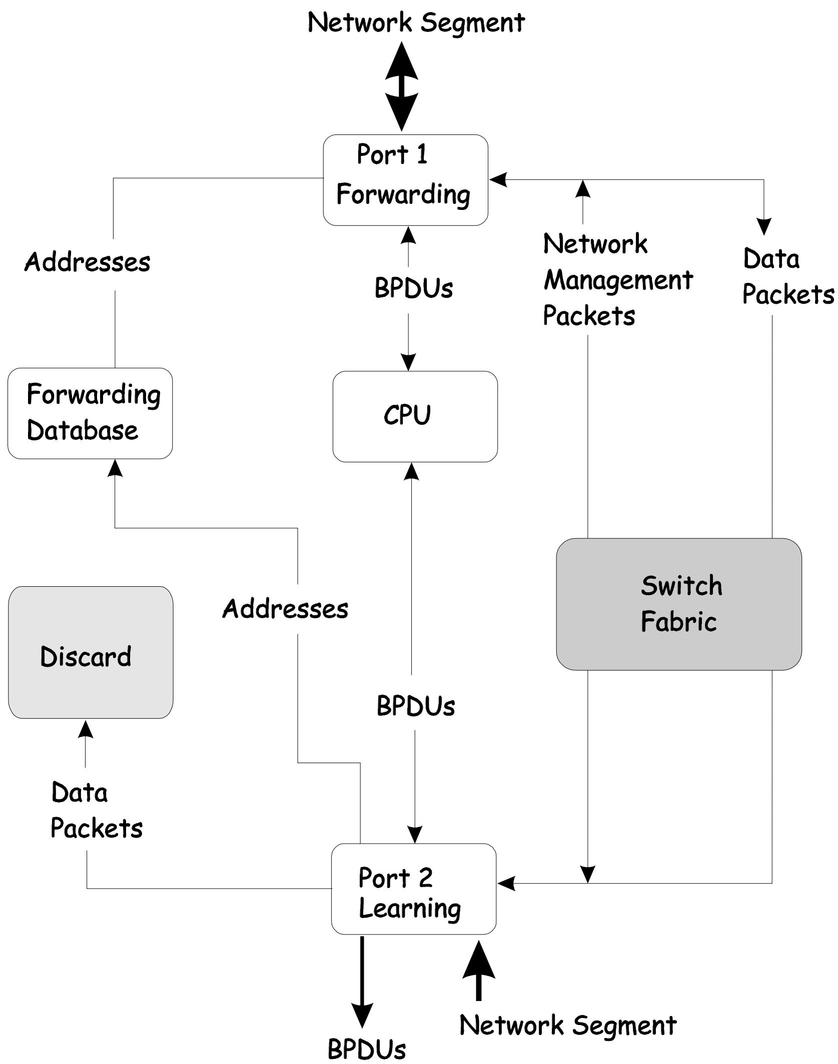


Learning State

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.

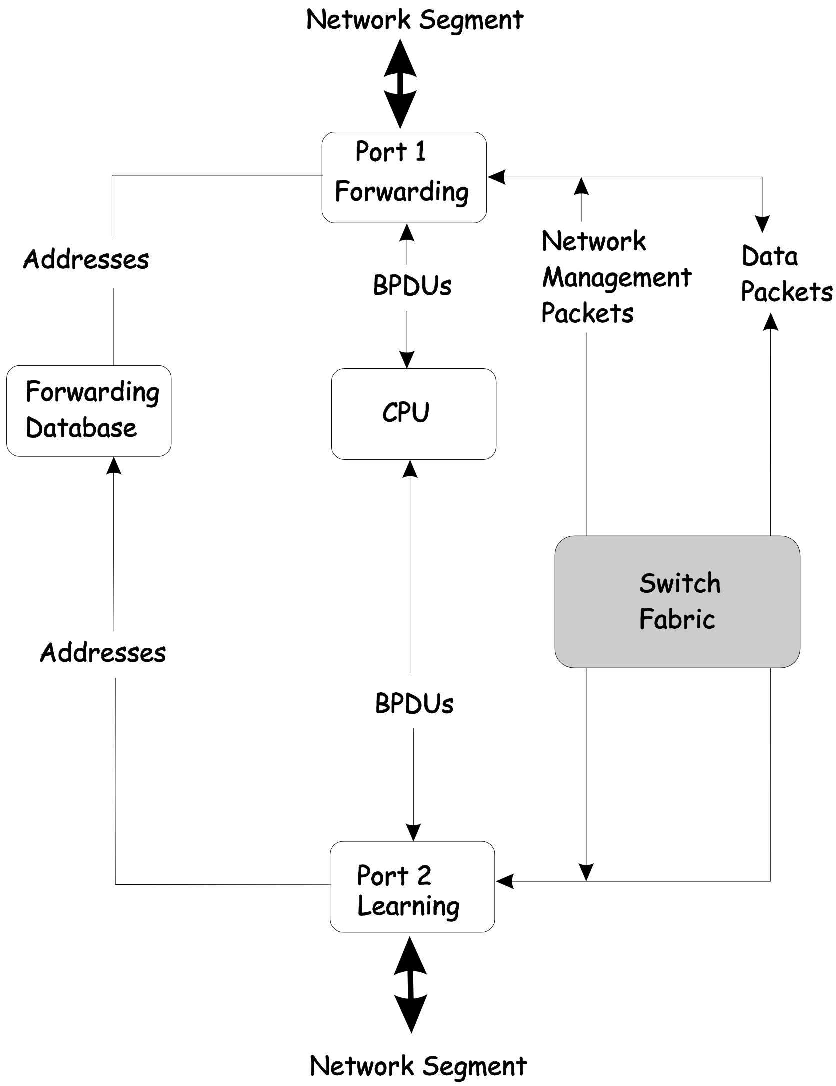


Forwarding State

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.

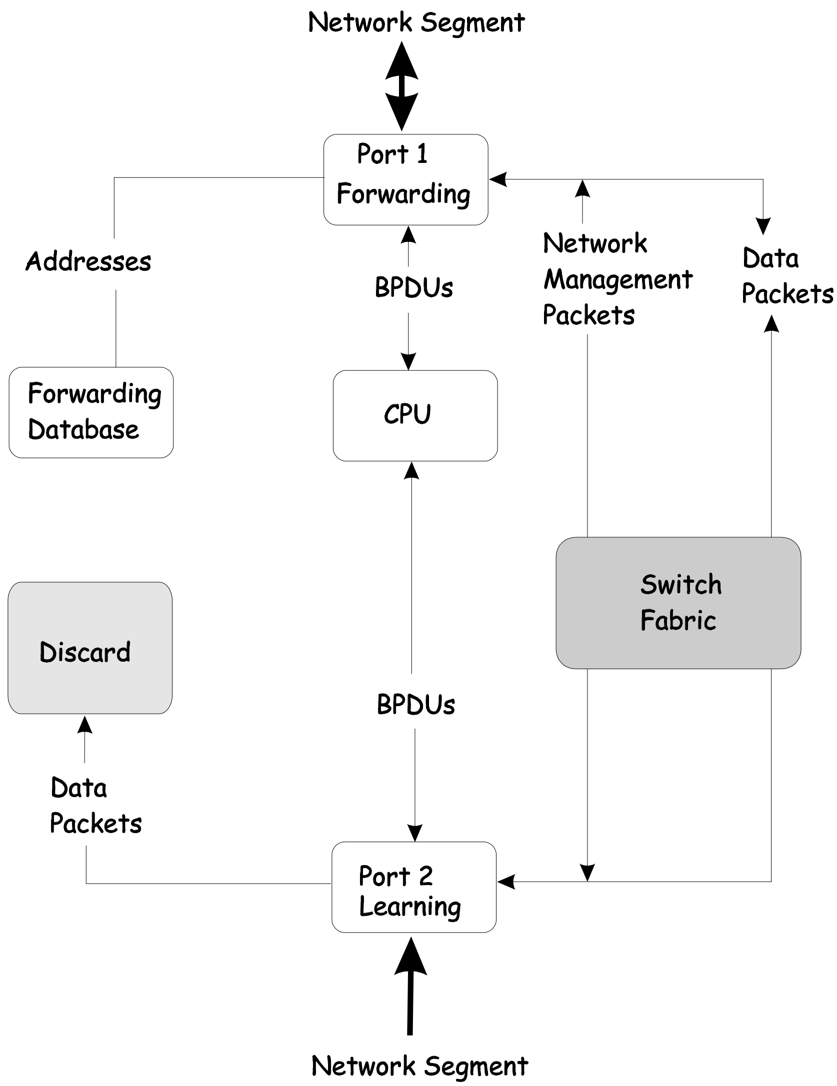


Disabled State

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:

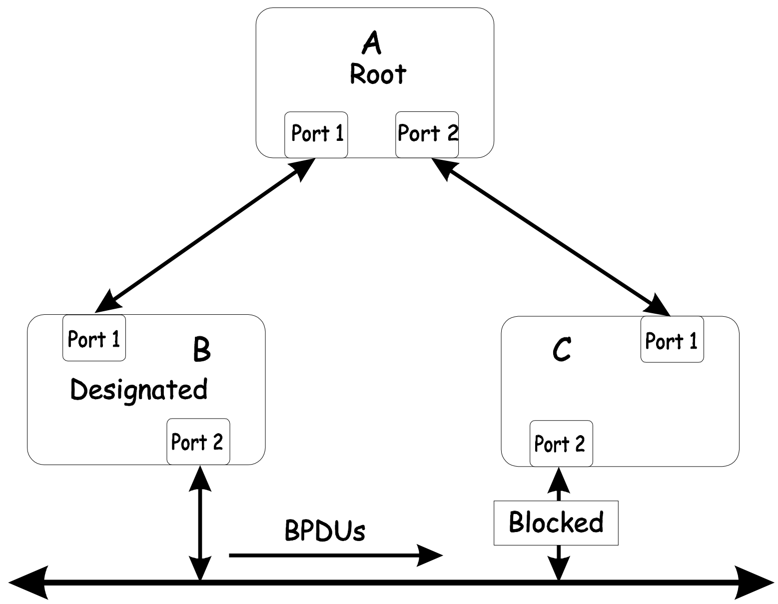
- Discards packets received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database.
- Receives BPDUs, but does not direct them to the system CPU.
- Does not receive BPDUs for transmission from the system CPU.
- Receives and responds to network management messages.


Network Segment
Port 1
Forwarding
Addresses
BPDUs
Network
Management
Packets
Data
Packets
Forwarding
Database
CPU
Switch
Fabric
Discard
BPDUs
Data
Packets
Port 2
Learning
Network Segment

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.



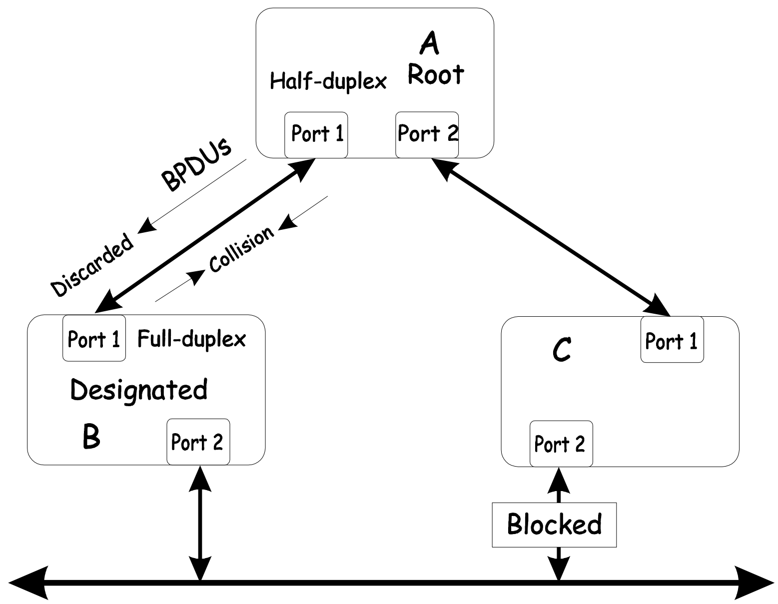
In this example, B has been elected as the designated bridge and port 2 on C is in the blocking state. The election of B as the designated bridge is determined by the exchange of BPDUs between B and C. B had a better BPDU than C. B continues sending BPDUs advertising its superiority over the other bridges 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.

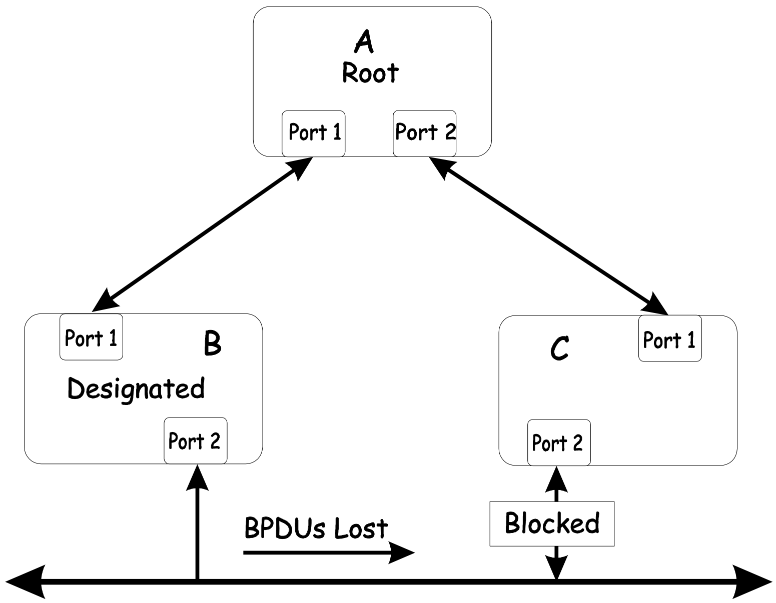


In the above example, port 1 on B is configured as a full-duplex port and port 1 on A is either configured as a half-duplex port, or left in auto-negotiation mode. Because port 1 on B is configured as a full-duplex port, it does not do the carrier sense when accessing the link. B will then start sending 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.

C

BRIEF REVIEW OF BITWISE LOGICAL OPERATIONS

AND

The logical AND operation compares 2 bits and if they are both "1", then the result is "1", otherwise, the result is "0".

	0	***1***
0	0	0
1	0	1

OR

The logical OR operation compares 2 bits and if either or both bits are "1", then the result is "1", otherwise, the result is "0".

	0	***1***
0	0	1
1	1	1

XOR

The logical XOR (exclusive OR) operation compares 2 bits and if exactly one of them is a "1", then the result is "1", otherwise the result is "0".

	0	*1*
0	0	1
1	1	0

NOT

The logical NOT operation simply changes the value of a single bit. If it is a "1", the result is "0", if it is a "0", the result is "1". This operation is carried out on a single bit.

0	*1*
1	0

INDEX

D-Link Offices

Australia	**D-Link Australasia** 1 Giffnock Avenue, North Ryde, NSW 2113, Sydney, Australia TEL: 61-2-8899-1800 FAX: 61-2-8899-1868 TOLL FREE (Australia): 1800-177100 TOLL FREE (New Zealand): 0800-900900 URL: www.dlink.com.au E-MAIL: support@dlink.com.au & info@dlink.com.au Level 1, 434 St. Kilda Road, Melbourne, Victoria 3004 Australia TEL: 61-3-9281-3232 FAX: 61-3-9281-3229 MOBILE: 0412-660-064
Canada	**D-Link Canada** 2180 Winston Park Drive, Oakville, Ontario, L6H 5W1 Canada TEL: 1-905-829-5033 FAX: 1-905-829-5095 BBS: 1-965-279-8732 TOLL FREE: 1-800-354-6522 URL: www.dlink.ca FTP: ftp.dlinknet.com E-MAIL: techsup@dlink.ca
Chile	**D-Link South America** Isidora Goyenechea 2934 Of. 702, Las Condes Fono, 2323185, Santiago, Chile, S. A. TEL: 56-2-232-3185 FAX: 56-2-232-0923 URL: www.dlink.cl E-MAIL: ccasassu@dlink.cl & tsilva@dlink.cl
China	**D-Link China** 15th Floor, Science & Technology Tower, No.11, Baishiqiao Road, Haidan District, 100081 Beijing, China TEL: 86-10-68467106 FAX: 86-10-68467110 URL: www.dlink.com.cn E-MAIL: liweii@digitalchina.com.cn
Denmark	**D-Link Denmark** Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark TEL: 45-43-969040 FAX:45-43-424347 URL: www.dlink.dk E-MAIL: info@dlink.dk
Egypt	**D-Link Middle East** 7 Assem Ebn Sabet Street, Heliopolis, Cairo, Egypt TEL: 20-2-635-6176 FAX: 20-2-635-6192 URL: www.dlink-me.com E-MAIL: support@dlink-me.com & fateen@dlink-me.com

Finland	**D-Link Finland** Pakkalankuja 7A, FIN– 0150 VANTAA, Finland TEL: 358-9-2707-5080 FAX: 358-9-2702-5081 URL: www.dlink-fi.com
France	**D-Link France** Le Florilege, No. 2, Allea de la Fresnerie, 78330 Fontenay Le Fleury, France TEL: 33-1-3023-8688 FAX: 33-1-3023-8689 URL: www.dlink-france.fr E-MAIL: info@dlink-france.fr
Germany	**D-Link Central Europe/D-Link Deutschland GmbH** Schwalbacher Strasse 74, D-65760 Eschborn, Germany TEL: 49-6196-77990 FAX: 49-6196-7799300 URL: www.dlink.de BBS: 49-(0) 6192-971199 (analog) BBS: 49-(0) 6192-971198 (ISDN) INFO: 00800-7250-0000 (toll free) HELP: 00800-7250-4000 (toll free) REPAIR: 00800-7250-8000 E-MAIL: info@dlink.de
India	**D-Link India** Plot No.5, Bandra-Kurla Complex Rd., Off Cst Rd., Santacruz (East), Mumbai, 400 098 India TEL: 91-022-652-6696/6578/6623 FAX: 91-022-652-8914/8476 URL: www.dlink-india.com, www.dlink.co.in & tushars@dlink-india.com E-MAIL: service@dlink.india.com
Italy	**D-Link Mediterraneo Srl/D-Link Italia** Via Nino Bonnet n. 6/B, 20154, Milano, Italy TEL: 39-02-2900-0676 FAX: 39-02-2900-1723 URL: www.dlink.it E-MAIL: info@dlink.it
Japan	**D-Link Japan** 10F, 8-8-15 Nishigotahda, Shinagawa, Tokyo 141, Japan TEL: 81-3-5434-9678 FAX: 81-3-5434-9868 URL: www.d-link.co.jp E-MAIL: kida@d-link.co.jp
Netherlands	**D-Link Benelux** Fellenoord 1305611 ZB, Eindhoven, the Netherlands TEL: 31-40-2668713 FAX: 31-40-2668666 URL: www.d-link-benelux.nl
Norway	**D-Link Norway** Waldemar Thranesgate 77, 0175 Oslo, Norway TEL: 47-22-991890 FAX: 47-22-207039 URL: www.dlink.no

Russia	**D-Link Russia** Michurinski Prospekt 49, 117607 Moscow, Russia TEL: 7-095-737-3389 & 7-095-737-3492 FAX: 7-095-737-3390 URL: www.dlink.ru E-MAIL: vl@dlink.ru
Singapore	**D-Link International** International Business Park, #03-12 The Synergy, Singapore 609917 TEL: 65-774-6233 FAX: 65-774-6322 E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com
South Africa	**D-Link South Africa** Unit 2, Parkside, 86 Oak Avenue, Highveld Technopark, Centurion, Gauteng, South Africa TEL: 27 (0) 12-665-2165 FAX: 27 (0) 12-665-2186 URL: www.d-link.co.za E-MAIL: attie@d-link.co.za
Spain	**D-Link Iberia** C/Sabino De Arana, 56 Bajos, 08028 Barcelona, Spain TEL: 34 93 4090770 FAX: 34 93 4910795 URL: www.dlinkiberia.es E-MAIL: info@dlinkiberia.es
Sweden	**D-Link Sweden** P. O. Box 15036, S-167 15 Bromma, Sweden TEL: 46-(0) 8-564-61900 FAX: 46-(0) 8-564-61901 E-MAIL: info@dlink.se URL: www.dlink.se
Taiwan	**D-Link Taiwan** 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.tw E-MAIL: dssqa@tsc.dlinktw.com.tw
Turkey	**D-Link Middle East** Deniz Bilgisayar, Buyukdere Cad. Naci Kasim Sk., No. 5 Mecidiyekoy, Istanbul, Turkey TEL: 90-212-213-3400 FAX: 90-212-213-3420 E-MAIL: smorovati@dlink-me.com
U.A.E.	**D-Link Middle East** CHS Aptec (Dubai), P.O. Box 33550 Dubai U.A.E. TEL: 971-4-366-885 FAX: 971-4-355-941 E-MAIL: Wxavier@dlink-me.com
U.K.	**D-Link Europe** 4th Floor, Merit House, Edgware Road, Colindale, London NW9 5AB United Kingdom TEL: 44 (0) 20-8731-5555 FAX: 44 (0) 20-8731-5511 BBS: 44 (0) 181-235-5511

URL: www.dlink.co.uk E-MAIL: info@dlink.co.uk

U.S.A. **D-Link U.S.A.**
53 Discovery Drive, Irvine, CA 92618, USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033
BBS: 1-949-455-1779 & 1-949-455-9616
INFO: 1-800-326-1688 URL: www.dlink.com
E-MAIL: tech@dlink.com & support@dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr./Ms____
Organization: ______________________________ Dept. ________________
Your title at organization: _______________________________________
Telephone: _________________________ Fax: _________________________
Organization's full address: ______________________________________
____
Country: ____
Date of purchase (Month/Day/Year): ________________________________

Product Model	Product Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:

Reseller's name: ____
Telephone: _________________________ Fax: _________________________
Reseller's full address: ____
____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?
☐Home ☐Office ☐Travel ☐Company Business ☐Home Business ☐Personal Use

2. How many employees work at installation site?
☐1 employee ☐2-9 ☐10-49 ☐50-99 ☐100-499 ☐500-999 ☐1000 or more

3. What network protocol(s) does your organization use ?
☐XNS/IPX ☐TCP/IP ☐DECnet ☐Others____________________________

4. What network operating system(s) does your organization use ?
☐D-Link LANsmart ☐Novell NetWare ☐NetWare Lite ☐SCO Unix/Xenix ☐PC NFS ☐3Com 3+Open
☐Banyan Vines ☐DECnet Pathwork ☐Windows NT ☐Windows NTAS ☐Windows '95
☐Others____

5. What network management program does your organization use ?
☐D-View ☐HP OpenView/Windows ☐HP OpenView/Unix ☐SunNet Manager ☐Novell NMS
☐NetView 6000 ☐Others______________________________________

6. What network medium/media does your organization use ?
☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP
☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_________________

7. What applications are used on your network?
☐Desktop publishing ☐Spreadsheet ☐Word processing ☐CAD/CAM
☐Database management ☐Accounting ☐Others_____________________

8. What category best describes your company?
☐Aerospace ☐Engineering ☐Education ☐Finance ☐Hospital ☐Legal ☐Insurance/Real Estate ☐Manufacturing
☐Retail/Chainstore/Wholesale ☐Government ☐Transportation/Utilities/Communication ☐VAR
☐System house/company ☐Other________________________________

9. Would you recommend your D-Link product to a friend?
☐Yes ☐No ☐Don't know yet

10.Your comments on this product?
____
____

PLEASE
PLACE STAMP
HERE

TO:

D-Link®